CA Access Control

リファレンス ガイド

12.6

サードパーティに関する通知

CONTAINS IBM(R) 32-bit Runtime Environment for AIX(TM), Java(TM) 2 Technology Edition, Version 1.4 Modules

サンプル スクリプトおよびサンプル SDK コード

CA Access Control 製品に含まれているサンプル スクリプトおよびサンプル SDK コードは、情報提供のみを目的として現状有姿のまま提供されます。これらは特定の環境で調整が必要な場合があるため、テストや検証を実行せずに実稼働システムにデプロイしないでください。

CA Technologies では、これらのサンプルに対するサポートを提供していません。また、これらのスクリプトによって引き起こされるいかなるエラーにも責任を負わないものとします。

CA Technologies 製品リファレンス

このマニュアルが参照している CA Technologies の製品は以下のとおりです。

- CA Access Control Enterprise Edition
- CA Access Control
- CA Single Sign-On（CA SSO）
- CA Top Secret®
- CA ACF2™
- CA Audit
- CA Network and Systems Management（CA NSM、旧 Unicenter NSM and Unicenter TNG）
- CA Software Delivery（旧 Unicenter Software Delivery）
- CA Service Desk（旧 Unicenter Service Desk）
- CA User Activity Reporting Module（旧 CA Enterprise Log Manager）
- CA Identity Manager

ドキュメントの表記規則

CA Access Control のドキュメントには、以下の規則があります。

形式	意味
等幅フォント	コードまたはプログラムの出力
斜体	強調または新規用語
太字	表示されているとおりに入力する必要のある要素
スラッシュ（/）	UNIX および Windows のパスの記述で使用される、プラットフォームに依存しないディレクトリの区切り文字

また、本書では、コマンド構文およびユーザ入力の説明に（等幅フォントで）以下の特殊な規則を使用します。

形式	意味
斜体	ユーザが入力する必要のある情報
角かっこ（[]）で囲まれた文字列	オプションのオペランド
中かっこ（{}）で囲まれた文字列	必須のオペランド セット
パイプ（|）で区切られた選択項目	代替オペランド（1 つ選択）を区切ります。 たとえば、以下の例は「*ユーザ名*または*グループ名*のいずれか」を意味します。 {*username*|*groupname*}
…	前の項目または項目のグループが繰り返し可能なことを示します
下線	デフォルト値
スペースに続く、行末の円記号（¥）	本書では、コマンドの記述が 1 行に収まらない場合があります。このような場合、行末の空白とそれに続く円記号（¥）は、そのコマンドが次の行に続くことを示します。 **注**：このような円記号はコピーしないでください。また、改行はコマンドに含めないようにしてください。これらの文字は、実際のコマンド構文の一部ではありません。

例：コマンドの表記規則

以下のコードは、本書でのコマンド表記規則の使用方法を示しています。

```
ruler className [props({all|{propertyName1[,propertyName2]...})]
```

この例の内容

- 標準的な等幅フォントで表示されているコマンド名（ruler）は表示されているとおりに入力します。
- 斜体で表示されている *className* オプションは、クラス名（USER など）のプレースホルダです。
- 2 番目の角かっこで囲まれた部分を指定しなくても、コマンドは実行できます。この部分は、オプションのオペランドを示します。
- オプションのパラメータ（props）を使用する場合は、キーワード *all* を選択するか、またはカンマで区切られたプロパティ名を 1 つ以上指定します。

ファイル ロケーションに関する規則

CA Access Control のドキュメントには、ファイル ロケーションに関する以下の規則があります。

- *ACInstallDir* -- CA Access Control のデフォルトのインストール ディレクトリ。
  - Windows -- <インストール パス>
  - UNIX -- <インストール パス 2>
- *ACSharedDir* -- CA Access Control for UNIX で使用される、デフォルトのディレクトリ。
  - UNIX -- /opt/CA/AccessControlShared
- *ACServerInstallDir* -- CA Access Control エンタープライズ管理 のデフォルトのインストール ディレクトリ。
  - /opt/CA/AccessControlServer
- *DistServerInstallDir* -- デフォルトの配布サーバ インストール ディレクトリ。
  - /opt/CA/DistributionServer
- *JBoss_HOME* -- デフォルトの JBoss インストール ディレクトリ。
  - /opt/jboss-4.2.3.GA

CA への連絡先

テクニカル サポートの詳細については、弊社テクニカル サポートの Web サイト（http://www.ca.com/jp/support/）をご覧ください。

マニュアルの変更点

以下のドキュメントのアップデートは、本書の最新のリリース以降に行われたものです。

- ユーティリティ -- 以下のユーティリティ、サービス、デーモンの更新に基づいて章の内容が更新されました。
  - acuchkey
  - seaudit
  - sepmd
  - uxconsole -verify
- 環境設定ファイル - 以下の新しいセクションや変更されたセクションに基づいて章の内容が更新されました。
  - seos.ini—seosd
  - 監査ログ ルーティング環境設定ファイル selogrd.cgf
  - uxauth.ini - ad
  - uxauth.ini - agent
  - uxauth.ini - map

目次

第 1 章: 概要

このセクションには、以下のトピックが含まれています。

本書の内容

本書では、CA Access Control ユーティリティ、環境設定ファイル、ステータスコード、メッセージなどについて説明します。また、エンタープライズ管理機能、レポート機能、および拡張ポリシー管理機能を備えた CA Access Control Enterprise Edition についても説明します。

用語を簡潔に示すために、本書の全体を通してこの製品を CA Access Control と呼びます。

本書の対象読者

本書は、コマンドの実行、CA Access Control で保護される環境のメンテナンスや設定を担当するセキュリティ管理者およびシステム管理者を対象としています。

第 2 章: ユーティリティ

CA Access Control には数多くのユーティリティがあります。便宜上、本章ではそれらのユーティリティをアルファベット順に説明します。

acpwd ユーティリティ-特権アカウント パスワードのチェックインおよびチェックアウト

特権ユーザ パスワード管理エージェントを使用して、CA Access Control エンドポイントから特権アカウントの パスワードを取得します。コマンド ラインを使用して特権ユーザ パスワード管理 エージェントを実行すると、CA Access Control エンタープライズ管理 に接続して、チェック イン、チェック アウト、および特権アカウント パスワードの取得ができます。

このコマンドの形式は以下のようになります。

```
acpwd {-checkin | -checkout | -get} -account name -ep name -eptype type -container name -[timeout <timeout>] [-nologo] [-help]
```

-checkin

特権アカウント パスワードのチェックイン プロセスを実行します。

-checkout

特権アカウント パスワードのチェックアウト プロセスを実行します。

-get

チェック アウト プロセスを実行せずに、特権アカウント パスワードを取得します。

-account *name*

特権アカウント パスワードをチェックアウトするかまたはチェックインするかを定義します。

-ep *name*

特権アカウントが存在するエンドポイントの名前を定義します。

-eptype *type*

エンドポイントのタイプを指定します。

例: Windows Agentless

-container *name*

アカウントが存在するコンテナの名前を定義します。

-nologo

出力に追加情報なしでパスワードだけを表示するように指定します。

-timeout *timeout*

サーバからの応答を待機するタイムアウト期間を、秒単位で指定します。

-help

ヘルプ ファイルを表示します。

acuxchkey Utility-暗号化鍵の設定変更

acuxchkey ユーティリティを使用して、暗号化鍵とメッセージ キューの設定を変更します。このコマンドの形式は以下のようになります。

```
acuxchkey -t -pwd password
```

-t

メッセージ キューの変更オプションを指定します。

-pwd *password*

メッセージ キューのパスワードを定義します。

例: メッセージ キューのパスワードの変更

このコマンドは、変更されたメッセージ キューの暗号化されたパスワードをデータベースに保存します。パスワードは "secret" です。このパスワードはクリア テキストで指定し、二重引用符で囲む必要があります。

```
acuxchkey -t -pwd "secret"
```

例: 配布サーバの通信設定の変更

この例では、配布サーバの設定を変更して SSL と共に動作させる方法を示します。

```
env config
editres CONFIG accommon.ini section (communication) token (Distribution_Server)
value ("ssl://DS_host:7243")
```

詳細情報:

sechkey ユーティリティ - メッセージ キューのパスワードの変更 (P. 141)

ChangeEncryptionMethod ユーティリティ - 暗号化方式の変更

UNIX で該当

ChangeEncryptionMethod ユーティリティは、暗号化方式を変更します。

注: このユーティリティはスクリプト ファイルとして提供され、lbin ディレクトリに置かれます。

このユーティリティを実行すると、以下のいずれかの暗号化方式を選択できます。

- DEFAULT
- AES(128 ビット、192 ビット、または 256 ビット)
- DES
- TRIPLEDES
- SCRAMBLE

暗号化方式を指定しない場合、指定するように求めるメッセージが表示されます。このユーティリティは、システム内の既存の Policy Model を検索し、「sepmd -de pmd_name」を実行して復号化します。次に、libcrypt を新しい共有ライブラリ(libaes128、libaes192、libaes256、libdes、libtripledes、または libscramble)にリンクして暗号化方式を変更します。

注: このユーティリティを実行するには、CA Access Control が実行されている必要があります。暗号化方式を変更する場合、一時的に CA Access Control を停止するかどうかを確認するメッセージが表示されます。

重要: CA Access Control エンタープライズ管理 サーバと CA Access Control エンドポイントで同一の暗号化方式を使用していることを確認してください。既存の CA Access Control エンドポイントの暗号化方式を変更する場合、すべてのパスワード履歴が失われます。

このコマンドの形式は以下のようになります。

```
ChangeEncryptionMethod.sh [DES|TRIPLEDES|SCRAMBLE|AES128|AES192|AES256]
```

詳細情報:

sechkey ユーティリティ - 対称暗号化方式の変更 (P. 136)

dbmgr ユーティリティ

dbmgr ユーティリティを使用すると、CA Access Control データベース ファイルを作成、管理、およびメンテナンスできます。

注: このユーティリティは、旧バージョンの dbdump、rdbdump、dbutil、secredb、sedb2scr、および semigrate の各ユーティリティに代わるものです。

重要: このユーティリティは、問題を解決する際にサポート担当者の指示に従って使用する必要があります。 詳細については、当社テクニカル サポート (http://www.ca.com/jp/support/) にお問い合わせください。

dbmgr ユーティリティを実行するには、ADMIN 属性、AUDITOR 属性、または SERVER 属性が必要です。

このユーティリティはいくつかのタスクを処理します。以下の関連する機能があります。

タスク	Function
データベースの作成 (P. 35)	`dbmgr -create`
データベース情報の表示 (P. 38)	`dbmgr -dump`
データベースを定義するスクリプトの作成 (P. 40)	`dbmgr -export`
フラット ファイルへのデータベース データのコピー (P. 42)	`dbmgr -migrate`
既存のデータベースの管理 (P. 44)	`dbmgr -util`
データベースのバックアップ (P. 46)	`dbmgr -backup`
データベースのリストア (P. 47)	`dbmgr -restore`

dbmgr -create 機能 - データベースの作成

dbmgr -create は、空の新規データベースを生成する機能です。この機能は、インストール時と、データベースまたは PMDB の作成時にのみ使用します。CA Access Control によって、現在のディレクトリにデータベースが作成されます。

注:ユーザ定義クラスを新しいデータベースに追加する場合は、新しいデータベースを作成した後に seclassadm ユーティリティを実行します。

このコマンドの形式は以下のようになります。

```
dbmgr {-create|-c} {-c[q]|-h} [-d] [-f filename] ¥
    [-n] [-o] [-t terminalNames] ¥
    [-u userName [,userName...]] [-ux userName [,userName...]]¥
    [-v] [-w] [-k] [-n pathName]
```

-create|-c

dbmgr ユーティリティのデータベース作成機能を実行します。

-c

新しいデータベースを作成するかどうかを確認するメッセージを表示します。

-cq

確認メッセージを表示せずに、新しいデータベースを作成します。

-h

この機能のヘルプを表示します。

-d

データベースレイアウトドキュメントを出力します。出力には、データベース構造の詳細な説明およびデータベースで使用されているプロパティの形式が含まれています。

-f *filename*

標準出力デバイスではなく、ファイルを出力先として指定します。

-k

データベースの作成が完了したら、共存ユーティリティを実行するように指定します。

-n *pathName*

(UNIX のみ)。バックアップする CA Access Control データベースの完全パス名を定義します。

新しいデータベースを作成するときに、基本的なクラス スキーマが生成されます。seclassadm ユーティリティを使用してデータベースに新しいクラスを追加すると、クラスの情報はデータベース ディレクトリ内のファイルに格納されます。このクラス スキーマで特定のデータベース(Policy Model データベースなど)をバックアップするには、-n オプションでデータベースの場所を指定します。ユーザ定義クラスの情報はその場所から取得します。-n オプションを指定しない場合、クラスの情報ファイルはデータベースが作成されるローカル ディレクトリで検索されます。このファイルが見つからない場合は、アクティブな CA Access Control セキュリティ データベース ディレクトリからファイルが取得されます。

-o

Unicenter TNG クラスを既存のデータベースに追加します。

-t *terminalName*

データベースに作成するカンマ区切りの端末リストを定義します。スーパーユーザはこのリストからローカル データベースを管理できます。

-u *userName [,userName...]*

データベースに作成するカンマ区切りのユーザ リストを定義します。これらのユーザは CA Access Control セキュリティ管理者として定義されます。

-t オプションを指定した場合、これらのユーザには指定された端末からローカル データベースを管理する権限が付与されます。

-ux パラメータも参照してください。

-xu *userName [,userName...]*

カンマ区切りのエンタープライズ ユーザのリストを定義します。これらのユーザは CA Access Control セキュリティ管理者として定義されます。

-t オプションを指定した場合、これらのユーザには指定された端末からローカル データベースを管理する権限が付与されます。

ユーザが作成されない場合、dbmgr -create によってユーザが作成されます。このユーザは、ADMIN 属性、AUDITOR 属性、および IGN_HOL 属性を持つ、UNIX の *root* または Windows の Administrator に相当します。

-v

進行状況を示すメッセージを無効にします。

-w

Unicenter TNG クラスを含む新しいデータベースを作成します。

注: -v オプションと -d オプションを同時に指定することはできません。

例: Windows での新しいデータベースの作成

たとえば、c:¥temp> というシステム プロンプトで、以下のコマンドを入力します。

```
dbmgr -c -c -u user1 -t myterminal.company.com
```

メッセージに応答してデータベースの作成を確定すると、ユーティリティによって c:¥temp ディレクトリに新しいデータベースが作成されます。データベースに *user1* というユーザが作成されます。このユーザは、ADMIN 属性、AUDITOR 属性、および IGN_HOL 属性を持ち、*myterminal.company.com* という端末からデータベースを管理できます。

例: UNIX での新しいデータベースの作成

たとえば、¥tmp¥db ディレクトリから、以下のコマンドを入力します。

```
dbmgr -c -cq -d -f dbLayout
```

ユーティリティによって、¥tmp¥db ディレクトリに新しいデータベースが作成されます。また、データベース レイアウトドキュメントを含むファイル (dbLayout) も作成されます。デフォルトでは、データベースに *root* というユーザが作成され、ADMIN 属性、AUDITOR 属性、および IGN_HOL 属性が割り当てられます。

詳細情報:

seclassadm ユーティリティ - CA Access Control クラスの管理 (P. 142)
eACoexist ユーティリティ - 共存 Trusted プログラムの検出および登録 (P. 59)

dbmgr -dump 機能 - データベース情報の表示

dbmgr -dump は、データベースのレコードに関する情報を報告する機能です。この機能を実行すると、以下の処理が行われます。

- 指定されたクラスの複数のレコード情報を表示する
- 指定されたクラスの 1 つのレコード情報を表示する
- 指定されたレコードを除く、1 つのクラスのすべてのレコード情報を表示する
- クラスおよびプロパティの定義のリストを生成する
- ユーザが所属するグループのリストを生成する
- 特定のクラスのレコードのリストを生成する

この機能は CA Access Control デーモンが実行されていないことを前提としています。また、データベースが格納されているディレクトリから呼び出す必要があります。-r スイッチを指定する場合は、CA Access Control デーモンが実行されている必要があります。また、ADMIN 属性、AUDITOR 属性、または SERVER 属性が必要です。この機能を実行するには、データベース ファイルに対する読み取り権限および書き込み権限も必要です。

このコマンドの形式は以下のようになります。

```
dbmgr {-dump|-d} [-h] [-r] [-f fileName] ¥
    [c] [fc] [g user] [l class] [p class] [fp class] ¥
    [d class [props|@fileName] ¥
    [dn class [props|@fileName] ¥
    [e class record [props|@fileName] ¥
    [en class record [props|@fileName] ¥
    [o class record [props|@fileName] ¥
    [on class record [props|@fileName]
```

-dump|-d

dbmgr ユーティリティのデータベース ダンプ機能を実行します。

-f *fileName*

標準出力デバイスではなく、指定されたファイルに出力を送信します。

-h

この機能のヘルプを表示します。

-r

認証デーモンで現在使用されているデータベースに関する情報を表示します。

このオプションを省略すると、現在のディレクトリにあるデータベースに関する情報が表示されます。

c

データベースに定義されているすべてのクラスの名前を一覧表示します。

d *class* [*props*|*@fileName*]

1 つのクラスのすべてのレコードについて、選択したプロパティの値を表示します。*class* パラメータでクラス名を指定します。*props* パラメータには、値を表示する、スペース区切りのプロパティのリストを定義します。

ファイルからプロパティリストを読み込むには、アット マーク(@)を入力し、その後にファイルの完全パス名を指定します。 ファイル内の各プロパティは、別々の行に記述されている必要があります。

プロパティを指定しない場合は、すべてのプロパティの値が表示されます。

dn *class* [*props*|*@fileName*]

d オプションと同様に、値が不明なプロパティのみが表示されません。

e *class record* [*props*|*@fileName*]

特定のクラスの指定した 1 つのレコードを*除く*すべてのレコードについて、選択したプロパティの値を表示します。*class* パラメータでクラス名を指定します。 *record* パラメータで、リストから除外するレコードの名前を指定します。*props* パラメータには、値を表示する、スペース区切りのプロパティのリストを定義します。

ファイルからプロパティリストを読み込むには、アット マーク(@)を入力し、その後にファイルの完全パス名を指定します。 ファイル内の各プロパティは、別々の行に記述されている必要があります。

プロパティを指定しない場合は、すべてのプロパティの値が表示されます。

en *class record* [*props*|*@fileName*]

e オプションと同様に、値が不明なプロパティのみが表示されません。

fc

データベース内のすべてのクラスについて、すべてのクラス情報を一覧表示します。

fp *class*

指定されたクラスのプロパティについて、すべてのプロパティ情報を一覧表示します。

g *user*

指定されたユーザが所属するグループを一覧表示します。

l *class*

指定されたクラスのすべてのレコードを一覧表示します。

o *class record property* / on *class record property*

1 つのクラスの 1 つのレコードについて、選択したプロパティの値を表示します。*class* パラメータでクラス名を指定します。*record* パラメータでレコード名を指定します。*props* パラメータには、値を表示する、スペース区切りのプロパティのリストを定義します。

ファイルからプロパティリストを読み込むには、アット マーク(@)を入力し、その後にファイルの完全パス名を指定します。 ファイル内の各プロパティは、別々の行に記述されている必要があります。

プロパティを指定しない場合は、すべてのプロパティの値が表示されます。

o *class record property* / on *class record property*

o オプションと同様に、値が不明なプロパティのみが表示されません。

p *class*

指定されたクラスのプロパティ名を一覧表示します。

注: -r および -f 以外に 1 つのオプションのみ指定できます。

dbmgr -export 機能 - データベースを定義するスクリプトの作成

dbmgr -export は、データベースを他の端末に複製する機能です。既存のデータベースの定義に必要な selang のコマンドで構成されたスクリプトを生成します。

注: ファイルのバイト順序が異なる場合は、ネイティブ コマンド(UNIX の cp または tar コマンド、Windows の copy コマンドなど)を使用して、アーキテクチャ間でデータベース ファイルをコピーすることはできません。たとえば、Sparc ベースのコンピュータから Intel ベースのコンピュータにデータベースをコピーすることはできません。これらのコンピュータでは異なるバイト順序が使用されているためです。

重要: スクリプトを実行する前にスクリプトの内容を確認してください。

このコマンドの形式は以下のようになります。

```
dbmgr {-export|-e} {-l|-r} [-c className] [-f fileName]
```

-export|-e

dbmgr ユーティリティのデータベース エクスポート機能を実行します。

-h

この機能のヘルプを表示します。

--l

現在のディレクトリにあるデータベースをエクスポートします。

注: このオプションでは、CA Access Control デーモンが実行されていないことを前提としています。デーモンが実行中の場合は、デーモンが使用しているデータベースとは別のデータベースに対して操作を行うことが前提となります。

-r

CA Access Control で現在使用されているデータベースをエクスポートします。ADMIN 属性または SERVER 属性が必要です。また、CA Access Control デーモンが実行されている必要があります。

-c *className*

データベースからエクスポートするクラスのスペース区切りのリストを定義します。

-f *fileName*

標準出力デバイスではなく、指定されたファイルに出力を送信します。ファイルからコマンドを読み込むように selang に指示すると、ファイルから新しいデータベースを作成できます。

dbmgr -migrate 機能 - フラット ファイルへのデータのコピー

dbmgr -migrate は、既存のデータベースにあるユーザ レコードおよびプログラム レコードのデータをフラット ファイル（バイナリ形式）にコピーする機能です。フラット ファイルのデータを新しいデータベースにコピーすることもできます。データのインポート元のデータベースは、バージョン 1.21 以上である必要があります。

フラット ファイルから新しいデータベースにデータをコピーする場合は、フラット ファイルを作成したバージョンと同じバージョンのコピー機能を使用する必要があります。バージョンが複数ある場合は、最新バージョンを使用することを強くお勧めします。

注：セキュリティ上の理由から、古いデータベースから新しいデータベースにデータをコピーした後に、古いデータベース、新しいデータベースの作成に使用したスクリプト、およびこの機能を使用して作成したフラット ファイルを削除してください。

重要：この機能を使用する前に、必ずデータベースのバックアップを作成してください。

このコマンドの形式は以下のようになります。

```
dbmgr {migrate|-m} {-r|-w|-h} [-s] filename ¥
    [-v versionNumber] [-f fileName]
```

-migrate|-m

dbmgr ユーティリティのデータベース移行機能を実行します。

filename

データのコピー元またはコピー先のフラット ファイルを指定します。

-f *filename*

標準出力デバイスではなく、指定されたファイルに出力を送信します。

-h

この機能のヘルプを表示します。

-r

現在のディレクトリにあるデータベースを読み取り、*filename* で指定されたフラット ファイルに特定のデータをコピーします。

-s

データベースを直接読み取るのではなく、CA Access Control サーバを使用してデータベースの情報を読み取ります。このオプションは、-r スイッチと同時に指定した場合のみ有効です。

このオプションを使用するには、端末に対する管理者権限と、R(読み取り)および W(書き込み)のアクセス権が必要です。

このオプションを指定しない場合、現在のディレクトリにあるデータベースに対して読み取りまたは書き込みが行われます。

-v *versionNumber*

旧バージョンで作成されたフラット ファイルを読み取ります。このオプションは、-w スイッチと同時に指定した場合にのみ有効です。このオプションをファイル名の後に入力し、バージョン番号を指定します。

-w

filename で指定されたフラット ファイルを読み取り、現在のディレクトリにあるデータベースにデータをコピーします。

例: 既存のデータベースから新しいデータベースへのデータのコピー

以下の手順では、既存のデータベースから新しいデータベースにデータをコピーする方法を示します。古いデータベースは /tmp/old_db ディレクトリにあるとします。新しいデータベースは *ACInstallDir*/seosdb ディレクトリにあるとします(*ACInstallDir* は CA Access Control のインストール ディレクトリです)。

注: この手順では UNIX のパス名を使用していますが、パス名を適切に変更することで Windows にも適用できます。

1. スーパーユーザとしてログインします。
2. CA Access Control デーモンが実行中の場合は、以下のコマンドを入力して停止します。

   ```
   secons -s
   ```

3. 古いデータベースを別の場所またはバックアップ用のメディアにコピーして、バックアップを作成します。
4. データベースを /tmp/old_db にコピーします。次に、古いデータベースに対して dbmgr ユーティリティを実行して、古いデータベースを複製するスクリプトを作成します。

   ```
   cd /tmp/old_db
   /opt/CA/AccessControl//bin/dbmgr -export -l -f lang_script
   ```

5. 新しいデータベースを作成します。

   ```
   cd /opt/CA/AccessControl//seosdb
   /opt/CA/AccessControl//bin/dbmgr -c -cq
   ```

6. 前の手順で生成されたスクリプトを実行して、新しいデータベースを作成します。

   ```
   cd /opt/CA/AccessControl//seosdb
   /opt/CA/AccessControl//bin/selang -l /tmp/old_db/lang_script
   ```

7. dbmgr ユーティリティを実行して、古いデータベースのデータを保存するフラット ファイルを作成します。

   ```
   cd /tmp/old_db
   /opt/CA/AccessControl//bin/dbmgr -migrate -r flat_file
   ```

8. 新しいデータベースにフラット ファイルのデータをロードします。

   ```
   cd /opt/CA/AccessControl//seosdb
   /opt/CA/AccessControl//bin/dbmgr -migrate -w /tmp/old_db/flat_file
   ```

dbmgr -util 機能 - 既存のデータベースの管理

dbmgr -util は、データベースの管理およびメンテナンスを実行する機能です。CA Access Control が現在実行中でないことが前提となります。この機能は、データベースが格納されているディレクトリから実行します。

-util は、*filename* パラメータで指定したローカル データベースを管理および操作するオプションです。データベース ファイルは拡張子 .dat が付いた DBIO ファイルです。-util オプションでは、データベース インデックス ファイル（拡張子 .001 のファイル）を使用できません。

このコマンドの形式は以下のようになります。

```
dbmgr {-util|-u} [-h] ¥
    [-all filename] ¥
    [-build filename] ¥
    [-check] ¥
    [-close] ¥
    [-dump filename] ¥
    [-dup src dst] ¥
    [-fast] ¥
    [-free filename] ¥
    [-index filename] ¥
    [-key filename] ¥
    [-load db ascii ¥
    [-scan filename] ¥
    [-scana filename] ¥
    [-stat filename] ¥
    [-verify] ¥
    [-f fileName]
```

-util-u

dbmgr ユーティリティのデータベース管理およびメンテナンスの機能を実行します。

-all *filename*

すべてのインデックス チェックを実行します。これは、*-index* オプションおよび *-free* オプションを指定した場合と同様です。

-build *filename*

データ レコードに基づいて DBIO のインデックスを作成します。

-check

（UNIX のみ）。すべてのデータベース ファイルのすべてのインデックス エントリに対して、状態および整合性の高速チェックを実行します。

-閉じる

開いているデータベースを閉じます。

-dump *filename*

データ ファイルを ASCII ファイルとして標準出力デバイスにダンプします。

-dup *src dst*

ファイル ヘッダに基づいて DBIO ファイルを複製します。

-f *fileName*

標準出力デバイスではなく、指定されたファイルに出力を送信します。

-fast

すべてのデータベース ファイルのすべてのインデックス エントリに対して、高速な状態チェックを実行します。

-free *filename*

フリー インデックスをチェックします。

-index *filename*

インデックスの整合性をチェックします。

-key *filename*

インデックス ファイルを順次スキャンします。

-load *db* ascii

ASCII ファイルをロードして DBIO ファイルに変換します。

-scan *filename*

データベースを順次スキャンします。

-scana *filename*

削除されたレコードも含め、データベースを順次スキャンします。

-stat *filename*

データベース ファイルのヘッダ情報を一覧表示します。

-確認

(UNIX のみ)。すべてのクラスについて、特定の事前定義オブジェクト (SEOS、ADMIN、および UACC など) がデータベース内に存在するかどうかを検証します。

dbmgr -backup 機能 - データベースのバックアップ

dbmgr -backup は、CA Access Control データベースを指定したディレクトリにオンラインでバックアップする機能です。この機能は、CA Access Control デーモンが実行されているかどうかに関わらず利用できます。

このコマンドの形式は以下のようになります。

```
dbmgr {-backup|-b} backup_directory
```

-backup|-b

dbmgr ユーティリティのデータベース バックアップ機能を実行します。

backup_directory

バックアップ ディレクトリを定義します。このディレクトリには、リモート コンピュータを指定できません。指定したディレクトリが存在しない場合は、作成されます。

dbmgr -restore 機能 - データベースのリストア

UNIX で該当

dbmgr -restore は、指定したディレクトリに CA Access Control データベースをオンラインでリストアする機能です。この機能は、CA Access Control デーモンが実行されているかどうかに関わらず利用できます。

このコマンドの形式は以下のようになります。

```
dbmgr {-restore|-r} restore_directory
```

-restore|-r

dbmgr ユーティリティのデータベース リストア機能を実行します。

restore_directory

リストアするデータベースがあるディレクトリを指定します。

defclass ユーティリティ - ユーザ定義のアセット タイプのクラスとしての定義

CA Access Control は、各 CA Access Control データベースおよび定義済みの新しい PMDB に Unicenter TNG の基本的なアセット タイプを定義します。defclass スクリプトは、CA Access Control データベースにユーザ定義のセキュリティ アセット タイプを CA Access Control クラスとして定義します。

注: インストール プログラムで[Unicenter 統合]を選択すると、このスクリプトが自動的に実行されます。新しい PMDB の作成時には、このスクリプトを必ず手動で実行する必要があります。

このコマンドの形式は以下のようになります。

```
defclass
```

注: UNIX では、このユーティリティはスクリプト ファイルとして用意されています。実行するには .sh という拡張子を指定する必要があります。Unicenter 統合を有効にした場合(デフォルトでは無効)にのみ利用できるようになります。

DictImport ユーティリティ - 辞書ファイルのインポート

DictImport ユーティリティは、辞書ファイルを準備し、CA Access Control データベースにインポートします。CA Access Control をインストールした後、辞書ファイルを CA Access Control データベースにインポートし、有効化する必要があります。パスワードによる保護を設定できます。

DictImport ユーティリティは、use_dbdict のパスワード ルールを *db* に設定し、DICTIONARY クラスおよび PASSWORD クラスを有効化します。

注: PASSWORD クラスが有効になっていない場合、一元化された辞書は無効になります。

このコマンドの形式は以下のようになります。

```
DictImport [-h] [-o selangFilename] [-f dictionaryFilename]
```

注: このユーティリティはスクリプト ファイルとして提供され、lbin ディレクトリに置かれます。

-f *dictionaryFilename*

指定されたファイルから辞書の単語をすべてインポートする selang のコマンドを生成します。このオプションを省略すると、辞書ファイルは環境設定の値から定義されます。

-h

このユーティリティのヘルプ画面を表示します。

-o *selangFilename*

指定されたファイルに selang のコマンドを書き込みます。このオプションを省略すると、selang のコマンドは標準出力デバイスに書き込まれます。

dmsmgr ユーティリティ

dmsmgr ユーティリティを使用すると、拡張ポリシー管理のインフラストクチャを管理できます。インフラストラクチャ コンポーネントには、CA Access Control エンドポイント、デプロイ マップ サーバ（DMS）、および分散ホスト（DH）が含まれます。

このユーティリティはいくつかのタスクを処理します。以下の関連する機能があります。

タスク	Function
DMS または DH の作成 (P. 50)	`dmsmgr -create`
DMS または DH の削除 (P. 51)	`dmsmgr -remove`
DMS データベースからの古いノードの削除 (P. 52)	`dmsmgr -cleanup`
拡張ポリシー管理の設定 (P. 53)	`dmsmgr -config`
DMS または DH のリストア (P. 54)	`dmsmgr -restore`

dmsmgr -create 機能 - DMS または DH の作成

dmsmgr -create は、デプロイ マップ サーバ（DMS）または分散ホスト（DH）を CA Access Control がインストールされているコンピュータに作成する機能です。

注：インストール中に DMS または DH を作成することもできます。

注：このユーティリティを実行するユーザには、作成される DMS または DH に対する管理権限が常に与えられます。

このコマンドの形式は以下のようになります。

```
dmsmgr -create -auto [-osgroups] [-admin user [,user...]] [-xadmin user [,user...]]
¥
[-desktop hosts]

dmsmgr -create -dms name ¥
[-admin user [,user...]] [-xadmin user [,user...]] ¥
[-desktop hosts] [-subscriber dh-names]

dmsmgr -create -dh name [-parent dms_name@hostname] ¥
[-admin user [,user...]] [-xadmin user [,user...]] ¥
[-desktop hosts]
```

-admin *user* [,*user*...]]

（オプション）作成される DMS または DH の管理者として内部ユーザを指定します。

-auto

DMS または DH をデフォルト名（DMS__、DH__、および DH__WRITER）で作成します。

このオプションを使用すると、DMS と DH、および両者間の必要な関連付けを簡単に作成できます。

-osgroups

（オプション）DMS を作成するときに、定義済みホスト グループを作成するように指定します。

-desktop *hosts*

（オプション）DMS または DH が作成されるコンピュータに対して TERMINAL アクセス権限を持つコンピュータのカンマ区切りのリストを定義します。

注：指定の有無に関わらず、このユーティリティを実行している端末には、作成される DMS または DH に対する管理権限が常に与えられます。

-dh *name*

ローカル ホストに指定した名前で DH を作成します。

注: このオプションを使用して DH を作成すると、DH がすでにサブスクライブされ、以前にポリシーが送信されていなくても、DMS と DH を同期させる必要があることが CA Access Control から通知されます。このメッセージは必要な手順を知らせる通知であり、実際の手順であるとは限りません。必要な手順がすべて完了していれば、このメッセージを無視してもかまいません。

-dms *name*

ローカル ホストに指定した名前で DMS を作成します。

-parent *dms_name@hostname*

(オプション) 作成される DH がエンドポイント通知を送信する DMS を指定します。DMS は *DMS_name@hostname* という形式で指定します。

-subscriber *dh_names*

(オプション) 作成される DMS がポリシーの更新を配布する DH PMDB のカンマ区切りのリストを定義します。各 DH は *DH_name@hostname* という形式で指定します。

-xadmin *user* [,*user*...]]

(オプション) 作成される DMS または DH の管理者としてエンタープライズ ユーザを指定します。

dmsmgr -remove 機能 - DMS または DH の削除

dmsmgr -remove は、CA Access Control がインストールされているコンピュータから DMS または DH を削除する機能です。

このコマンドの形式は以下のようになります。

```
dmsmgr -remove {-dms|dh} name
```

```
dmsmgr -remove -auto
```

-auto

デフォルトの DMS および DH をローカル ホストから削除します。

削除されるのは、インストール時または dmsmgr -create -auto を使用したときにデフォルトで作成された DMS データベースおよび DH データベースです。

-dh *name*

指定した名前の DH をローカル ホストから削除します。

-dms *name*

指定した名前の DMS をローカル ホストから削除します。

dmsmgr -cleanup 機能 - 古いノードの削除

dmsmgr -cleanup は、DMS データベースまたは DH データベースから古いノードを削除する機能です。削除されるのは、CA Access Control ノードを表す HNODE オブジェクトのうち、指定された期間、無効になっていたオブジェクトです。

注: 定期的なメンテナンス手順として、これらの古いノードから DMS および DH を消去する必要があります。

このコマンドの形式は以下のようになります。

```
dmsmgr -cleanup {-hnode|-deployment} -days number {-dms|-dh} name

dmsmgr -cleanup -policy name -vcount number {-dms|dh} name
```

-hnode

CA Access Control ノードを表す HNODE オブジェクトのうち、指定した日数（*number*）を超えて無効になっているオブジェクトを削除します。

-deployment

指定した日数（*number*）より古い DEPLOYMENT オブジェクトを削除します。

-policy *name*

指定したポリシーに属し、指定したバージョン番号（*number*）より古い POLICY オブジェクト（ポリシー バージョン）を削除します。

-dh *name*

古いノードを削除する DH の名前を指定します。

-dms *name*

古いノードを削除する DMS の名前を指定します。

-vcount

保存するバージョンの数を定義します。

dmsmgr -config 機能 - 拡張ポリシー管理の設定

dmsmgr -config は、拡張ポリシー管理を設定する機能です。

このコマンドの形式は以下のようになります。

```
dmsmgr -config[-] [host_name] {-endpoint|-dhname names|-drname names}

dmsmgr -config -osgroups [-dms name]
```

-config[-]

拡張ポリシー管理の環境設定を設定または削除します。

-dhname *names*

エンドポイントを設定して、カンマ区切りの分散ホストのリストを処理します。

-dms *name*

自動ホスト グループを作成した DMS の名前を定義します。

-drname *names*

エンドポイントを設定して、カンマ区切りの惨事復旧分散ホストのリストを処理します。

-endpoint

エンドポイントを拡張ポリシー管理用に設定します。

host_name

host_name に対して設定を実行します。ホストを指定しない場合は、ローカル コンピュータが設定されます。

-osgroups

自動ホスト グループを DMS に追加します。

注: 自動ホスト グループの詳細については、「*エンタープライズ管理ガイド*」を参照してください。

dmsmgr -restore 機能 - DMS または DH のリストア

dmsmgr -restore 機能は DMS または DH をバックアップ ファイルからリストアします。DMS や DH は、CA Access Control が実行中、または停止しているときに、既存の DMS に、または新しいディレクトリにリストアできます。

このコマンドの形式は以下のようになります。

```
dmsmgr -restore -dms name -source path¥
[-replica name|-parent name] [-subscriber dhname[,dhname...]]¥
[-admin user[,user...]] [-xadmin user[,user...]]

dmsmgr -restore -dh name -source path¥
[-parent name] [-admin user[,user...]]¥
[-xadmin user[,user...]] [-desktop host[,host...]]
```

-admin *user*[,*user*...]

(UNIX)リストアされる DMS または DH の管理者として内部ユーザを指定します。

-desktop *host*[, *host*...]

(オプション)リストアする DH があるコンピュータに対して TERMINAL アクセス権限を持つコンピュータのリストを定義します。

注: 指定の有無に関わらず、このユーティリティを実行している端末には、リストアする DH に対する管理権限が常に与えられます。

-dh *name*

ローカル ホストにリストアする DH の名前を定義します。

-dms *name*

ローカル ホストにリストアする DMS の名前を定義します。

-parent *name*

(オプション) サブスクライバの親の名前を定義します。ディザスタ リカバリ デプロイに CA Access Control をセットアップしており、ディザスタ DMS または DH をリストアする場合は、このパラメータを使用します。ディザスタ DMS をリストアする場合は本番 DMS の名前を指定し、DH をリストアする場合は親 DMS の名前を指定します。親は、*name@hostname* のフォーマットで指定します。

-replica *name*

(オプション) ディザスタ リカバリ DMS の名前を定義します。ディザスタ リカバリ デプロイに CA Access Control をセットアップしており、本番 DMS をリストアする場合は、このパラメータを使用します。ディザスタ リカバリ DMS 名を「*DMS_name@hostname*」という形式で指定します。

-source *path*

リストアするバックアップ ファイルが存在するディレクトリを定義します。

-subscriber *dh_name*[, *dh_name*...]

(オプション) リストアされる DMS がポリシーの更新を送信する DH のリストをカンマ区切りで定義します。各 DH は *DH_name@hostname* という形式で指定します。

-xadmin *user*[,*user*...]

(UNIX) リストアされる DMS または DH の管理者としてエンタープライズ ユーザを定義します。

eacpg_gen ユーティリティ - ベスト プラクティス ポリシーの定義

Linux で有効

eacpg_gen は、ポリシー生成プログラムとも呼ばれます。このユーティリティにはメニュー方式が採用されており、CA Access Control アプリケーションのポリシーを容易に定義できます。ポリシー生成プログラムは、CA Access Control ルールが設定されていないテスト システムで使用できます。重要な電子資産に対してセキュリティのベスト プラクティスを適用することによって、エンタープライズ アプリケーションやオペレーティング システム、および機密データを保護することを目的としています。

アプリケーション セルは、「default-deny」パラダイムを使用して作成されます。このポリシーは、UNIX の chroot() jail の概念に似ています。このようなポリシーを生成してインターネットを利用するアプリケーションに適用すると、アプリケーションの使用によってホストのセキュリティが侵害されるリスクを飛躍的に減少させることができます。

1 つのアプリケーション セルは、あるアプリケーションをブロックする 1 つのアクセス制御リスト（ACL）ルールに相当します。eacpg_gen は、アプリケーションごとに複数のアプリケーション セルを生成します。アプリケーション セルによって、アクセスが特定のリソースのみに制限されます。セル ポリシーで保護されたプロセスは、ポリシーによって明確にアクセスが許可されたリソース以外にはアクセスできません。これにより、潜在的な攻撃者による権限のないディスク領域への書き込みや、権限のないバイナリ ファイルの実行を防止できます。

注: このユーティリティを実行する前に、secadmin および group secadmin がデータベースに存在していることを確認してください。

ポリシーの生成にはいくつか重要な手順があります。

- 初期化
- アプリケーションの検査
- アプリケーションのテスト
- ポリシーの生成
- ポリシーの適用
- ポリシーのテスト

このコマンドの形式は以下のようになります。

```
eacpg_gen ¥
    [-u user] ¥
    [-g group] ¥
    [-p path] ¥
    [-o owner] ¥
    [-w wheel] ¥
    [-m machine] ¥
    [-a] ¥
    [-s file] ¥
    [-# step] ¥
    [-x]
```

-u *user*

プロセスを実行するユーザを指定します。

-g *group*

プロセスを所有するグループの名前を指定します。

-p *path*

プログラムの完全パスを指定します

-o *owner*

ポリシーの所有者を指定します。

-w *wheel*

'secadmins' グループとして設定します(推奨)。

-m *machine*

コンピュータ名を指定します。

-a

生成されたルールを適用するかどうかを設定します。

-s *file*

ポリシー ルールを保存する場所の完全パスおよびファイル名を指定します。

-# *step 1-2*

2 に設定する必要があります。

-x

warn モードと fail モードを切り替えます。

例: ポリシー生成プログラムの実行

1. (初期化)。ポリシー生成プログラムを実行します。

   ```
   eacpg_gen
   ```

2. プロンプトで「**y**」と入力し、システムを warn モードにします。
3. ポリシー生成プログラムに実行可能ファイルの完全パスを指定します。以下に例を示します。

   ```
   /work/WebServers/apache_1.3.26/bin/htppd
   ```

4. デフォルトのユーザ名を使用します。
5. デフォルトのグループ名を使用します。
6. プロンプトで「**y**」と入力し、情報が正しいかどうかを確認します。

   (アプリケーションの検査)。ポリシー生成プログラムによって、ポリシーの作成対象となるプロセスについてのデータ収集が開始されます。

7. 画面に表示される情報を確認し、Enter キーを押します。
8. (アプリケーションのテスト)。アプリケーションを起動します。例:

   ```
   ./apachectl start
   ```

9. アプリケーションを停止します。例:

   ```
   ./apachectl stop
   ```

   注: この時点では、アプリケーションを起動した後、停止しています。もう一度アプリケーションを起動して、通常使用のデータを収集することをお勧めします。検査にかける時間には、特に制限はありません。実行時間が長くなるほど、ポリシー生成プログラムが収集するデータが増加し、完成後のポリシーがより正確になります。十分なデータを収集したら、次の手順に進みます。

10. (ポリシーの生成)。ポリシーをファイルに保存します(「*filename*.txt」と入力し、Enter キーを押します)。

11. (ポリシーの適用)。「**y**」と入力してポリシーを適用します。

12. 「**y**」と入力してシステムを *Fail* モードに設定し、ポリシーの実施を開始します。

13. (ポリシーのテスト)。ポリシーをテストします。

    以下に、evil.html という名前のファイルに対して行ったポリシー テストのサンプル画面を示します。

```
Linux:/srv/www/htdocs: #telnet localhost 80
Trying ::1...
telnet: connect to address ::1: Connection refused
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
GET /evil.html
<!DOCTYPE HTML PUBLIC “-//IETF//DTD HTML 2.0//EN”>
<HTML><HEAD>
<TITLE>403 Forbidden</TITLE>
<HEAD><BODY>
<H1>Forbidden</H1>
You don't have permission to access /evil.html
on the server. <P>
<HR>
<ADDRESS>Apache/1.3.26 Server at linux.local Port 80</ADDRESS>
</BODY></HTML>
Connection closed by foreign host.
Linux:/srv/www/htdocs# []
```

    ポリシーが適用されたため、evil.html というファイルは無効になりました。これは、ファイルが通常使用のプロファイルの範囲外であったためです。

eACoexist ユーティリティ - 共存 Trusted プログラムの検出および登録

Windows で該当

eACoexist ユーティリティはローカル システム内で共存するプログラム（CA Anti-Virus など）を検出します。検出されたプログラムが Trusted 状態である場合は、CA Access Control は SPECIALPGM ルールを使用してプログラムを登録します。特別プログラム ルールではそのプログラムへのアクセスのタイプを定義し、アクセスを付与するときに CA Access Control が確実にそれを回避するようにします。

このコマンドの形式は以下のようになります。

```
eACoexist [plug-in-path]
```

plug-in-path

（オプション）共存プログラムに使用する共存プラグインが含まれたフォルダへのパスを定義します。

パスを定義しないと、プログラムは共存プラグインが保存されているデフォルトのパスを使用します（*ACInstallDir*/Coexistence）。

詳細情報:

共存ユーティリティの機能 (P. 60)
response.ini - 共存ユーティリティの設定 (P. 77)

共存ユーティリティの機能

CA Access Control が提供する共存ユーティリティ(eACoexist)を使用すると、ローカル コンピュータ上の他のプログラムとの潜在的な衝突を解決することができます。CA Access Control がこれらの潜在的な衝突を解決するために行う動作について理解し、それらの衝突を解決する方法に影響を与えることができるように、ユーティリティの機能を理解する必要があります。

共存ユーティリティが実行すると、以下のアクションを行います。

1. 以下の条件の *1* つが該当しているか確認します。
   a. CA Access Control が実行されていないこと
   b. ADMIN 属性が割り当てられていること

   いずれの条件にも該当しない場合、ユーティリティは終了します。
2. 以下のようにして response.ini ファイルを検索します。
   - ユーティリティがインストール中に実行する場合は、次のパスを使用します。*media_drive*:¥Coexistence¥*_architecture*
   - CA Access Control がコンピュータにインストールされている場合は、以下のレジストリ キー値を使用します。

     HKLM¥SOFTWARE¥ComputerAssociates¥AccessControl¥AccessControl¥SeOSD¥ResponseFile

   ファイルが存在しない場合、ユーティリティは終了します。
3. 以下のようにして共存プラグイン ディレクトリを検索します。
   - ユーティリティを実行していて、コマンド ラインからパラメータを渡す場合は、これをプラグインのパスとして使用します。
   - ユーティリティがインストール中に実行する場合は、次のパスを使用します。*media_drive*:¥Coexistence¥*_architecture*
   - パラメータなしでユーティリティを実行すると、文字列「¥Coexistence」が以下のレジストリ キー値に連結されます。

     HKLM¥SOFTWARE¥ComputerAssociates¥AccessControl¥AccessControl¥SeOSPath

   ディレクトリが存在しない場合、またはディレクトリに共存プラグインがない場合、ユーティリティは終了します。

4. 検出プロセスを実行します。

   これを行うには、共存プラグイン ディレクトリ内の実行ファイルを表示して、以下のようにして 1 つずつ実行します。

   a. プラグイン実行の結果を %windir%¥EACDiscovery.ini に保存します。

      注: プラグイン検出プロセスが正常に終了したら、ユーティリティは自動的にこのファイルを削除します。

   b. 出力ファイル EACDiscovery.ini が存在するかどうか確認します。

      ファイルが存在しない場合は、ユーティリティは引き続き次のプラグインを実行します。

   c. EACDiscovery.ini の各製品セクションでは、セクション(製品)名およびバージョン値を連結して応答ファイルに一致するセクションが含まれるかどうか確認します。

      注: response.ini ファイルには、共存プログラムごとにセクションがあります。たとえば、eTrust Audit-1.5 など、セクション名がバージョン番号と共に表示される場合は、ユーティリティは指定されたバージョンでのみアクションを実行します。

   d. 一致するセクションが応答ファイルに存在する場合は、そのセクションの Act-Utility-0 の値によって設定されたアクションを以下のようにして実行します。

      - **1** - 検出された製品が CA Access Control と互換性のないことを示す警告を発行します。
      - **2** - 検出された製品のサービスを停止します。

        ユーティリティは検出された製品のサービスを EACDiscovery.ini ファイルから取得します。
      - **3** - 2 と同じですが、CA Access Control のインストールの間です。
      - **4** - 検出された製品のサービスを開始します。

        ユーティリティは検出された製品のサービスを EACDiscovery.ini ファイルから取得します。

- **5** - 検出された製品のプロセスで trusted プログラム ルール（SPECIALPGM）を作成して CA Access Control を開始します。

  ユーティリティは検出された製品のプロセスを EACDiscovery.ini ファイルから取得します。また、このファイルからそれぞれのプログラム タイプ（pgmtype）も取得します。次に、CA Access Control が開始するときに実行する一時スクリプト ファイル（*ACInstallDir*¥Data¥discoveryscp）を作成します。

- **6** - 2 と同じですが、CA Access Control のアンインストールの間です。

中: 各セクションには複数のアクションを含めることができます。たとえば、「Act-Utility-0」、「Act-Utility-1」、および「Act-Utility-2」を含めると、この順番で実行されます。

詳細情報:

Policy Manager プラグインの概要 (P. 63)
BrightStor プラグインの機能 (P. 64)
Dr. Watson プラグインの機能 (P. 66)
eTrust AV プラグインの概要 (P. 67)
Scout プラグインの機能 (P. 68)
Unicenter プラグインの概要 (P. 68)
Asset Management プラグインの概要 (P. 69)
Windows プラグインの概要 (P. 71)
eTrust Audit プラグインの概要 (P. 71)
eTrust Audit80 プラグインの概要 (P. 73)
F-Secure Antivirus プラグインの概要 (P. 74)
McAfee VirusScan プラグインの概要 (P. 75)
Windows Modules Installer プラグインの概要 (P. 75)
Services and Controller プラグインの概要 (P. 76)
リソース ホスティング サブシステム プラグインのしくみ (P. 76)

Policy Manager プラグインの概要

以下のように、CA Access Control インストールの開始前に、共存ユーティリティが Policy Manager プラグインを実行してコンピュータ内の Policy Manager レジストリ キーおよび実行可能ファイルをスキャンします。

- 次のレジストリ キーの存在を照会します。

  HKLM¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥App Paths¥SeAM.Exe

  レジストリ キーが存在する場合、プラグインは以下のように動作します。

  - パス エントリの値を読み取ります。
  - 以下の実行可能ファイルのパス名を返します。

    FilePathFromRegistry¥Bin¥SeAM.exe

  - CA Access Control インストール時に互換性の警告を発行します。

    これは、応答ファイルに定義されているデフォルト アクションです。Policy Manager プラグインは、信頼できるプログラム(SPECIALPGM)ルールをデフォルトでは追加しません。

注: 応答ファイルは、規定ステージで共存ユーティリティが実行するデフォルト アクションを決定します(CA Access Control インストール前に実行すること、CA Access Control インストール後に実行することなど)。また、Policy Manager アプリケーションには CA Access Control が提供されません。

BrightStor プラグインの機能

共存ユーティリティは、CA Access Control のインストールの最後およびユーティリティが実行されるたびに、以下のようにして BrightStor プラグインを実行して CA BrightStor レジストリ キーおよび実行ファイルについてコンピュータをスキャンします。

1. 以下のレジストリ キーが存在するかどうかをクエリします。

   HKLM¥SOFTWARE¥ComputerAssociates¥BrightStor ARCserve Backup¥UniversalClientAgent¥Common
   HKLM¥SOFTWARE¥ComputerAssociates¥Cheetah¥UniversalClientAgent¥Common
   HKLM¥SOFTWARE¥ComputerAssociates¥BrightStor Enterprise Backup¥UniversalClientAgent¥Common

   最初のレジストリ キーが存在する場合は、プラグインは以下のようにします。

   - パス エントリの値を読み取ります。
   - 以下の実行可能ファイルのパス名を返します。

     FilePathFromRegistry¥UnivAgent.exe

   - タイプ DCM の SPECIALPGM リソースを作成します。

     これは、応答ファイルに定義されているデフォルト アクションです。

2. 手順 1 でプラグインがレジストリ キーを検出できない場合は、以下のレジストリ キーが存在するかどうかをクエリします。

   HKLM¥SOFTWARE¥ComputerAssociates¥BrightStor ARCserve Backup¥Base¥Path
   HKLM¥SOFTWARE¥ComputerAssociates¥Cheetah¥Base¥Path
   HKLM¥SOFTWARE¥ComputerAssociates¥BrightStor Enterprise Backup¥Base¥Path

   最初のレジストリ キーが存在する場合は、プラグインは以下のようにします。

   - HOME エントリの値を読み取ります。
   - 以下の実行可能ファイルのパス名を返します。

     FilePathFromRegistry¥carunjob.exe

   - タイプ DCM の SPECIALPGM リソースを作成します。

     これは、応答ファイルに定義されているデフォルト アクションです。

3. 手順 2 でもプラグインがレジストリ キーを検出できない場合は、以下のレジストリ キーが存在するかどうかをクエリします。

   HKLM¥SOFTWARE¥ComputerAssociates¥ARCserveIT¥Base¥Path

   レジストリ キーが存在する場合、プラグインは以下のように動作します。

   - HOME エントリの値を読み取ります。
   - 以下の実行可能ファイルのパス名を返します。

     FilePathFromRegistry¥ASRunJob.exe

   - タイプ DCM の SPECIALPGM リソースを作成します。

     これは、応答ファイルに定義されているデフォルト アクションです。

4. 以下のレジストリ キーが存在するかどうかをクエリします。

   HKLM¥SOFTWARE¥ComputerAssociates¥CA BAOF¥CurrentVersion
   HKLM¥SOFTWARE¥ComputerAssociates¥BrightStor Backup Agent for Open Files¥CurrentVersion

   最初のレジストリ キーが存在する場合は、プラグインは以下のようにします。

   - ServicePath エントリの値を読み取ります。
   - *ServicePathFromRegistry* にタイプ DCM の SPECIALPGM リソースを作成します。

     これは、応答ファイルに定義されているデフォルト アクションです。

注: 応答ファイルは、規定ステージで共存ユーティリティが実行するデフォルト アクションを決定します（CA Access Control インストール前に実行すること、CA Access Control インストール後に実行することなど）。

Dr. Watson プラグインの機能

共存ユーティリティは、Dr. Watson プラグインを実行して Dr. Watson の実行ファイルについて CA Access Control のインストールの最後およびユーティリティが実行されるたびに、以下のようにしてコンピュータをスキャンします。

- 以下のパス名が存在するかどうかクエリします。

  ```
  %windir%¥system32¥drwtsn32.exe
  ```

  ファイルが存在する場合は、プラグインはタイプ DCM の SPECIALPGM リソースを作成します。

  これは、応答ファイルに定義されているデフォルト アクションです。

注: 応答ファイルは、規定ステージで共存ユーティリティが実行するデフォルト アクションを決定します（CA Access Control インストール前に実行すること、CA Access Control インストール後に実行することなど）。

eTrust AV プラグインの概要

共存ユーティリティは、CA Access Control のインストールの最後およびユーティリティが実行されるたびに、以下のようにして eTrust AV プラグインを実行して CA Antivirus レジストリ キーおよび実行ファイルについてコンピュータをスキャンします。

1. 以下のレジストリ キーのエントリ値を読み取ります。

   HKLM¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥App Paths¥InocIT.Exe¥Path
   HKLM¥SOFTWARE¥ComputerAssociates¥eTrustITM¥CurrentVersion¥Path¥Home

   以下のエントリのいずれか 1 つが値を返した場合、プラグインはタイプ DCM の以下の SPECIALPGM リソースを作成します。

   - *FilePathFromRegistry*¥InoRT.exe
   - *FilePathFromRegistry*¥InoTask.exe
   - *FilePathFromRegistry*¥InocIT.exe
   - *FilePathFromRegistry*¥ShellScn.exe

   これは、応答ファイルに定義されているデフォルト アクションです。

2. 以下のレジストリ キーのエントリ値を読み取ります。

   HKLM¥SOFTWARE¥ComputerAssociates¥ScanEngine¥Path¥Engine

   エントリが値を返した場合は、プラグインは DCM タイプの以下の SPECIALPGM リソースを作成します。

   FilePathFromRegistry¥InoCmd32.exe

注: 応答ファイルは、規定ステージで共存ユーティリティが実行するデフォルト アクションを決定します（CA Access Control インストール前に実行すること、CA Access Control インストール後に実行することなど）。

Scout プラグインの機能

共存ユーティリティは、CA Access Control のインストールの最後およびユーティリティが実行されるたびに、以下のようにして Scout プラグインを実行して SurfControl Web フィルタで Windows レジストリ キーおよび実行ファイルについてコンピュータをスキャンします。

- 次のレジストリ キーの存在を照会します。

  HKLM¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥App Paths¥Scscout.Exe

  レジストリ キーが存在する場合、プラグインは以下のように動作します。

  - パス エントリの値を読み取ります。
  - 以下の実行可能ファイルのパス名を返します。

    FilePathFromRegistry¥scoutsvc.exe
  - タイプ DCM の SPECIALPGM リソースを作成します。

    これは、応答ファイルに定義されているデフォルト アクションです。

注: 応答ファイルは、規定ステージで共存ユーティリティが実行するデフォルト アクションを決定します（CA Access Control インストール前に実行すること、CA Access Control インストール後に実行することなど）。

Unicenter プラグインの概要

以下のように、CA Access Control インストールの最後とユーティリティの実行時に常に、共存ユーティリティが Unicenter プラグインを実行してコンピュータ内の CA Unicenter レジストリ キーおよび実行可能ファイルをスキャンします。

1. CAUENV.dll を使用して、CA Unicenter ディレクトリのパス（*UniPath*）を取得します。
2. 以下の DCM タイプの SPECIALPGM リソースを作成します。
   - *UniPath*¥Bin¥sfauditd.exe
   - *UniPath*¥Bin¥secdos2.exe
   - *UniPath*¥Bin¥caulgnd.exe
   - *UniPath*¥Bin¥sccommit.exe
   - *UniPath*¥Bin¥dsbulist.exe
   - *UniPath*¥Bin¥fmpost.exe
   - *UniPath*¥Bin¥catlbl.exe

- *UniPath*¥Bin¥caanal.exe
- *UniPath*¥Bin¥cascan.exe
- *UniPath*¥Bin¥causamd.exe
- *UniPath*¥Bin¥acbrows.exe
- *UniPath*¥Bin¥secadmin.exe
- *UniPath*¥Bin¥dsbufcrt.exe
- *UniPath*¥Bin¥cnvpwd.exe
- *UniPath*¥Bin¥fmeng.exe
- *UniPath*¥Bin¥fmmscan.exe
- *UniPath*¥Bin¥cadevscn.exe
- *UniPath*¥AGENTS¥Bin¥prfagent.exe
- *UniPath*¥AGENTS¥Bin¥msexchagnt.exe

注: 応答ファイルは、規定ステージで共存ユーティリティが実行するデフォルトアクションを決定します(CA Access Control インストール前に実行すること、CA Access Control インストール後に実行することなど)。

Asset Management プラグインの概要

以下のように、CA Access Control インストールの最後とユーティリティの実行時に常に、共存ユーティリティが Asset Management プラグインを実行してコンピュータ内の Unicenter サービスをスキャンします。

1. サービス「UAM の CA Unicenter NSM システム パフォーマンス エージェント」の実行可能ファイルのディレクトリ パス(*ServicePath*)を抽出します。
2. 次の REGISTRY タイプの SPECIALPGM リソースを作成します。

   ServicePath¥agents¥bin¥hpacbcol.exe
3. サービス「caf」の実行可能ファイルのディレクトリ パス(*ServicePath*)を抽出します。
4. 次の REGISTRY タイプの SPECIALPGM リソースを作成します。
   ServicePath¥PMAgent¥agents¥bin¥hpacbcol.exe

また、以下のように、CA Access Control インストールの最後とユーティリティの実行時に常に、共存ユーティリティが Asset Management プラグインを実行してコンピュータ内の Unicenter Asset Management バージョン 4 サービスをスキャンします。

1. サービス「UAM の CA Unicenter NSM システム パフォーマンス エージェント」の実行可能ファイルのディレクトリ パス(*ServicePath*)を抽出します。
2. 次の REGISTRY タイプの SPECIALPGM リソースを作成します。

   ServicePath¥agents¥bin¥hpacbcol.exe

また、以下のように、CA Access Control インストールの最後とユーティリティの実行時に常に、共存ユーティリティが Asset Management プラグインを実行してコンピュータ内の Unicenter DSM r11 サービスをスキャンします。

1. サービス「caf」の実行可能ファイルのディレクトリ パス(*ServicePath*)を抽出します。
2. 次の REGISTRY タイプの SPECIALPGM リソースを作成します。

   ServicePath¥PMAgent¥agents¥bin¥hpacbcol.exe

注: 応答ファイルは、規定ステージで共存ユーティリティが実行するデフォルトアクションを決定します(CA Access Control インストール前に実行すること、CA Access Control インストール後に実行することなど)。

Windows プラグインの概要

以下のように、CA Access Control インストールの最後とユーティリティの実行時に常に、共存ユーティリティが Windows プラグインを実行してコンピュータ内の Windows サービスおよびレジストリ キーをスキャンします。

1. サービス「WinMgmt」の実行可能ファイルのディレクトリ パス(*ServicePath*)を抽出します。
2. 次の REGISTRY タイプの SPECIALPGM リソースを作成します。

   ServicePath

   これは、応答ファイルに定義されているデフォルト アクションです。
3. 次の PBF タイプの SPECIALPGM リソースを作成します。

   %windir%¥System32¥cidaemon.exe

   これは、応答ファイルに定義されているデフォルト アクションです。

注: 応答ファイルは、規定ステージで共存ユーティリティが実行するデフォルト アクションを決定します(CA Access Control インストール前に実行すること、CA Access Control インストール後に実行することなど)。

eTrust Audit プラグインの概要

以下のように、CA Access Control インストールの開始前に、共存ユーティリティが eTrust Audit プラグインを実行してコンピュータ内の eTrust Audit バージョン 1.5 レジストリ キーおよびファイルをスキャンします。

1. 次のレジストリ キーの存在を照会します。

   HKLM¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥App Paths¥acdistagn.exe

   成功すると、「パス」値指定の %PathFromRegistry% が抽出されます。

   レジストリ キーが存在する場合、プラグインは以下のように動作します。

   - パス エントリの値を読み取ります。
   - 次の実行可能ファイル パス名を返します。

     FilePathFromRegistry¥bin¥acactmgr.exe
     FilePathFromRegistry¥bin¥SeLogRcd.exe
     FilePathFromRegistry¥bin¥acdistagn.exe
     FilePathFromRegistry¥acdistsrv.exe
     FilePathFromRegistry¥acfwrecd.exe
     FilePathFromRegistry¥acrecorderd.exe
     FilePathFromRegistry¥aclogrd.exe
     FilePathFromRegistry¥portmap.exe

FilePathFromRegistry¥SeLogRec.exe
FilePathFromRegistry¥SeLogRd.exe
FilePathFromRegistry¥snmprec.exe

これは、応答ファイルに定義されているデフォルト アクションです。eTrust Audit プラグインは、信頼できるプログラム（SPECIALPGM）ルールをデフォルトでは追加しません。

2. 以下のサービスを停止します。
   - 「eAudit アクション マネージャ」
   - 「eAudit 配布エージェント」
   - 「eAudit ログ ルータ」
   - 「eAudit レコーダ」
   - 「eAudit リダイレクタ」
   - 「eAudit ポートマップ」

   より新しいバージョンの eTrust Audit インストールされている場合、以下のサービスを停止します。
   - 「eTrust Audit アクション マネージャ」
   - 「eTrust Audit コレクタ」
   - 「eTrust Audit 配布エージェント」
   - 「eTrust Audit 配布サーバ」
   - 「eTrust Audit FW-1 レコーダ」
   - 「eTrust Audit 汎用レコーダ」
   - 「eTrust Audit ログ ルータ」
   - 「eTrust Audit ポートマップ」
   - 「eTrust Audit レコーダ」
   - 「eTrust Audit リダイレクタ」
   - 「eTrust Audit SNMP レコーダ」
3. CA Access Control インストールが完了すると、これらの同じサービスが再起動されます。

また、共存ユーティリティが eTrust Audit プラグインを実行して以下を実行します。

- CA Access Control をアンインストールすると eTrust Audit サービスを停止します。
- CA Access Control アンインストール完了後に eTrust Audit サービスを開始します。

注: 応答ファイルは、規定ステージで共存ユーティリティが実行するデフォルトアクションを決定します（CA Access Control インストール前に実行すること、CA Access Control インストール後に実行することなど）。

eTrust Audit80 プラグインの概要

以下のように、CA Access Control インストールの最後とユーティリティの実行時に常に、共存ユーティリティが eTrust Audit80 プラグインを実行してコンピュータ内の eTrust Audit r8 レジストリ キーおよびファイルをスキャンします。

- 次のレジストリ キーの存在を照会します。

  HKLM¥SOFTWARE¥ComputerAssociates¥eTrust Audit¥Paths

  成功すると、「パス」値指定の %PathFromRegistry% が抽出されます。

  レジストリ キーが存在する場合、プラグインは以下のように動作します。

  - RootPath エントリの値を読み取ります。
  - 以下の DCM タイプの SPECIALPGM リソースを作成します。

    FilePathFromRegistry¥bin¥acactmgr.exe
    FilePathFromRegistry¥bin¥SeLogRcd.exe
    FilePathFromRegistry¥bin¥acdistagn.exe
    FilePathFromRegistry¥acdistsrv.exe
    FilePathFromRegistry¥acfwrecd.exe
    FilePathFromRegistry¥acrecorderd.exe
    FilePathFromRegistry¥aclogrd.exe
    FilePathFromRegistry¥portmap.exe
    FilePathFromRegistry¥SeLogRec.exe
    FilePathFromRegistry¥SeLogRd.exe
    FilePathFromRegistry¥snmprec.exe

    これは、応答ファイルに定義されているデフォルト アクションです。

注: 応答ファイルは、規定ステージで共存ユーティリティが実行するデフォルトアクションを決定します（CA Access Control インストール前に実行すること、CA Access Control インストール後に実行することなど）。

F-Secure Antivirus プラグインの概要

以下のように、共存ユーティリティが F-Secure Antivirus プラグインを実行してコンピュータ内の F-Secure Anti-Virus レジストリ キーおよびファイルをスキャンします。

- CA Access Control インストールの開始前に、プラグインは F-Secure Anti-Virus サービスを停止します。
- CA Access Control インストールが完了すると、プラグインは次のレジストリ キーの存在を照会します。

  HKLM¥SOFTWARE¥Data Fellows¥F-Secure¥Anti-Virus

  成功すると、「パス」値指定の %PathFromRegistry% が抽出されます。

  レジストリ キーが存在する場合、プラグインは以下のように動作します。

  - パス エントリの値を読み取ります。
  - 以下の DCM タイプの SPECIALPGM リソースを作成します。

    FilePathFromRegistry¥fssm32.exe
    FilePathFromRegistry¥fsgk32st.exe

    これは、応答ファイルに定義されているデフォルト アクションです。eTrust Audit プラグインは、信頼できるプログラム（SPECIALPGM）ルールをデフォルトでは追加しません。
- 共存ユーティリティが実行される場合は常に、プラグインが以下を実行します。

  a. F-Secure Anti-Virus サービスを停止します。

  b. CA Access Control インストールが完了したときに作成される SPECIALPGM リソース（このトピックで既述）と同じリソースを作成します。

  c. F-Secure Anti-Virus サービスを再起動します。

注: 応答ファイルは、規定ステージで共存ユーティリティが実行するデフォルト アクションを決定します（CA Access Control インストール前に実行すること、CA Access Control インストール後に実行することなど）。

McAfee VirusScan プラグインの概要

以下のように、CA Access Control インストールの最後とユーティリティの実行時に常に、共存ユーティリティが McAfee VirusScan プラグインを実行してコンピュータ内の McAfee VirusScan サービスをスキャンします。

1. サービス「McShield」の実行可能ファイルのディレクトリ パス(*ServicePath*)を抽出します。
2. 次の DCM タイプの SPECIALPGM リソースを作成します。

   ServicePath

   これは、応答ファイルに定義されているデフォルト アクションです。

注: 応答ファイルは、規定ステージで共存ユーティリティが実行するデフォルト アクションを決定します(CA Access Control インストール前に実行すること、CA Access Control インストール後に実行することなど)。

Windows Modules Installer プラグインの概要

以下のように、CA Access Control インストールの最後とユーティリティの実行時に常に、共存ユーティリティが Windows Modules Installer プラグインを実行してコンピュータ内の Windows Modules Installer サービスをスキャンします。

1. サービス「TrusterInstaller」の実行可能ファイルのディレクトリ パス(*ServicePath*)を抽出します。
2. 次の PBF タイプの SPECIALPGM リソースを作成します。

   ServicePath

   これは、応答ファイルに定義されているデフォルト アクションです。

注: 応答ファイルは、規定ステージで共存ユーティリティが実行するデフォルト アクションを決定します(CA Access Control インストール前に実行すること、CA Access Control インストール後に実行することなど)。

Services and Controller プラグインの概要

以下のように、CA Access Control インストールの最後とユーティリティの実行時に常に、共存ユーティリティが Services and Controller プラグインを実行してコンピュータ内の Windows サービス管理実行可能ファイルをスキャンします。

1. オペレーティング システムのバージョンが Windows Vista 以降であるかを確認します。

   OS が Windows それ以前のバージョンであれば、プラグインは終了します。

2. 次の KILL タイプの SPECIALPGM リソースを作成します。

   ```
   %windir%¥system32¥services.exe
   ```

   これは、応答ファイルに定義されているデフォルト アクションです。

注: 応答ファイルは、規定ステージで共存ユーティリティが実行するデフォルトアクションを決定します（CA Access Control インストール前に実行すること、CA Access Control インストール後に実行することなど）。

リソース ホスティング サブシステム プラグインのしくみ

CA Access Control のインストール プロセスは、CA Access Control のインストール中にリソース ホスティング サブシステム プラグインを実行します。また、共存ユーティリティは、顧客がその共存ユーティリティを実行しているときにリソース ホスティング サブシステムを実行します。リソース ホスティング サブシステム プラグインは以下のように、コンピュータでクラスタ サービス エレメントをスキャンします。

1. オペレーティング システムのバージョンが Windows Server 2008 以降であるかを確認します。

   OS が Windows それ以前のバージョンであれば、プラグインは終了します。

2. クラスタ サービス エレメントがコンピュータにインストールされているかどうかを確認します。

   クラスタ サービス エレメントがインストールされていない場合、プラグインは終了します。

3. 次の PBF タイプの SPECIALPGM リソースを作成します。

   ```
   system_drive:¥Windows¥Cluster¥rhs.exe
   ```

注: 応答ファイルは、規定ステージで共存ユーティリティが実行するデフォルトアクションを決定します（CA Access Control インストール前に実行すること、CA Access Control インストール後に実行することなど）。

response.ini - 共存ユーティリティの設定

Windows で該当

応答ファイルは、共存ユーティリティ（eACoexist）が実行されるときに実行するべきアクションを共存ユーティリティに指示します。応答ファイルには、共存ユーティリティが実行するすべてのプラグインのアクションに関する事前定義のセットが含まれています。応答ファイルを編集して、デフォルトのプラグイン アクションを変更できます。

注: 応答ファイルのパス名は SeOSD セクションの ResponseFile 構成設定で指定します。デフォルトでは、このファイルは *ACInstallDir*¥Data¥response.ini です。

このファイルの形式は以下のとおりです。

```
[セクション名]
Act-段階-#=Action
...
```

セクション名

共存プラグインに一致するセクションの名前を定義します。

共存ユーティリティは、このセクションで定義されるアクションに従ってプラグインを実行します。

Act-*Stage-#=アクション#*

規定ステージでプラグインが実行するアクションを定義します。

段階

以下のように、プラグインがアクションを実行する規定ステージを指定します。

- **BeginInstall** - CA Access Control がインストールを開始する前に、プラグインが指定アクションを実行します。
- **EndInstall** - CA Access Control インストールが完了した後に、プラグインが指定アクションを実行します。
- **Utility** - 共存ユーティリティを実行すると、プラグインが指定アクションを実行します。
- **BeginUninstall** - CA Access Control がアンインストールを開始する前に、プラグインが指定アクションを実行します。
- **EndUninstall** - CA Access Control アンインストールが完了した後に、プラグインが指定アクションを実行します。

#

プラグインがステージでアクションを実行する順序を指定します。

Action

以下のように、プラグインが実行するアクションを定義する番号を指定します。

- **1** - 検出された製品と CA Access Control に互換性がないことを警告します。
- **2** - CA Access Control インストール時にサービスを停止します。
- **3** - サービスを停止します。
- **4** - サービスを開始します。
- **5** - SPECIALPGM ルールを作成します。
- **6** - CA Access Control アンインストール時にサービスを停止します。

例: Dr. Watson プラグインのアクション

Dr. Watson プログラムがコンピュータで 検出された場合にデフォルトで Dr. Watson 共存プラグインが実行するデフォルト アクションについて、以下に例を示します。

```
[DrWatson]
Act-EndInstall-0=5
Act-Utility-0=5
```

このセクションでは、CA Access Control インストール完了後にプラグインが実行されると、プログラムの SPECIALPGM ルールが作成されることを示します。ユーティリティを実行したときに、同じアクションが実行されることも示しています。

eACSigUpdate ユーティリティ - STOP シグネチャ ファイルの置換

Windows で該当

eACSigUpdate ユーティリティは、ローカルの STOP（Stack Overflow Protection）シグネチャ ファイルを別のコンピュータで更新したファイルで置き換えます。

注: シグネチャ ファイルのブローカまたは親 Policy Model が定義されている場合、eACSigUpdate ユーティリティは、CA Access Control の起動時を初回としてそれ以降は定期的に、自動的に実行されます。

このコマンドの形式は以下のようになります。

```
eACSigUpdate hostname target_file
```

hostname

このコンピュータにコピーする、更新済みの STOP シグネチャ ファイルがあるホスト コンピュータの名前を指定します。

注:このコマンドが正常に機能するには、リモート ホストに対する管理者権限が必要です。

target_file

新しいシグネチャ ファイルの完全パスおよびファイル名を指定します。指定したホストから取得されたシグネチャの場所および名前です。

eACSyncLockout ユーティリティ - アカウントのロックアウトの同期化

Windows で該当

eACSyncLockout は、アカウントのロックアウトを CA Access Control データベースと同期させるユーティリティです（つまり、アカウントがロックアウトされると、CA Access Control データベースにある対応するユーザのレコードが保留されます）。このユーティリティは、パスワードの同期が有効で、かつユーティリティを実行しているユーザに ADMIN プロパティがある場合にのみ有効です。

このコマンドの形式は以下のようになります。

```
eACSyncLockout -start [-u username] [-p password]
```

```
eACSyncLockout -stop|-remove|-debug
```

-p *password*

インストールおよび起動されるサービスのユーザ パスワードを指定します。-p を指定しない場合、ユーザにパスワードがないとみなされます。

-削除

サービスが停止され、アンインストールされます（次回のコンピュータ起動時には、このサービスはサービス コントロール マネージャに表示されません）。

-start

サービスがインストールされ、起動されます。-u を指定しない場合、現在のユーザ コンテキストでサービスがインストールおよび起動されます。

-stop

サービスを停止します。

-u *user*

サービスをインストールおよび起動するユーザ コンテキストを指定します。

exporttngdb ユーティリティ - Unicenter セキュリティ データの移行

exporttngdb は、現在の Unicenter セキュリティのデータをローカルの CA Access Control データベースまたは PMDB に移行するプログラムです。

注: UNIX では、このプログラムは uni_migrate_master.sh および uni_migrate_node.sh という 2 つのスクリプトによって自動的に実行されます。マスタ コンピュータで両方のスクリプトが実行された場合は、最初に uni_migrate_master.sh スクリプトによってプログラムが呼び出され、グローバルな Unicenter セキュリティのデータがグローバル PMDB に移行されます。uni_migrate_node.sh スクリプトによってプログラムが呼び出されると、ローカル Unicenter セキュリティのデータがローカル CA Access Control データベースに移行されます。

このコマンドの形式は以下のようになります。

```
exporttngdb
```

issec ユーティリティ - CA Access Control デーモンのステータスの表示

UNIX で有効

issec ユーティリティは、CA Access Control のセキュリティ デーモンのステータスを表示します。どのオプションも指定しない場合は、以下の情報が表示されます。

- CA Access Control のバージョンおよびインストール ディレクトリ
- CA Access Control のカーネル拡張機能のステータス
- CA Access Control の 3 つの主要なデーモン（seosd、Agent、および Watchdog）のステータス
- CA Access Control デーモンのステータス: serevu、selogrd、selogrcd、eacws、ReportAgent、policyfetcher、KBLAudMgr
- PMDB デーモンのステータスおよびそのデーモンの名前
- seos.ini の [daemons] セクションに指定されているデーモンのステータス

このコマンドの形式は以下のようになります。

```
issec [-b] [-k] [-h]
```

-b

主要なデーモン（seosd、Agent、および Watchdog）のステータスおよび PID を表示します。

-k

CA Access Control のカーネル拡張機能がロードされているかどうかを確認します。

-h

このユーティリティのヘルプ画面を表示します。

ldap2seos スクリプト - ユーザの LDAP からの抽出と CA Access Control への追加

UNIX で該当

ldap2seos ユーティリティは、サーバ ホストにある LDAP データベースからユーザを抽出して、CA Access Control データベースに追加します。

重要: CA Access Control では、LDAP ユーザ ストアがオペレーティング システムによって使用される場合（つまり、エンタープライズ ユーザ ストアの場合）、LDAP ユーザをインポートせずに直接使用できます。ldap2seos ユーティリティの代わりに、CA Access Control のこの機能を使用することも検討してください。

ldap2seos ユーティリティを実行すると、定義されたユーザに関する情報が LDAP サーバから抽出されます。抽出された情報を使用して、データベースにユーザを追加する selang のコマンドが自動的に実行されます。生成されたコマンドは標準出力にも記録され、/tmp/ldap2seos.tcl.log というファイルに自動的に保存されます。

このユーティリティでは TCL シェル環境にアクセスする必要があります。ldap2seos スクリプトでは、TCL シェルのパスが /usr/local/bin/tclsh であるとみなされます。TCL シェルが他の場所にある場合は、スクリプトの最初の行を変更します。

このユーティリティが正常に機能するには、CA Access Control が実行されている必要があります。このユーティリティはデータベースを更新するため、ADMIN 権限を持つユーザが実行する必要があります。また、このユーザは LDAP データベース設定で検索クエリの実行が許可されている必要があります。

このスクリプトの構文は以下のとおりです。

```
ldap2seos [options]
```

-accfld *account-field*

CA Access Control のユーザ ID が格納されている LDAP フィールド名を指定します。

UNIX ユーザ ID が LDAP ユーザ ID フィールド内に指定されている場合、このオプションは不要です。

UNIX ユーザ ID がユーザ ID フィールド以外の LDAP フィールドに割り当てられている場合は、その LDAP フィールドを *account-field* として指定します。このように指定すると、LDAP ユーザ ID フィールドは無視されます。

注: このスクリプトでユーザ ID を検出できない場合、ユーザは CA Access Control データベースにアップロードされません。

-b *base-entry*

ユーザが抽出される LDAP データベースの基本エントリを指定します。このエントリは、LDAP データベース内で有効である必要があります。基本エントリを省略した場合は、デフォルトの基本エントリを使用してユーザが抽出されます。

-d *dn*

-w スイッチを使用し、別のユーザとして LDAP への認証を行う際に使用されるエントリ名を指定します。これが最も必要になるのは、ADMIN ユーザとして LDAP にログインする場合です。

-f *filename*

LDAP サーバから取得したデータを一時的に格納するファイルを指定します。

-h

このユーティリティのヘルプを表示します。ヘルプ画面には seos2ldap の使用法およびオプションの一覧と説明が表示されます。

-h *ldap-host*

LDAP データベースが格納されているホストの名前を指定します。デフォルトは、ローカル ホストです。

-l *ldap-dir*

bin サブディレクトリにあると想定される、ライン コマンド ユーティリティが格納されているディレクトリを指定します。デフォルトでは /usr/local/ldap です。

-p *port*

LDAP で接続に使用されるポートを指定します。デフォルトでは 389 です。

-u

-h と同様にヘルプを表示します。ヘルプ画面には seos2ldap の使用法およびオプションの一覧と説明が表示されます。

-w *bindpasswd*

ユーザ パスワードを指定します。LDAP データベースにアクセスするために認証が必要な場合には、-d オプションと共に使用します。

例: ユーザ情報の抽出

以下のコマンドは、ホスト myhost.mysite.com にある LDAP データベースからユーザに関する情報を抽出し、その情報を CA Access Control データベースに追加します。

```
ldap2seos -h myhost.mysite.com
```

seos2ldap スクリプト - CA Access Control ユーザの LDAP へのエクスポート

seos2ldap は、CA Access Control のユーザをデータベースからサーバ ホストにある LDAP データベースにエクスポートします。CA Access Control データベースからユーザに関する適切な情報を抽出します。抽出された情報は、選択されたサーバの LDAP データベースに送信されます。抽出された情報を使用して、LDIF ファイルが生成されます。指定されたユーザが LDAP データベースに追加されます。応答は、自動的に /tmp/seos2ldap.tcl.log というファイルに保存されます。

このユーティリティでは TCL シェル環境にアクセスする必要があります。seos2ldap では、TCL シェルのパスが /usr/local/bin/tclsh であるとみなされます。TCL シェルが他の場所にある場合は、スクリプトの最初の行を変更します。

このユーティリティが正常に機能するには、CA Access Control が実行されている必要があります。このユーティリティはデータベースの読み取りを行うため、ADMIN 権限を持つユーザが実行する必要があります。また、このユーザは、LDAP データベース設定で変更が許可されている必要があります。

LDAP データベースのエントリ スキーマ(使用する場合)は、Netscape サーバのスキーマと同じにする必要があります。Netscape のスキーマを変更している場合、または別の種類の LDAP サーバを使用している場合は、seos2ldap サンプル スクリプトを適宜編集する必要があります。

CA Access Control データベース ユーザが LDAP データベースにすでに入力されている場合、ユーザは追加されません。 エラー メッセージが生成されますが、エクスポート プロセスは続行されます。

このスクリプトの構文は以下のとおりです。

```
seos2ldap [options]
```

-b *base-entry*

ユーザ情報を格納する、LDAP データベースの基本エントリを指定します。このエントリは、LDAP データベース内で有効である必要があります。基本エントリを省略した場合は、この入力が求められます。

-d *dn*

-w スイッチを使用し、別のユーザとして LDAP への認証を行う際に使用されるエントリ名を指定します。このオプションは、admin ユーザとして LDAP にログインするために必要です。

-f *filename*

LDAP サーバから取得したデータを一時的に格納するファイルを指定します。

-h

このユーティリティのヘルプを表示します。ヘルプ画面には seos2ldap の使用法およびオプションの一覧と説明が表示されます。

-h *ldap-host*

LDAP データベースが格納されているホストの名前を指定します。デフォルトは、ローカル ホストです。

-l *ldap-dir*

bin サブディレクトリにあると想定される、ライン コマンド ユーティリティが格納されているディレクトリを指定します。デフォルトでは /usr/local/ldap です。

-noprompt

基本エントリのプロンプトを表示しません。基本 LDAP エントリを指定するために -b *base-entry* フラグを使用しなかった場合、デフォルトでは基本エントリの入力を促す seos2ldap のプロンプトが表示されます。このフラグを使用すると、プロンプトは表示されません。

-p *port*

LDAP で接続に使用されるポートを定義します。デフォルトでは 389 です。

-u

-h と同様にヘルプを表示します。ヘルプ画面には seos2ldap の使用法およびオプションの一覧と説明が表示されます。

-w *bindpasswd*

ユーザ パスワードを定義します。LDAP データベースにアクセスするために認証が必要な場合には、-d オプションと共に使用します。

例: ユーザ情報のエクスポート

以下のコマンドは、CA Access Control データベースからユーザに関する情報を抽出し、SeOS_user_dump という LDIF ファイルを作成します。このコマンドは、ホスト myhost.mysite.com にある LDAP データベースにレコードを追加します。後から LDIF ファイルを編集して LDAP を手動で更新できます。

```
seos2ldap -h myhost.mysite.com
```

migopts ユーティリティ - Unicenter セキュリティ設定の変換

migopts ユーティリティは、現在の Unicenter セキュリティの環境設定をローカルの CA Access Control データベースまたは PMDB のいずれかのグローバル設定に変換します。

注: インストール プログラムで[Unicenter 統合]を選択すると、このスクリプトが自動的に実行されます。新しい PMDB の作成時には、このスクリプトを必ず手動で実行する必要があります。

このコマンドの形式は以下のようになります。

```
migopts [options]
```

-d *pmdName*

selang の任意のコマンドを実行して、インポートした PMDB(デフォルトのローカル CA Access Control データベースではなく)を更新する前に、CA Access Control **hosts** コマンドを発行します。

-f *fileName*

実行可能なスクリプト ファイルに対して **selang -c** コマンドを生成します。

-l *logfileName*

絶対パスで指定されたファイルにログ メッセージを記録します。

ntimport ユーティリティ - Windows ユーザおよびグループのインポート

Windows で該当

ntimport ユーティリティは、Windows のユーザおよびグループを Windows オペレーティング システム データベースから取り出し、ローカル データベースにインポートします。このユーティリティを使用すると、ユーザおよびグループをローカルの CA Access Control データベースに追加する Windows コマンドが作成されます。

重要: CA Access Control では、Windows ユーザおよびグループをデータベースにインポートせずに、直接使用できます。ntimport ユーティリティの代わりに、CA Access Control のこの機能を使用することを検討してください。ntimport ユーティリティは、CA Access Control で Windows ユーザおよびグループを直接使用できるようになる前に開発されたものです。

生成されたコマンドは標準出力に表示されます。selang ユーティリティへの入力として使用するファイルを作成する場合は、-f オプションを使用します。

このコマンドの形式は以下のようになります。

```
ntimport {-a|{[-u] [-g] [-c]}} [-d] [-U] ¥
    [-D] [-f filename] [-o owner] [-p pmdb] ¥
    [-pa pmdb] [-r remote-host] [-v]
```

--a

-c、-g、および -u スイッチのすべてのアクションを実行します。

-c

デフォルトのグループにユーザを追加する selang のコマンドを生成します。

-d

ドメインをプレフィクスとしてユーザおよびグループをインポートします。

-D

使用可能な最初のドメイン コントローラからユーザおよびグループの情報を取得します。

-f *filename*

指定されたファイルに出力します。

--g

Windows からローカル データベースにグループをインポートする selang のコマンドを生成します。

-o *owner*

インポートした各レコードに所有者権限ルールを設定します。*Administrator* が自動的にすべてのレコードの所有者として設定されないようにするには、このフラグを使用します。*Owner* には、ntimport で定義したすべてのレコードの所有者権限の割り当て対象となるユーザまたはグループの名前を指定します。

-p *pmdb*

ユーザおよびグループを pmdb の AC 環境にインポートするコマンドを生成します。

-pa *pmdb*

ユーザおよびグループを pmdb の AC 環境およびネイティブ環境の両方にインポートするコマンドを生成します。

-pn *pmdb*

ユーザおよびグループを pmdb のネイティブ環境にインポートするコマンドを生成します。

-r *remote-host*

指定されたリモート ホストからユーザおよびグループの情報を取得します。

-u

Windows データベースからローカル データベースにユーザをインポートする selang のコマンドを生成します。名前の 40 文字を超える部分は切り捨てられます。

-U

ユーザの Surrogate ルールのインポートに必要な selang のコマンドを生成します。

-v

進行状況に関する情報を表示します。ユーザまたはグループが多数存在する環境でプログラムの進行状況を確認するには、このフラグを使用します。

policydeploy ユーティリティ - エンタープライズ ポリシーのデプロイの管理

policydeploy ユーティリティは、複数ルールのポリシーを管理します（拡張ポリシー管理）。このユーティリティを使用すると、DMS ノードへのポリシー バージョンの格納、ホストおよびホスト グループへのポリシーの割り当てと割り当ての解除、格納されたポリシーの直接的なデプロイとデプロイの解除、またはデプロイされたポリシーの最新バージョンへのアップグレードを行うことができます。

このユーティリティはいくつかのタスクを処理します。以下の関数を使用します。

タスク	Function
ポリシーの割り当てまたは割り当て解除 (P. 90)	`policydeploy -assign`
ポリシーの削除 (P. 93)	`policydeploy -delete`
ポリシーの展開 (P. 95)	`policydeploy -deploy`
ポリシーの展開解除 (P. 95)	`policydeploy -undeploy`
展開タスクを再実行します。 (P. 97)	`policydeploy -fix`
展開スクリプトの表示 (P. 98)	`policydeploy -getrules`
ホスト グループにホストを追加するか削除します。 (P. 100)	`policydeploy -join`
拡張ポリシー管理への PMD の移行 (P. 101)	`policydeploy -migrate`
ポリシー展開のリセット (P. 104)	`policydeploy -reset`
すべてのポリシーのリストア (P. 105)	`policydeploy -restore`
ポリシーの格納 (P. 106)	`policydeploy -store`
ポリシー バージョンのアップグレード (P. 109)	`policydeploy -upgrade`
ポリシー バージョンのダウングレード (P. 109)	`policydeploy -downgrade`

policydeploy -assign 機能 - ポリシーの割り当てまたは割り当て解除

この機能では、指定されたポリシーを 1 つ以上のホストまたはホスト グループに対して割り当てまたは割り当て解除します。

この関数の構文は、以下のようになります。

```
policydeploy -assign[-] name -hnode|-ghnode list [-dms list]
```

-assign *name*

指定されたポリシーを 1 つ以上のホストまたはホスト グループに割り当てします。

-assign- *name*

指定されたポリシーを 1 つ以上のホストまたはホスト グループから割り当解除します。

-dms *list*

(オプション) 使用する DMS ノードのカンマ区切りリストを指定します。ポリシーをデプロイまたはデプロイ解除する場合、そのアクションは DMS ノードにレポートされます。ポリシーを格納すると、DMS ノードに格納されます。

このオプションで DMS ノードを指定しない場合、policydeploy ユーティリティでは、ローカル CA Access Control データベースで指定された DMS ノードのリストが使用されます。DMS ノードのリストをデータベースに指定するには、dmsmgr を使用して新しい DMS を作成した後に、以下の selang コマンドを発行する必要があります。

```
so dms+(new_dms_name)
```

注: インストール時に DMS ノードを指定しなかった場合、またはエンドポイント上の登録済み DMS を置換したり、エンドポイントに登録済み DMS を追加する場合は、このコマンドを発行する必要があります。ただし、拡張ポリシー管理サーバの作成をインストール時に指定した場合、DMS はデータベースに追加され、このコマンドを手動で実行する必要はありません。

-ghnode *list*

ポリシーを割り当てるホスト グループ (GHNODE オブジェクト) のカンマ区切りリストを定義します。

-hnode *list*

ポリシーを割り当てるホスト (HNODE オブジェクト) のカンマ区切りリストを定義します。

例: IIS 5 保護ポリシーの割り当て

次の例は、policydeploy ユーティリティを使用してインターネット インフォメーション サービス(IIS)5 サーバを保護するためのポリシーの割り当て方法を示します。ポリシーおよびポリシー IIS5 の最新の(4 番目)バージョンを確認し、IIS5Servers と呼ばれるホスト グループにポリシーを割り当てます。ポリシー IIS5 は crDMS@cr_host.company.com DMS ノードに格納されています。

1. selang を使用して次の DMS に接続します。

   ```
   hosts crDMS@cr_host.company.com
   ```

   これで、selang を使用して DMS のクエリを実行できます。

2. ポリシーの最新のファイナライズされたバージョンが不明な場合、以下の selang コマンドを発行してポリシーのすべてのバージョンを検出します。

   ```
   sr GPOLICY IIS5
   ```

   IIS5 ポリシーのプロパティが selang ウィンドウに一覧表示されます。たとえば、割り当て可能なポリシーの最新バージョン(ファイナライズ済み)である[最終ポリシー]などが表示されます。

3. 以下の selang コマンドを発行して、ポリシーデプロイおよびデプロイ解除スクリプトを表示します。

   ```
   sr RULESET IIS5#04
   ```

   selang ウィンドウに、IIS5 ポリシーの 4 番目のバージョンに関連するデプロイおよびデプロイ解除ルールを含む IIS5#04 RULESET オブジェクトが表示されます。

4. コマンド プロンプト ウィンドウで、policydeploy ユーティリティを実行します。

   ```
   policydeploy -assign IIS5 -ghnode IIS5Servers
   ```

   これにより、IIS5Servers 論理ホスト グループ内のすべてのホストに IIS5 ポリシーが割り当てられ、さらに、IIS5 ポリシーの 4 番目のバージョンがこれらのホストでデプロイされます。

例: IIS 5 保護ポリシーの割り当て解除

次の例は、以前の例で IIS 5 ポリシーを割り当てた Web サーバからそのポリシーを割り当て解除する方法について説明しています。

コマンド プロンプト ウィンドウで、policydeploy ユーティリティを実行します。

```
policydeploy -assign- IIS5 -ghnode IIS5Servers
```

これにより、IIS5Servers 論理ホスト グループ内のすべてのホストから IIS5 ポリシーが割り当て解除され、さらに、これらのホストにデプロイされている IIS5 ポリシーのバージョンがデプロイ解除されます。

policydeploy -delete 機能 - ポリシーの削除

この機能は、指定されたポリシーまたはポリシー バージョンを削除します。

注: 次のようなポリシーまたはポリシー バージョンは削除できません。ホストまたはホスト グループに割り当てられている、ホストまたはホスト グループ上にデプロイされている、デプロイ解除に失敗したステータスがある、DMS 上のステータスがある。ポリシーまたはポリシー バージョンは、すべてのホストおよびホスト グループから確実にデプロイ解除するか割り当て解除してから削除します。さらに、別のポリシーの前提条件であるポリシーは削除できません。ポリシーは、すべての依存関係を削除してから削除してください。

この関数の構文は、以下のようになります。

```
policydeploy -delete name[#xx] [-dms list]
```

-delete *name*[*#xx*]

指定されたポリシーまたはポリシー バージョンを削除します。

-dms *list*

(オプション) 使用する DMS ノードのカンマ区切りリストを指定します。ポリシーをデプロイまたはデプロイ解除する場合、そのアクションは DMS ノードにレポートされます。ポリシーを格納すると、DMS ノードに格納されます。

このオプションで DMS ノードを指定しない場合、policydeploy ユーティリティでは、ローカル CA Access Control データベースで指定された DMS ノードのリストが使用されます。DMS ノードのリストをデータベースに指定するには、dmsmgr を使用して新しい DMS を作成した後に、以下の selang コマンドを発行する必要があります。

```
so dms+(new_dms_name)
```

注: インストール時に DMS ノードを指定しなかった場合、またはエンドポイント上の登録済み DMS を置換したり、エンドポイントに登録済み DMS を追加する場合は、このコマンドを発行する必要があります。ただし、拡張ポリシー管理サーバの作成をインストール時に指定した場合、DMS はデータベースに追加され、このコマンドを手動で実行する必要はありません。

例: IIS 5 保護ポリシーの割り当て解除

次の例は、DMS から割り当て解除された IIS 5 ポリシーを削除する方法を示します。この例では、ポリシー IIS5 はいずれのホストまたはホスト グループにも割り当てられず、crDMS@cr_host.company.com DMS ノード上に格納されます。

IIS 5 保護ポリシーを削除するには、コマンド プロンプト ウィンドウを開き、policydeploy ユーティリティを実行します。

```
policydeploy -delete IIS5
```

ポリシー IIS5 は crDMS@cr_host.company.com DMS ノードから削除されています。

例: IIS 5 保護ポリシー バージョンの削除

以下の例は、DMS から割り当て解除されたポリシー バージョン IIS5#05 を削除する方法を示します。この例では、ポリシー バージョン IIS5#05 はどのホストまたはホスト グループにも割り当てられておらず、crDMS@cr_host.company.com DMS ノード上に格納されています。

IIS 5 保護ポリシー バージョンを削除し、コマンド プロンプト ウィンドウを開き、policydeploy ユーティリティを実行する場合:

```
policydeploy -delete IIS5#05
```

ポリシー バージョン IIS5#05 は crDMS@cr_host.company.com DMS ノードから削除されます。

policydeploy -deploy 機能 - ポリシーのデプロイまたはデプロイ解除

この機能は、ホストへのポリシー割り当てまたはホストからのポリシー割り当て解除なしで、指定されたエンドポイントに関するポリシーをデプロイまたはデプロイ解除します。

この関数の構文は、以下のようになります。

```
policydeploy { -deploy name[#xx] | -undeploy name[#xx] } {-nodelist hnode_list | -root dbs} [-dms list]
```

-deploy *name*[#*xx*]

指定されたポリシー バージョンを(ホストにポリシーを割り当てずに)定義されたエンドポイントに直接デプロイするかどうかを確認するメッセージを表示します。格納されている最新バージョンのポリシーをデプロイするには、ポリシー バージョン番号を省略します。

-dms *list*

(オプション)使用する DMS ノードのカンマ区切りリストを指定します。ポリシーをデプロイまたはデプロイ解除する場合、そのアクションは DMS ノードにレポートされます。ポリシーを格納すると、DMS ノードに格納されます。

このオプションで DMS ノードを指定しない場合、policydeploy ユーティリティでは、ローカル CA Access Control データベースで指定された DMS ノードのリストが使用されます。DMS ノードのリストをデータベースに指定するには、dmsmgr を使用して新しい DMS を作成した後に、以下の selang コマンドを発行する必要があります。

```
so dms+(new_dms_name)
```

注: インストール時に DMS ノードを指定しなかった場合、またはエンドポイント上の登録済み DMS を置換したり、エンドポイントに登録済み DMS を追加する場合は、このコマンドを発行する必要があります。ただし、拡張ポリシー管理サーバの作成をインストール時に指定した場合、DMS はデータベースに追加され、このコマンドを手動で実行する必要はありません。

-nodelist *hnode_list*

操作を実行するホスト(HNODE オブジェクト)のカンマ区切りリストを定義します。

-root *dbs*

ポリシーがデプロイまたはデプロイ解除されるデータベースのカンマ区切りリストを定義します。

注: ルート データベースが Policy Model の親である場合、サブスクライバ データベース全体でそのポリシーがデプロイまたはデプロイ解除されます。ルート データベースが CA Access Control エンドポイントである場合、ポリシーは指定されたデータベースでのみデプロイまたはデプロイ解除されます。このオプションは r8 SP1 データベースおよび PMDB との後方互換性のためのものです。

-undeploy *name*[*#xx*]

指定されたポリシー バージョン *name#xx* を(そのポリシーの割り当ては解除せずに)定義されたエンドポイントから直接デプロイ解除するかどうかを確認するメッセージを表示します。

格納されている最新バージョンのポリシーのデプロイを解除するには、ポリシー バージョン番号を省略します。

policydeploy -fix 機能 - デプロイ タスクの再実行

この機能は指定されたデプロイ タスクまたはパッケージを修正し、そのタスクまたはパッケージを再デプロイします。

この関数の構文は、以下のようになります。

```
policydeploy -fix {-task list|-package list} [-dms list]
```

-dms *list*

(オプション) 使用する DMS ノードのカンマ区切りリストを指定します。ポリシーをデプロイまたはデプロイ解除する場合、そのアクションは DMS ノードにレポートされます。ポリシーを格納すると、DMS ノードに格納されます。

このオプションで DMS ノードを指定しない場合、policydeploy ユーティリティでは、ローカル CA Access Control データベースで指定された DMS ノードのリストが使用されます。DMS ノードのリストをデータベースに指定するには、dmsmgr を使用して新しい DMS を作成した後に、以下の selang コマンドを発行する必要があります。

```
so dms+(new_dms_name)
```

注: インストール時に DMS ノードを指定しなかった場合、またはエンドポイント上の登録済み DMS を置換したり、エンドポイントに登録済み DMS を追加する場合は、このコマンドを発行する必要があります。ただし、拡張ポリシー管理サーバの作成をインストール時に指定した場合、DMS はデータベースに追加され、このコマンドを手動で実行する必要はありません。

-fix

指定されたデプロイ タスクまたはパッケージを修正および再デプロイします。

-package *list*

デプロイ パッケージ (GDEPLOYMENT) のカンマ区切りリストを定義します。

-task *list*

デプロイ タスクのカンマ区切りリストを定義します。

policydeploy -getrules 機能 - デプロイ スクリプトの表示

この機能では、指定されたポリシー バージョンに対する selang デプロイおよびデプロイ解除スクリプトを表示できます。

```
policydeploy -getrules name[#xx]> -ds file1 -uds file2 [-dms list]
```

-dms *list*

(オプション) 使用する DMS ノードのカンマ区切りリストを指定します。ポリシーをデプロイまたはデプロイ解除する場合、そのアクションは DMS ノードにレポートされます。ポリシーを格納すると、DMS ノードに格納されます。

このオプションで DMS ノードを指定しない場合、policydeploy ユーティリティでは、ローカル CA Access Control データベースで指定された DMS ノードのリストが使用されます。DMS ノードのリストをデータベースに指定するには、dmsmgr を使用して新しい DMS を作成した後に、以下の selang コマンドを発行する必要があります。

```
so dms+(new_dms_name)
```

注: インストール時に DMS ノードを指定しなかった場合、またはエンドポイント上の登録済み DMS を置換したり、エンドポイントに登録済み DMS を追加する場合は、このコマンドを発行する必要があります。ただし、拡張ポリシー管理サーバの作成をインストール時に指定した場合、DMS はデータベースに追加され、このコマンドを手動で実行する必要はありません。

-ds *file1*

デプロイ ルールを含むファイルのパス名を指定します。これらは、ポリシーを作成するために必要なコマンドです。-getrules オプションを使用すると、ユーティリティによってこのファイルが作成されます。

重要: ポリシーのデプロイでは、ユーザ パスワードを設定するコマンドはサポートされていません。そのようなコマンドをデプロイ スクリプト ファイルに含めないでください。ネイティブ selang コマンドはサポートされていますが、偏差レポートには示されません。

getrules *name*[#*xx*]

指定されたポリシー バージョンの selang デプロイ スクリプトおよびデプロイ解除スクリプトを取得します。ポリシー バージョンが指定されていない場合は、最新のポリシー バージョンに対してこのコマンドが適用されます。

-uds *file2*

ポリシーのデプロイ解除に必要なルールを含むファイルのパス名を定義します。これらは、ポリシーのデプロイを解除するために必要なコマンドです。-getrules オプションを使用すると、ユーティリティによってこのファイルが作成されます。

CA Access Control によってポリシーがデプロイ解除される場合に、ポリシーのデプロイ解除スクリプトが格納されていないと、CA Access Control によってポリシーの削除に必要なコマンドが算出されます。

例: IIS 5 保護ポリシーと関連付けられたデプロイ スクリプトの表示

次の例では、インターネット インフォメーション サービス(IIS)5 サーバを保護するためのポリシーをデプロイおよびデプロイ解除することに関連する selang スクリプトを表示する方法を示します。ポリシー名は myPolicy です。

selang スクリプトを表示するためには、以下のコマンドを実行します。

```
policydeploy -getrules myPolicy -ds c:¥folder¥deployRules.txt -uds undeployRules.txt
```

policydeploy -join 機能 - ホストをホスト グループに対して結合ないし削除

この機能は、ホスト グループにホストを結合するか、またはホスト グループからホストを削除します。

この関数の構文は、以下のようになります。

```
policydeploy -join[-] hnode_name -ghnode name [-dms list]
```

-dms *list*

(オプション) 使用する DMS ノードのカンマ区切りリストを指定します。ポリシーをデプロイまたはデプロイ解除する場合、そのアクションは DMS ノードにレポートされます。ポリシーを格納すると、DMS ノードに格納されます。

このオプションで DMS ノードを指定しない場合、policydeploy ユーティリティでは、ローカル CA Access Control データベースで指定された DMS ノードのリストが使用されます。DMS ノードのリストをデータベースに指定するには、dmsmgr を使用して新しい DMS を作成した後に、以下の selang コマンドを発行する必要があります。

```
so dms+(new_dms_name)
```

注: インストール時に DMS ノードを指定しなかった場合、またはエンドポイント上の登録済み DMS を置換したり、エンドポイントに登録済み DMS を追加する場合は、このコマンドを発行する必要があります。ただし、拡張ポリシー管理サーバの作成をインストール時に指定した場合、DMS はデータベースに追加され、このコマンドを手動で実行する必要はありません。

-ghnode *name*

実行する操作のホスト グループの名前を定義します。

-join *hnode_name*

ホスト グループに指定されたホストを追加します。

-join *hnode_name*

ホスト グループから指定のホストを削除します。

policydeploy -migrate 機能 - PMD から拡張ポリシー管理への移行

この機能では、拡張ポリシー管理環境へ PMD を移行します。拡張ポリシー管理へ PMD を移行する場合、PMD のルールからポリシーを作成し、DMS にホストグループおよび ホストを作成し、さらにポリシーをホスト グループに割り当てます。

この関数の構文は、以下のようになります。

```
policydeploy -migrate pmdName@hostName [-dms name] [-policydir directory] ¥
[-exportfilter "class, class..."] [-hgcreate] [-pcreate name] [-addpmdfilter]¥
[-unsubs] [-delete] [-auto]
```

pmdName@hostName

移行する PMD の名前を定義します。

-dms *name*

（オプション）PMD のルールが移行される DMS 名を定義します。 特に DMS 名を指定しない場合、DMS 名はローカル ホスト上の CA Access Control データベースから検索されます。

注: ここで特に DMS 名を指定せず、ローカル ホスト上の CA Access Control データベースの中で 1 つ以上の DMS 名が指定されている場合、PMD のルールはすべての指定された DMS に移行されます。

-policydir *directory*

（オプション）ポリシー ファイルが格納されているディレクトリを定義します。特にディレクトリを指定しない場合、このポリシー ファイルはユーザの現在の作業ディレクトリに格納されます。

ポリシー ファイルの名前は *pmdName_hostName*_policy です。

-exportfilter "*class*, *class*..."

（オプション）PMD データベースからエクスポートする CA Access Control クラスを指定します。特にクラスを指定しない場合、PMD データベース中のクラスがすべてエクスポートされます。

次のポイントが -exportfilter パラメータに適用されます。

- 特定のクラスのリソースを変更するルールをエクスポートし、そのクラスに対応するリソース グループが含まれる場合、CA Access Control はそのリソース グループに存在するリソースを変更するルールもエクスポートします。

- 特定のリソース グループのリソースを変更するルールをエクスポートする場合、CA Access Control はそのリソース グループのメンバ リソースを変更するルールもエクスポートします。
- 特定のクラスのリソースを変更するルールをエクスポートし、そのクラスに PACL が含まれる場合、CA Access Control は PROGRAM クラスに存在するリソースを変更するルールもエクスポートします。
- 特定のクラスのリソースを変更するルールをエクスポートし、そのクラスに CALACL が含まれる場合、CA Access Control は CALENDAR クラスに存在するリソースを変更するルールもエクスポートします。
- 特定のクラスのリソースを変更するルールをエクスポートし、そのクラスのリソースの 1 つが CONTAINER リソースグループのメンバである場合、CA Access Control は CONTAINER クラスのリソースを変更するルール、および各 CONTAINER リソース ループのメンバとなっているリソースを変更するルールをエクスポートします。

- hgcreate

(オプション) *pmdName* に対応するホスト グループ (GHNODE オブジェクト) を DMS 上に作成、また *pmdName* のエンドポイント サブスクライバに対応するホスト (HNODE オブジェクト) を DMS 上に作成、またホスト グループへホストを結合します。

-pcreate *name*

(オプション) DMS 上に *pmdName* からエクスポートされたポリシー ファイルのルールを含む POLICY オブジェクトを作成し、*pmdName* に対応する DMS 上のホスト グループへ、その POLICY オブジェクトを割り当てます。*名前*を指定すれば、作成された POLICY オブジェクトは指定された名前を name 部分につけて *name*_POLICY#01 と命名されます ; 名前を指定しなければ、作成された POLICY オブジェクトは *pmdName*_POLICY#01 と命名されます。

- addpmdfilter

(オプション) *pmdName* へのフィルタ ファイルの適用。フィルタ ファイルは filter.flt と命名され、*pmdName* と同じディレクトリに位置します。

注: フィルタ ファイルを使用して、パスワード PMD を作成します。フィルタ ファイルは *pmdName* のサブスクライバに対して、ユーザ パスワード コマンドのみを送信します。

-unsubs

(オプション) *pmdName* からエンドポイント サブスクライバをサブスクライブ解除します。

-delete

（オプション）policydeploy -migrate 機能の実行完了後に *pmdName* を削除します。

-auto

（オプション）-hgcreate および -pcreate オプションの両方を実行するように指定します。このオプションでは、以下のことを行います。

- pmdName のルールをエクスポートします。
- *pmdName* に対応する DMS 上のホスト グループ（GHNODE オブジェクト）を作成します。
- *pmdName* のエンドポイント サブスクライバに対応する DMS 上のホスト（HNODE オブジェクト）を作成します。
- ホスト グループにホストを結合します。
- *pmdName* からエクスポートされたポリシー ファイルのルールを含んでいる POLICY オブジェクトを DMS 上に作成します。
- *pmdName* に対応する DMS 上のホスト グループに POLICY オブジェクトを帰します。

例: ルールの移行とホスト グループの作成

この例では、ホスト A 上の Master PMD からホスト B 上の DMS__ までルールを移行、ポリシー ファイルを C: ¥Data¥policies_MasterPMD_hostA ディレクトリへ保存、DMS__ 上に MasterPMD という名のホスト グループを作成、Master PMD のエンドポイント サブスクライバに対応する DMS__ 上にホストを作成、さらに MasterPMD ホスト グループにホストを結合します。

```
policydeploy -migrate MasterPMD@hostA -dms DMS__@hostB -policydir
"C:¥Data¥policies_MasterPMD_hostA" -hgcreate
```

policydeploy -reset 機能 - ポリシーのデプロイをリセット

この機能では、エンドポイント上のポリシーのデプロイをリセットします。CA Access Control によって、エンドポイント上の有効なポリシーのデプロイがすべて解除され、拡張ポリシー管理プロパティがすべて削除されて、ホストのステータスがリセットされます。

この関数の構文は、以下のようになります。

```
policydeploy -reset hnode_name [-dms list]
```

-dms *list*

(オプション) 使用する DMS ノードのカンマ区切りリストを指定します。ポリシーをデプロイまたはデプロイ解除する場合、そのアクションは DMS ノードにレポートされます。ポリシーを格納すると、DMS ノードに格納されます。

このオプションで DMS ノードを指定しない場合、policydeploy ユーティリティでは、ローカル CA Access Control データベースで指定された DMS ノードのリストが使用されます。DMS ノードのリストをデータベースに指定するには、dmsmgr を使用して新しい DMS を作成した後に、以下の selang コマンドを発行する必要があります。

```
so dms+(new_dms_name)
```

注: インストール時に DMS ノードを指定しなかった場合、またはエンドポイント上の登録済み DMS を置換したり、エンドポイントに登録済み DMS を追加する場合は、このコマンドを発行する必要があります。ただし、拡張ポリシー管理サーバの作成をインストール時に指定した場合、DMS はデータベースに追加され、このコマンドを手動で実行する必要はありません。

-reset *hnode_name*

指定されたエンドポイント上のポリシーのデプロイをリセットします。

policydeploy - restore 機能 - すべてのポリシーのリストア

指定されたホストのポリシーをデプロイ解除した後、すべてのデプロイ タスクをそのホストに再送して実行することで、デプロイ(割り当てまたは直接デプロイ)する必要のあるすべてのポリシーをリストア(直接再デプロイ)します。

重要: すでに適用されているポリシーがそのホストに存在する場合は、ホストのステータスがリストアの実行前にリセットされないため、リストアは失敗します。policydeploy - reset 機能を代わりに使用します。

この関数の構文は、以下のようになります。

```
policydeploy -restore hnode_name [-dms list]
```

-dms *list*

(オプション)使用する DMS ノードのカンマ区切りリストを指定します。ポリシーをデプロイまたはデプロイ解除する場合、そのアクションは DMS ノードにレポートされます。ポリシーを格納すると、DMS ノードに格納されます。

このオプションで DMS ノードを指定しない場合、policydeploy ユーティリティでは、ローカル CA Access Control データベースで指定された DMS ノードのリストが使用されます。DMS ノードのリストをデータベースに指定するには、dmsmgr を使用して新しい DMS を作成した後に、以下の selang コマンドを発行する必要があります。

```
so dms+(new_dms_name)
```

注: インストール時に DMS ノードを指定しなかった場合、またはエンドポイント上の登録済み DMS を置換したり、エンドポイントに登録済み DMS を追加する場合は、このコマンドを発行する必要があります。ただし、拡張ポリシー管理サーバの作成をインストール時に指定した場合、DMS はデータベースに追加され、このコマンドを手動で実行する必要はありません。

-restore *hnode_name*

指定されたホスト上でデプロイするべきポリシーをすべてリストア(直接再デプロイ)します。

policydeploy -store 機能 - ポリシーの格納

この機能により、コマンドによって指定された DMS ノードまたはローカル CA Access Control データベースに、指定されたポリシーを格納します。-silent オプションを使用していない場合は、表示されるメッセージでこのアクションを確認する必要があります。

指定されたポリシーの前のバージョンが DMS に格納されていない場合、このポリシーのバージョン 1（*name*#01）が作成されます。ポリシーの前のバージョンが存在する場合は、ポリシーの新しいバージョン（*name#last_version+1*）が作成されます。格納するポリシー バージョンは自動的にファイナライズされます。ポリシーを更新する必要がある場合は、変更された必要なポリシー デプロイおよびデプロイ解除ルールを含む新しいバージョンのポリシーを格納する必要があります。

この関数の構文は、以下のようになります。

```
policydeploy -store name -ds file1 [-uds file2] [-dms list] [-desc description]
[-prereq list] [-silent]
```

-desc *description*

（オプション）ポリシーに関する業務上の説明を定義します。

-dms *list*

（オプション）使用する DMS ノードのカンマ区切りリストを指定します。ポリシーをデプロイまたはデプロイ解除する場合、そのアクションは DMS ノードにレポートされます。ポリシーを格納すると、DMS ノードに格納されます。

このオプションで DMS ノードを指定しない場合、policydeploy ユーティリティでは、ローカル CA Access Control データベースで指定された DMS ノードのリストが使用されます。DMS ノードのリストをデータベースに指定するには、dmsmgr を使用して新しい DMS を作成した後に、以下の selang コマンドを発行する必要があります。

```
so dms+(new_dms_name)
```

注: インストール時に DMS ノードを指定しなかった場合、またはエンドポイント上の登録済み DMS を置換したり、エンドポイントに登録済み DMS を追加する場合は、このコマンドを発行する必要があります。ただし、拡張ポリシー管理サーバの作成をインストール時に指定した場合、DMS はデータベースに追加され、このコマンドを手動で実行する必要はありません。

-ds *file1*

デプロイ ルールを含むファイルのパス名を指定します。これらは、ポリシーを作成するために必要なコマンドです。-getrules オプションを使用すると、ユーティリティによってこのファイルが作成されます。

重要: ポリシーのデプロイでは、ユーザ パスワードを設定するコマンドはサポートされていません。そのようなコマンドをデプロイ スクリプト ファイルに含めないでください。ネイティブ selang コマンドはサポートされていますが、偏差レポートには示されません。

-prereq *list*

(オプション) このポリシーをデプロイする前にデプロイする必要のあるポリシーのカンマ区切りリストを定義します。

重要: 前提となるポリシー (必須ポリシー) がデプロイされていない状態で、それに依存するポリシー (依存ポリシー) をデプロイしようとすると、デプロイ タスクのステータスは *Pending Prerequisite* に変わります。必須ポリシーがすべてデプロイされると、依存ポリシーのデプロイが再開されます。同様に、別のデプロイ済みポリシーの必須ポリシーのデプロイを解除しようとすると、デプロイ タスクのステータスは *Pending Dependents* に変わり、すべての依存ポリシーのデプロイが解除された後に、デプロイが再開されます。

-silent

(オプション) 要求されたアクションに対する確認メッセージを抑制します。

-store *name*

指定された DMS ノードまたはローカル CA Access Control データベースに、指定されたポリシーを格納します。

注: ポリシー名には # (ハッシュ) 文字を使用できません。この文字は、ポリシーのバージョン番号を示すために予約されており、自動的に追加されます。

-uds *file2*

ポリシーのデプロイ解除に必要なルールを含むファイルのパス名を定義します。これらは、ポリシーのデプロイを解除するために必要なコマンドです。-getrules オプションを使用すると、ユーティリティによってこのファイルが作成されます。

CA Access Control によってポリシーがデプロイ解除される場合に、ポリシーのデプロイ解除スクリプトが格納されていないと、CA Access Control によってポリシーの削除に必要なコマンドが算出されます。

例: IIS 5 保護ポリシーの格納

次の例は、インターネット インフォメーション サービス(IIS)5 Web サーバを保護するためのポリシーの格納方法を示します。ここでは、今回初めて DMS にこのポリシーを格納するものとします。

注: この例に示した selang コマンドは Windows オペレーティング システムのリソースに対するものですが、UNIX でも同じ手順が適用されます。

1. 以下の IIS スクリプトを含む IIS5.selang というファイルを保存します。

```
# IIS5 デプロイ スクリプト
eu inet_pers owner(nobody)
er FILE c:¥InetPub¥wwwroot¥* defaccess(none) owner(nobody)
authorize FILE c:&yen;InetPub&yen;wwwroot&yen;* uid(inet_pers) access(all)
er FILE c:¥InetPub¥wwwroot¥scripts defaccess(none) owner(nobody)
er FILE *.asp defaccess(none) owner(nobody)
authorize FILE *.asp uid(inet_pers) via(pgm(inetinfo.exe)) access(read, execute)
```

   これらは、IIS 5 保護ポリシーをデプロイするために必要なコマンドです。

2. 以下のスクリプトを含む IIS5_rm.selang というファイルを保存します。

```
# IIS5 デプロイ解除スクリプト
ru inet_pers
rr FILE c:&yen;InetPub&yen;wwwroot&yen;*
rr FILE c:&yen;InetPub&yen;wwwroot&yen;scripts
rr FILE *.asp
```

   これらは、手順 1 で作成した IIS 5 保護ポリシーをデプロイ解除するために必要なコマンドです。

3. コマンド プロンプト ウィンドウを開き、policydeploy ユーティリティを実行します。

```
policydeploy -store IIS5 -ds IIS5.selang -uds IIS5_rm.selang -desc "IIS5 web
server security policy" -silent
```

   これにより、IIS5.selang および IIS5_rm.selang で定義されたスクリプトで、ポリシー IIS5(GPOLICY オブジェクト)および最初のポリシー バージョン(IIS5#01 POLICY オブジェクト)が DMS に格納されます。

policydeploy -upgrade 機能 - ポリシー バージョンのアップグレードまたはダウングレード

この機能は、定義されたホスト上でポリシーを最新のファイナライズされたバージョンにアップグレードするか、または定義されたホスト上で指定されたポリシーバージョンへダウングレードします。

この関数の構文は、以下のようになります。

```
policydeploy {-upgrade name | -downgrade name#xx} [-nodelist hnode_list|-ghnode name]
[-list] [-dms name]
```

-dms *list*

(オプション)使用する DMS ノードのカンマ区切りリストを指定します。ポリシーをデプロイまたはデプロイ解除する場合、そのアクションは DMS ノードにレポートされます。ポリシーを格納すると、DMS ノードに格納されます。

このオプションで DMS ノードを指定しない場合、policydeploy ユーティリティでは、ローカル CA Access Control データベースで指定された DMS ノードのリストが使用されます。DMS ノードのリストをデータベースに指定するには、dmsmgr を使用して新しい DMS を作成した後に、以下の selang コマンドを発行する必要があります。

```
so dms+(new_dms_name)
```

注: インストール時に DMS ノードを指定しなかった場合、またはエンドポイント上の登録済み DMS を置換したり、エンドポイントに登録済み DMS を追加する場合は、このコマンドを発行する必要があります。ただし、拡張ポリシー管理サーバの作成をインストール時に指定した場合、DMS はデータベースに追加され、このコマンドを手動で実行する必要はありません。

-downgrade *name#xx*

定義されたホスト上の指定されたポリシー バージョンにポリシーを戻します。

-ghnode *name*

実行する操作のホスト グループの名前を定義します。

-list

(オプション)指定したデプロイ済みポリシーと同じバージョンを持つホストを一覧表示します。バージョンは指定しません。-upgrade を使用すると、暗黙的に指定されるバージョンは、使用可能な最新バージョンになります。

-nodelist *hnode_list*

操作を実行するホスト（HNODE オブジェクト）のカンマ区切りリストを定義します。

-upgrade *name*

指定されたポリシーを、定義されたホスト上の最新の最終バージョンにアップグレードします。

例: IIS 5 保護ポリシーのアップグレード

次の例は、policydeploy ユーティリティを使用してポリシーをアップグレードする方法を示しています。まず、デプロイを確認して、このポリシーの最新バージョンがデプロイされていないホストを明らかにします。

1. コマンド プロンプト ウィンドウで、policydeploy ユーティリティを実行します。

   ```
   policydeploy -upgrade IIS5 -list
   ```

   IIS5 ポリシーの古いバージョンがデプロイされているホストが一覧表示されます。

2. このようなホストをすべて、最新のポリシー バージョンにアップグレードします。

   ```
   policydeploy -upgrade IIS5
   ```

例: IIS 5 保護ポリシーのダウングレード

次の例は、policydeploy ユーティリティを使用してポリシーをダウングレードする方法を示します。まず、デプロイを確認して、どのホストにおいてデプロイされているポリシーに古いバージョンが存在しているかを明らかにします。

1. コマンド プロンプト ウィンドウで、policydeploy ユーティリティを実行します。

   ```
   policydeploy -downgrade IIS5#3 -list
   ```

   バージョン 3 より新しい IIS5 ポリシー バージョンがデプロイされているホストが一覧表示されます。

2. これらのホストをすべて、ポリシーの 3 番目のバージョンにダウングレードします。

   ```
   policydeploy -downgrade IIS5#3
   ```

pwextractor ユーティリティ -- 特権アカウント パスワードを抽出します。

pwextractor ユーティリティはデータベースから特権アカウントのパスワードを抽出します。特権アカウントのパスワードをバックアップする場合、または 特権ユーザ パスワード管理 が利用可能ではないため特権アカウントをチェックアウトできない場合、pwextractor を使用することができます。

pwextractor を使用するには、以下が必要になります。

- データベース テーブルへのアクセス権
- データベースにアクセスするために 特権ユーザ パスワード管理 で使用するアカウントのユーザ名およびパスワード

  注: これらのクレデンシャルは、エンタープライズ管理サーバをインストールする際に使用します。

Microsoft SQL Server データベースを使用しており、そのデータベースの認証モデルが Windows 認証である場合、pwextractor を使用するときには、以下のことを行う必要があります。

- sqljdbc_auth.dll ファイルが JAVA_HOME¥bin ディレクトリ内にあることを確認します。
- pwextractor -url 形式を使用します。
- JDBC URL 文字列中に「integratedSecurity=true;」を指定します。

注: pwextractor -url 形式を使用できるのは、Windows コンピュータにエンタープライズ管理サーバをインストールしており、かつ、Microsoft SQL Server データベースを使用している場合のみです。sqljdbc_auth.dll ファイルの詳細については、Microsoft SQL Server ドキュメントを参照してください。

pwextractor は、以下のディレクトリに配置されています。

ACServerInstallDir/IAM Suite/Access Control/tools/pwextractor

このコマンドの形式は以下のようになります。

```
pwextractor -h hostname [-r port] -d {database | schema} -t {mssql | oracle} -l login
-p password -f filename [-k key_file]
```

JDBC データベースが対象の場合のコマンド形式は以下のとおりです。この形式が有効なのは、Windows コンピュータにエンタープライズ管理サーバをインストールしており、かつ、Microsoft SQL Server データベースを使用している場合のみです。

```
pwextractor -url url -f filename [-k key_file]
```

-h *hostname*

データベース ホストの名前を定義します。

-r *port*

データベースが通信するポート番号を定義します。

-d {*database* | *schema*}

以下を定義します:

- （MS SQL）データベース名を定義します。
- （Oracle）スキーマ名を定義します。

-t {mssql | oracle}

データベース タイプを指定します。

値: mssql、Oracle

-l *login*

データベースにアクセスするために 特権ユーザ パスワード管理 で使用するアカウントのユーザ名を定義します。

-p *password*

データベースにアクセスするために 特権ユーザ パスワード管理 で使用するアカウントのパスワードを定義します。

-f *filename*

出力ファイルのディレクトリ パスおよびファイル名を定義します。既存のファイルを指定すると、pwextractor によって既存のファイルが新しく出力されたファイルに置き換えられます。

-k *key_file*

パスワードの暗号化に使用した暗号化ファイルの完全パスおよびファイル名を定義します。

-url *url*

データベースにアクセスするために使用する JDBC URL 文字列を定義します。

形式: jdbc:sqlserver://*servername*:*port*[;*property*=*value*]

例:
jdbc:sqlserver://localhost:1433;selectMethod=cursor;DatabaseName=mydb;user=sa;password=mypwd;

例: Microsoft SQL Server データベース から 特権ユーザ パスワード管理 パスワードを抽出する

以下の例では、ホスト myhost.example.com 上にある、mydb という名前の Microsoft SQL Server データベースから 特権ユーザ パスワード管理 パスワードを抽出しています。エンタープライズ管理サーバは Windows コンピュータ上にあり、暗号化ファイルは C:¥FIPSkey.dat にあります。pwextractor は出力を C:¥accounts.txt ファイルに書き込みます。

- 次の例は、データベース認証モードが SQL Server 認証であるときにパスワードを抽出します。

```
pwextractor.bat -h myhost.example.com –r 1433 -d mydb -t mssql -l sa -p mypwd -f
C:¥accounts.txt -k "C:¥FIPSkey.dat"
```

- 次の例は、データベース認証モードが Windows 認証であるときにパスワードを抽出します。

```
pwextractor.bat -url
jdbc:sqlserver://myhost.example.com:1433;selectMethod=cursor;DatabaseName=myd
b;user=sa;password=mypwd;integratedSecurity=true; -f C:¥accounts.txt -k
"C:¥FIPSkey.dat"
```

ReportAgent ユーティリティ -- レポートのスナップショットおよび監査イベントを送信します。

レポート エージェント（ReportAgent）は、レポート スナップショットおよび監査イベントを配布サーバに送信し、CA Access Control、UNIX 認証ブローカ、および CA Enterprise Log Manager のレポートに含まれるようにします。

レポート エージェントを実行するには、レポート用にエンドポイントを設定する必要があります。レポート用にエンドポイントを設定する際は、レポート エージェントが通信する配布サーバと、実行されるスケジュールを指定します。レポート用にエンドポイントを設定したら、レポート エージェントはデーモンまたはサービスとして実行され、スケジュールされた時間にスナップショットを送信します。ただし、配布サーバにすぐにレポート スナップショットまたは監査イベントを送信する必要がある場合は、レポート エージェントをオンデマンドで実行できます。

注: レポート用にエンドポイントを設定する方法の詳細については、「実装ガイド」を参照してください。report_agent.sh スクリプトを使用して、UNIX コンピュータ上でレポート エージェントを設定、開始、停止することもできます。

UNIX コンピュータで、ReportAgent ユーティリティを *ACSharedDir*/bin ディレクトリから実行します。*ACSharedDir* は、デフォルトでは /opt/CA/AccessControlShared ディレクトリです。また、ライブラリ パス環境変数を設定する必要がある場合があります。

このコマンドの構文は、以下のようになります。

```
ReportAgent -debug {0 | 1 | 2} -task {0 | 1 | 2 | 3 | 4} [-now]
ReportAgent -report snapshot
```

-debug {0 | 1 | 2}

レポート エージェントをデバッグ モードで実行するように指定します。このオプションを使用するには、ReportAgent サービスまたはデーモンを停止する必要があります。

制限: 0 -- デバッグ情報をコンソールに出力します。

1 -- デバッグ情報をログ ファイルに出力します。

2 -- デバッグ情報を出力しません。

-task {0 | 1 | 2 | 3 | 4}

レポート エージェントが配布サーバに送信する情報を指定します。

制限 0 -- CA Access Control データベースのスナップショットおよびすべてのローカル PMDB を、配布サーバ上のキュー/スナップショット キューに送信します。

1 -- エンドポイント監査イベントを、配布サーバ上のキュー/監査キューに送信します。

2 -- (UNIX) UNIX 認証ブローカ データベースのスナップショットを、配布サーバ上の ac_endpoint_to_server キューに送信します。

3 -- (UNIX) UNIX 認証ブローカ 監査イベントを配布サーバ上のキュー/監査キューに送信します。

4 -- (UNIX) キー ロガー監査イベントを、配布サーバ上のキュー/監査キューに送信します。

-now

レポート エージェントを今すぐ実行するよう指定します。

このオプションを指定しない場合、レポート エージェントは次にスケジュールされている時間に実行されます。

-report snapshot

CA Access Control データベースのスナップショットおよびすべてのローカル PMDB を、配布サーバ上のキュー/スナップショット キューにすぐに送信するよう指定します。このオプションを使用するには、ReportAgent サービスまたはデーモンが実行されている必要があります。

例: レポート エージェントのデバッグ情報の表示

以下の例は、Linux コンピュータ上でライブラリ パス環境変数を設定し、レポート エージェントがデバッグ モードですぐに実行されるように指定し、デバッグ情報をコンソールに出力して、監査イベントを配布サーバに送信します。

```
LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:/opt/CA/AccessControlShared/lib
export LD_LIBRARY_PATH
cd /opt/CA/AccessControlShared/bin
./ReportAgent -debug 0 -task 1 -now
```

詳細情報:

ReportAgent (P. 328)
ReportAgent キー - レジストリの設定 (P. 621)

レポート エージェントのログ ファイル

以下の表は、ReportAgent -debug 1 コマンドを実行した場合に、レポート エージェントによってデバッグ情報が書き込まれるログ ファイルを示しています。この表では、*ACSharedDir* はデフォルトの /opt/CA/AccessControlShared ディレクトリで、*ACInstallDir* は CA Access Control をインストールしたディレクトリです。

ReportAgent オプション	UNIX ログ ファイル	Windows ログ ファイル
-task 0	*ACSharedDir*/log/ac2xml.log	*ACInstallDir*¥log¥ac2xml.log
-task 1	*ACSharedDir*/log/ac2elm.log	*ACInstallDir*¥log¥ac2elm.log
-task 2	*ACSharedDir*/log/unab2xml.log	-
-task 3	*ACSharedDir*/log/unab2elm.log	-
-task 4	*ACSharedDir*/log/kbl2elm.log	-

report_agent.sh スクリプト - レポート エージェントの設定

UNIX で該当

report_agent.sh スクリプトによって、インストール後にレポート エージェント デーモンを設定できます。CA Access Control のインストール時に設定したレポート エージェント構成設定を変更する必要がある場合に、report_agent.sh スクリプトを使用します。

report_agent.sh スクリプトは、*ACSharedDir*/lbin にあります。デフォルトでは、このディレクトリは /opt/CA/AccessControlShared/lbin です。

このコマンドの形式は以下のようになります。

```
report_agent.sh start
report_agent.sh stop
report_agent.sh config -server hostname [-proto {ssl|tcp}] [-port port_number]
[-rqueue queue_name] ¥
[-schedule <time@day[,day2,...]>] [-audit] [-bak] [-silent]
```

config

その他のパラメータがレポート エージェント デーモンを設定することを指定します。

start

レポート エージェントを起動します。

stop

レポート エージェントを停止します。

-server *hostname*

配布サーバ ホスト名を定義します。-port オプションによる入力と組み合わせて、配布サーバ URL が構成され、ReportAgent セクションに report_server 設定が設定されます。

-audit

エンドポイント監査データを配布サーバに送信するかどうかを指定します。ReportAgent セクションの reportagent_enabled 構成設定が設定されます。

-bak

監査ファイルのタイムスタンプがあるバックアップを保存することを指定します。logmgr セクションの構成設定 Backup_Date が yes に設定され、audit_max_files が 50 に設定されます。

-port *port_number*

配布サーバとの通信に使用するポート番号を定義します。-server オプションによる入力と組み合わせて、配布サーバ URL が構成され、ReportAgent セクションに report_server 設定が設定されます。

-proto

接続プロトコル（TCP または SSL）を指定します。ReportAgent セクションの use_ssl 構成設定が設定されます。

-rqueue *queue_name*

レポート エージェントがローカル データベースおよび PMDB のスナップショットを送信するキューの名前を定義します。ReportAgent セクションの send_queue 構成設定が設定されます。

-schedule <*time*@*day*[,*day2*,...]>

レポートを生成する日時と配布サーバに送信する日時を定義します。

-silent

確認を求めないことを指定します。

例: レポート エージェントの設定

この例では、レポート エージェントがデータベース スナップショットを rscomp.com の配布サーバに送信するように設定します。SSL でポート 7243 および queue/snapshots という名前のキューを使用します。また、配布サーバに監査データを送信するようにし、監査ログ ファイルのバックアップ設定も行います。

```
report_agent.sh config -server rscomp.com -proto ssl -port 7243 -rqueue
queue/snapshots -audit
```

レポート エージェントを設定したら、配布サーバが認識可能な正しいパスワード(共有秘密)を使用して +reportagent user を更新してください。それには、以下のように入力します。

```
eu +reportagent epassword(Shared_Secret) nonnative
```

詳細情報:

ReportAgent (P. 328)

seaudit ユーティリティ - 監査ログ レコードの表示

seaudit ユーティリティは、CA Access Control 監査ログ ファイルのレコードを表示します。Windows 上で seaudit ユーティリティを実行するには、AUDITOR 属性が必要です。UNIX 上で seaudit ユーティリティを実行するには、seos.ini 内の audir_group に属している必要があります。パスワードが含まれる監査レコードを表示する場合、seaudit によってパスワード テキストの部分がアスタリスク(***)に置き換えられて、パスワードが保護されます。

注: コマンド スイッチおよびオプションでは、文字列マッチングが可能です。マスクの引数を自動的に展開する UNIX シェルもあります。このようなシェルから seaudit を起動する場合は、マスクがシェルによって処理されないように、アスタリスクまたは疑問符の前に円記号(¥)を入力する必要があります。

注: seaudit ユーティリティでは、トレース レコードがユーザ ID 別ではなく、ユーザ名別に表示されます。

このコマンドの形式は以下のようになります。

```
seaudit switch [options]
```

switch

seaudit ユーティリティの操作モードを定義します。以下の*いずれか*を指定できます。

-a | -all

すべてのレコードを表示します。ただし、トレース機能によって監査ログに送信されたユーザ トレース レコードは除きます。

注: UNIX で使用可能な接続された TCP レコードも表示されません。これらのレコードを表示するには、-c オプションも指定する必要があります。

-h | -help

このユーティリティのヘルプ画面を表示します。

{-i | -inet} *host service*

指定されたサービスの指定されたホストから受け取った TCP 要求の INET 監査レコードを表示します。*host* および *service* は、seaudit が検索するホストとサービスを特定するマスクです。

UNIX 上で、接続が行われたネットワーク ID(ポート番号)を持つ TCP レコードを一覧表示するには -c フラグを追加します。例:

```
seaudit -i -c myhost telnet
```

{-l | -login} *user1, user2, ... terminal*

指定された端末上の、カンマで区切られた指定ユーザに関する LOGIN レコードを表示します。

user と *terminal* はいずれもマスクです。

UNIX では、ユーザを有効化または無効化するときに serevu で作成されたレコード、および無効なパスワードを入力するときに認証デーモンで作成されたレコードも表示されます。

{-r | -resource} *class resource user1, user2, ...*

カンマで区切られた指定ユーザについて、指定されたリソースの指定されたクラスに関する一般リソース監査レコードを表示します。

- *class* は、アクセスされたリソースが属しているクラスを特定するマスクです。
- *resource* は、アクセスされたリソースの名前を特定するマスクです。
- *user* は、リソースにアクセスしたユーザの名前を特定するマスクです。

-s | -start

CA Access Control の起動メッセージおよび停止メッセージを表示します。

-St | -Stat *message_number*

（UNIX のみ）。Watchdog のメッセージ番号の説明を表示します。

-t | -table

ログ コードの表を表示します。

-tr

アクティビティがトレース対象になっているすべてのユーザのトレース レコードを表示します。

注: トレース レコードは、ログイン セッション ID 列をデフォルトで表示します。この列を表示しない場合は、th -format オプションを使用します。

-trr *resource*

指定されたリソースのトレース レコードを表示します。

-tru {*uid1*|*user1*}, {*uid1*|*user2*}, ...

指定されたユーザ ID またはユーザ名を持つユーザのトレース レコードを表示します。

-u *command class record user*

以下のようなデータベース更新の監査レコードを表示します。

- *command* は、検索対象の selang のコマンド セットを特定するマスクです。
- *class* は、検索対象のクラスを特定するマスクです。
- *record* は、検索対象のレコードを特定するマスクです。
- *user* は、コマンドを実行したユーザを特定するマスクです。

-w

Watchdog の監査レコードを表示します。

options

seaudit ユーティリティが情報を表示する方法を変更する、オプションの修飾子を定義します。以下の 1 つまたは複数の修飾子を指定できます。

-c

（UNIX のみ）。接続された INET レコードを表示します。これらのレコードは、セッション ID の追跡中に生成され、成功した TCP 接続のポート番号を一覧表示します。

たとえば、ユーザ（user1）が Telnet セッションを comp1 から comp2 に開きます。comp1 と comp2 の両方に CA Access Control がインストールされています。comp2 の CA Access Control は、Telnet セッションによりログインしたユーザ（user1 以外のユーザの場合もあります）のクレデンシャルと共に確認応答を comp1 に送信するように設定（logconnected 構成設定）できます。comp1 はこの確認応答を受け取ると、TCP-CONNECTED レコード（セッション確立レコード）を作成します。このレコードは、-c オプションを使用して表示できます。

-detail

各レコードに関する詳細情報を表示します。

-delim *delimiter*

最初のフィールドの前および残りの各フィールド間で使用する区切り文字を定義します。たとえば、以下のコマンドにより、フィールド全体が引用符で囲まれ、各フィールドがカンマで区切られて表示されます。

seaudit -a -delim ¥",¥"

-delim2 *delimiter*

区切り文字が最初のフィールドの前に表示されないこと以外は、-delim オプションと同じです。

-delim3 *delimiter*

曜日、月、年の間の区切り文字が含まれる以外は、-delim オプションと同じです。

-delim4 *delimiter*

-delim2 オプションと同じです。

-ed *date*

終了日を指定します。この日付より後にログに記録されたレコードは表示*されません*。

以下の 2 つの方法のいずれかを使用して、日付を指定できます。

- 形式 *dd-mm-yyyy* を使用します。
- 文字列 *today* を使用して、今日の日付を設定します。

文字列「*today*」の後に「- (マイナス)」と数値を指定することもできます。これにより、今日の日付から指定された日数だけ前の日付を定義できます。たとえば *today-3* の場合、現在の日付から 3 日前の日付を指定することを意味します。

-et *time*

終了時刻を指定します。この時刻より後にログに記録されたレコードは表示*されません*。

以下の 2 つの方法のいずれかを使用して、時刻を指定できます。

- 24 時間形式の *hh:mm* を使用します。
- 文字列 *now* を使用して、現在の時刻を設定します。

  文字列「*now*」の後に「- (マイナス)」と数値を指定することもできます。これにより、現在の時刻から指定された分数だけ前の時刻を定義できます。たとえば now-*60* の場合、現在の時刻から 60 分 (1 時間) 前の時刻を指定することを意味します。特定の日付の範囲内で時間枠を正確に定義するには、このオプションを -sd、-ed、またはその両方と組み合わせて指定します。

-f | -failure

失敗したアクセスを表示*しないように*指定します。

{-fn | -file} *fileName*

検索対象の監査ログ ファイルの名前を指定します。

-format *release*

出力形式が CA Access Control *リリース*の形式と同じであることを指定します。

release - リリース番号を定義します。有効な値は以下のとおりです。

- **80sp1** - r8 SP1 の出力には、新しいリリースに存在する有効な UID 列は含まれていません。
- **12** - r12.0 の出力には、パスワード変更レコードを表示する機能は含まれません。トレース レコードでは、r12.0 の出力にもログイン セッション ID 情報は含まれていませんでした。

-g | -grant

成功した(許可された)アクセスを表示*しないように*指定します。

-gn | -grantnotify

通知レコードを除き、成功した(許可された)アクセスを表示*しないように*指定します。

-kbl -a -sid *sid* {-rp | -pr | -cmd | -exe | -disp}

(UNIX のみ)キー ロギング監査ファイル(kbl.audit)のコンテンツを表示するよう指定します。

-a

監査ファイル内の記録されたセッションをすべて表示します。

-sid *sid*

キー ロギング セッション ID を指定します。

-rp

キー ロギング セッション全体を再生します。

-pr

キー ロギング セッション全体を表示します(制御文字を除く)。

-cmd

(UNIX のみ)コマンド ラインのロギング セッション中にユーザが入力したコマンドを表示します。

-exe

ユーザがシェルで実行したコマンドの EXECARGS 詳細を表示します。

-disp

記録されたセッション期間を表示するように指定します。

注: このコマンドは、シェル bash、tcsh、csh、ksh、jsh、rsh、ash、zsh で実行できます。

-logout

(UNIX のみ)ログアウト レコードを表示しないように指定します。

-millennium

(UNIX のみ)年を下 2 桁ではなく 4 桁で表示するように指定します。

-n | -netaddr

TCP/IP レコードのホスト名ではなく、インターネット アドレスが表示されるように指定します。

-notify

NOTIFY 監査レコードが表示されないように指定します。

{-o | -origin} *host*

指定された host から送信されたレコードのみが表示されるように指定します。

このオプションは、selogrcd ログ ルーティング収集デーモンで作成された統合監査ファイルからレコードを参照する場合にのみ使用できます。

-pwa

（UNIX のみ）パスワード試行レコードが表示されないように指定します。

-sd *date*

開始日を指定します。この日付より前にログに記録されたレコードは表示*されません*。

以下の 2 つの方法のいずれかを使用して、日付を指定できます。

- 形式 *dd-mm-yyyy* を使用します。
- 文字列 *today* を使用して、今日の日付を設定します。

文字列「*today*」の後に「- （マイナス）」と数値を指定することもできます。これにより、今日の日付から指定された日数だけ前の日付を定義できます。たとえば *today-3* の場合、現在の日付から 3 日前の日付を指定することを意味します。

sessionid

ユーザ ログイン セッション ID 情報が含まれている列を表示するように指定します。この列は、デフォルトでは非表示です。

注: このオプションは、r12.0 SP1 以上のエンドポイントでのみ有効です。

-st *time*

開始時刻を指定します。この時刻より前にログに記録されたレコードは表示*されません*。

以下の 2 つの方法のいずれかを使用して、時刻を指定できます。

- 24 時間形式の *hh:mm* を使用します。
- 文字列 *now* を使用して、現在の時刻を設定します。

文字列「*now*」の後に「- (マイナス)」と数値を指定することもできます。これにより、現在の時刻から指定された分数だけ前の時刻を定義できます。たとえば now-*60* の場合、現在の時刻から 60 分(1 時間)前の時刻を指定することを意味します。特定の日付の範囲内で時間枠を正確に定義するには、このオプションを -sd、-ed、またはその両方と組み合わせて指定します。

-v | -servnum

サービス名ではなく、ポート番号が表示されるように指定します。

-warn

警告レコードが表示*されないように*指定します。

例

- 2004 年 1 月 3 日以降のすべての監査レコードを一覧表示するには、以下のコマンドを使用します。

```
seaudit -a -sd 04-Jan-2004
```

- 2004 年 1 月 3 日に実行された、root ユーザによる任意の端末からの失敗したログインを一覧表示するには、以下のコマンドを使用します。

```
seaudit -sd 04-Jan-2004 -ed 04-Jan-2004 -l root * -g
```

- ユーザ John が FILE クラスのすべてのリソースに対して行ったすべてのアクセスを一覧表示するには、以下のコマンドを使用します。

```
seaudit -r FILE * John
```

- すべての日付の 17:00 (最初の日)から 08:00 (次の日)の間に記録されたすべての監査レコードを一覧表示するには、以下のコマンドを使用します。

```
seaudit -a -st 17:00 -et 08:00
```

- 08:00 から 17:00 の間に記録されたすべての監査レコードを一覧表示するには、以下のコマンドを使用します。

```
seaudit -a -st 08:00 -et 17:00
```

- 1 人のユーザについて、ログインおよびリソースへのアクセスに関するすべての警告レコードを一覧表示するには、以下のコマンドを使用します。

  ```
  seaudit -login * * -resource * * * -grant -failure -logout -pwa
  ```

- 2 人のユーザについて、すべてのログイン レコードを一覧表示するには、以下のコマンドを使用します。

  ```
  seaudit -login "user1, user2"
  ```

- 昨日の監査レコードをすべて一覧表示するには、以下のコマンドを使用します。

  ```
  seaudit -a -sd today-1 -ed today-1
  ```

- kbl.audit ログ ファイル内の監査レコードをすべて一覧表示するには、以下のコマンドを使用します。

  ```
  seaudit -kbl
  ```

- ユーザ セッションを再生するには、以下のコマンドを使用します。

  ```
  seaudit -kbl -sid 22316 -rp
  ```

- ユーザがセッション中に入力したコマンドをすべて表示するには、以下のコマンドを使用します。

  ```
  seaudit -kbl -sid 22316 -cmd
  ```

- UID 244 の単一ユーザがファイルにアクセスしようとしたアクティビティをトレースする監査レコードをすべて一覧表示するには、以下のコマンドを使用します。

  ```
  seaudit -tru 244 -trr FILE
  ```

- 2 人のユーザのアクティビティをトレースする監査レコードをすべて一覧表示するには、以下のコマンドを使用します。

  ```
  seaudit -tru "user1, 244"
  ```

詳細情報:

監査レコードのイベント タイプを識別する方法 (P. 644)
監査イベント タイプ (P. 646)

sebuildla ユーティリティ - lookaside データベースの作成

UNIX で該当

sebuildla ユーティリティは、CA Access Control の seosd デーモンで使用される lookaside データベースを作成します。seosd デーモンは、lookaside データベースを使用して、UNIX UID をユーザ名に、GID をグループ名に、ホストの IP アドレスをホスト名に、およびサービス ポートをポート名にそれぞれ変換します。このデータベースには、名前を変換するための数値のみが含まれています。sebuildla を使用すると、LDAP ディレクトリ情報ツリー（DIT）からユーザ lookaside データベースに情報を追加することもできます。

重要: sebuildla および必要な LDAP 設定をセットアップするには、LDAP をよく理解していること、および ldapsearch コマンドを実行できることが必要です。ldap（1）、ldapsearch（1）についての man ページ、および LDAP クライアント用のマニュアルでセットアップの説明を参照することをお勧めします。また、sebuildla を使用して lookaside データベースを作成する前に、その lookaside データベースの完全パスを lookaside_path 構成設定に指定できます。

初めて lookaside データベースを作成する場合は、以下のコマンドを実行します。

```
sebuildla -a
```

このコマンドによって、データベースの すべてのコンポーネントが作成されます。このデータベースの各ファイルは、適切なスイッチを使用して後で更新できます。

CA Access Control を NIS サーバ、NIS+ サーバ、または DNS サーバにインストールした場合は、sebuildla ユーティリティの呼び出しを、関連する makefile に挿入する必要があります。

注: デフォルトでは、lookaside データベース ファイル（groupdb.la、hostdb.la、servdb.la、および userdb.la）は、sebuildla プログラムによるアクセスを除くすべてのユーザ アクセスから保護されています。

sebuildla ユーティリティは、/etc ファイルや NIS などのシステムの解決メカニズムをスキャンして、lookaside データベースを作成します。

- sebuildla は /etc/resolv.conf を読み取り、使用したドメイン名を取得します。

  注: CA Access Control ホスト名を完全修飾名に解決するには、resolv.conf ファイルに定義済みのドメイン設定オプションまたは検索設定オプションが含まれている必要があります。resolv.conf ファイルの詳細については、このファイルの man ページを参照してください。

- sebuildla はシステム解決オプションを使用して、lookaside データベースを作成します（通常、これはネットワーク キャッシング デーモンです）。
- CA Access Control は、（ネットワーク キャッシング デーモンまたはその他のシステム解決オプションに）/etc/nsswitch.conf ファイルを使用して、データを取得する場所を決定します。

たとえば、/etc/nsswitch.conf ファイルにホストに関する以下の行が含まれている場合、情報はまずローカル コンピュータのファイル（/etc/hosts）から取得されます。その後、DNS、NIS から順に情報が取得されます。

```
hosts:      files dns nis
```

ファイルに以下の行が含まれている場合、情報はローカル コンピュータのファイルからのみ取得されます。lookaside データベースには、/etc/hosts 内のホストのみが含まれます。

```
hosts:      files
```

注: ホストに完全修飾名がある場合、sebuildla はその完全修飾名を使用します。

コンピュータの環境設定の違いが原因で、sebuildla でローカル環境名が一部表示されない場合があります。その場合は、sebuildla を使用して、必要なすべてのエントリをリスト ファイルからロードすることができます。これを行うには、各オブジェクト名が別々の行に指定されたリスト ファイルを作成します。sebuildla はこのリスト ファイルを読み取り、必要に応じて、そのリストファイル内のすべてのオブジェクトが、関連する lookaside データベースに追加されたことを確認します。sebuildla では、重複したオブジェクトは無視されます。

以下の表に、sebuildla が各 lookaside データベースの作成に使用するファイルを示します。

リスト ファイル内のオブジェクト	追加先データベース
ACInstallDir/ladb/userlist	ユーザの lookaside データベース
ACInstallDir/ladb/grouplist	グループの lookaside データベース
ACInstallDir/ladb/hostlist	ホストの lookaside データベース
ACInstallDir/ladb/servlist	サービスの lookaside データベース

ACInstallDir/ladb ディレクトリにあるファイルの形式は、以下のとおりです。

- sebuildla では、空白行と、感嘆符(!)、番号記号(#)、またはセミコロン(;)で始まる行は無視されます。
- その他の行は、sebuildla が適切な lookaside データベースに追加する必要があるエントリを示します(エントリが解決できる場合)。
- ユーザ名、グループ名、ホスト名、またはサービス名は、行の先頭から開始する必要があります。

リスト ファイルの作成には dbmgr -dump -r を使用できます。たとえば、ローカル データベースの HOST クラスに定義されているホストのリストを作成するには、以下のように入力します。

```
dbmgr -dump -r l HOST > /opt/CA/AccessControl//ladb/hostlist
```

-l スイッチを指定すると、各ホスト エントリを取得するたびにその FQDN を DNS サーバに問い合わせる代わりに、デフォルト ドメイン内の全ホストのリストに対する要求が DNS から一括して行われます。高速ロード オプションは、DNS がインストールされている場合にのみ有効です。完全修飾されるのは、デフォルト ドメイン内のホスト名のみです。完全修飾名は、そのままの状態です。システム メカニズムでスキャンされた完全修飾されていないホスト名およびデフォルト ドメインにないホスト名は、未修飾のままです。hostlist ファイルからロードされた完全修飾されていないホスト名は除外されます。

このコマンドの形式は以下のようになります。

```
sebuildla switch [options]
```

switch

sebuildla ユーティリティの操作モードを指定します。以下の*いずれか*を指定できます。

--a

すべての lookaside データベース ファイルを作成します。

--e

DNS を除く、ホストの lookaside データベース ファイルを作成します。

--g

グループの lookaside データベース ファイルを作成します。

-h

DNS でホストの lookaside データベース ファイルを作成します。

-help

このユーティリティのヘルプ画面を表示します。

-n

LDAP ディレクトリ情報ツリー(DIT)から情報を収集し、プライマリ ユーザ データ ソース(-u スイッチ)から作成したユーザの lookaside データベースにその情報を追加します。このスイッチは、-u スイッチまたは -a スイッチと同時に使用できます。このため、LDAP DIT が、追加のユーザ データを提供し、システムのネーミング サービスとして使用されない場合は、最も便利なスイッチとなります。

このスイッチを使用する前に、以下の手順に従います。

a. seos.ini ファイルの ldap_base、ldap_hostname、および ldap_userdn の各トークンを CA Access Control に設定して、LDAP サービスを検索します。

b. seldapcred ユーティリティを実行して、暗号化された LDAP パスワードを格納します。

c. （オプション）ldap_port トークンおよび ldap_timeout トークンを現在の環境に設定します。

LDAP サービスから情報を取得する際にかかる時間は、LDAP サービスの実行速度、および DIT に格納されているユーザ データ量によって異なります。これらのことを考慮した上で、seos.ini ファイルの [seos] セクション内の ldap_timeout トークンを調整します。

d. （オプション）標準以外のスキーマを使用している場合は、ldap_uid_attr、ldap_uidNumber_attr、および ldap_user_class の各トークンを設定します。

-s

サービスの lookaside データベース ファイルを作成します。

-u

ユーザの lookaside データベース ファイルを作成します。

注: -n スイッチを -u スイッチと同時に指定して、LDAP サービスから収集したユーザ データを追加することができます。

--G

グループの lookaside データベース ファイルの内容を一覧表示します。

--H [IPv4 | IPv6]

ホストの lookaside データベース ファイルの内容を一覧表示します。

-S

サービスの lookaside データベース ファイルの内容を一覧表示します。

-U

ユーザの lookaside データベース ファイルの内容を一覧表示します。

options

ユーティリティが情報を表示する方法を変更する、オプションの修飾子を定義します。以下の 1 つまたは複数の修飾子を指定できます。

--l

リスト ファイルのみを使用して lookaside データベースをロードします。この場合、システムの解決メカニズムは除外されます。

-f

-h スイッチを使用して、lookaside データベース（ホストのみ）を高速でロードします。

詳細情報:

seos.ini 初期設定ファイル (P. 337)

sechkey ユーティリティ

sechkey ユーティリティを使用すると、CA Access Control 暗号化を管理し、CA Access Control での管理上の通信を保護できます。sechkey パラメータを使用するには ADMIN 属性が必要です。

sechkey ユーティリティを使用して対称暗号化用の暗号化鍵を設定し、その鍵を SSL（PKI）暗号化に使用します。

対称鍵を使用する場合は、鍵をデフォルトから変更することをお勧めします。SSL を使用する場合は、証明書および関連付けられた秘密鍵をデフォルトから変更することをお勧めします。

どの暗号化を使用する場合でも、CA Access Control をインストールまたはアップグレードした後に、サイトのすべてのコンピュータ上の鍵を変更します。これにより、権限のないユーザによるシステムへのアクセスを防ぐことができます。

このユーティリティは以下のタスクを処理します。

- 対称暗号化鍵の変更 (P. 134)
- 対称暗号化方式の変更 (P. 136)
- X.509 証明書の設定 (P. 138)
- メッセージ キューのパスワードの変更 (P. 141)

sechkey ユーティリティ - 対称暗号化鍵の変更

sechkey ユーティリティは、CA Access Control プログラムの CA Access Control 対称暗号化鍵を変更します。

このユーティリティは、対話モードまたは非対話モードで実行できます。sechkey を対話モードで実行する場合、古い鍵と新しい鍵の入力を求めるメッセージが表示されます。

sechkey を使用して対称暗号化鍵を変更する前に、CA Access Control を停止する必要があります。sechkey パラメータを使用するには ADMIN 属性が必要です。

重要: 通信の問題を回避するには、CA Access Control コンポーネントを実行するすべてのコンピュータ上で同じ暗号化鍵を使用します。

対話モードでは、このユーティリティを以下の形式で使用します。

```
sechkey
```

非対話モードでは、このユーティリティを以下の形式で使用します。

```
sechkey {oldkey | -d} {newkey | -d} [-s registry_path]
```

sechkey には UNIX コンピュータのみで有効ないくつかの追加スイッチがあります。UNIX コンピュータでは、このユーティリティを以下の形式で使用します。

```
sechkey {oldkey | -d} {newkey | -d | -n} [-nopmd | -r hostname]
```

```
sechkey -k newkey
```

```
sechkey -c
```

-c

（UNIX）selogrd 暗号化鍵を消去します。デフォルトの鍵は鍵ファイルに保存されます。

注: 保存された鍵自体は、デフォルトの暗号化方式で暗号化されます。

-d

デフォルトの CA Access Control キーを指定します。

-k

（UNIX）変更する selogrd 暗号化鍵を指定します。この暗号化鍵は、新しいファイルに保存されるか、または古いファイルで更新されます。

-n

（UNIX）別の鍵に変更せずに、現在の鍵を使用しているプログラムを一覧表示します。

newkey

新しい暗号化鍵を指定します。

--nopmd

（UNIX）Policy Model 更新ファイルを新しい鍵で更新せずに、鍵を変更します。

oldkey

変更する現在の暗号化鍵を指定します。

-r *hostname*

（UNIX）暗号化鍵の変更を行うリモートコンピュータの名前を指定します。

このオプションを使用するには、CA Access Control がローカル コンピュータとリモートコンピュータの両方で実行されている必要があります。このパラメータを指定しても実際には鍵の変更は行われません。代わりに、リモートコンピュータで（seload -c を使用して）CA Access Control を次回起動したときに鍵の変更が行われるように情報が保存されます。

-s *registry_path*

（Windows）CA Access Control プログラムの暗号化鍵が格納されているレジストリのルート パスを指定します。このスイッチは、CA Access Control SDK を使用するサードパーティ プログラムのみで有効です。

例：UNIX コンピュータでデフォルトの暗号化鍵を使用しているかどうかを確認する

以下のコマンドを使用して、UNIX コンピュータがデフォルトの CA Access Control 暗号化鍵を使用しているかどうかを確認します。

```
sechkey -d -n
```

sechkey ユーティリティ - 対称暗号化方式の変更

sechkey ユーティリティは、CA Access Control プログラムの CA Access Control 暗号化鍵を変更します。対称暗号化方式を変更する場合、sechkey は CA Access Control データベース内の暗号化された各パスワードを複合化した後、新しい暗号化方式を使用して各パスワードを暗号化します。

注: CA Access Control が FIPS 専用モードで実行されている場合、対称暗号化方式を変更することはできません。crypto セクションの fips_only 構成トークンの値が 1 の場合、CA Access Control は FIPS のみのモードで動作します。この制限によって、暗号化方式が FIPS 準拠でない暗号化方式に変更されるのを防ぐことができます。

sechkey を使用して対称暗号化鍵を変更する前に、CA Access Control を停止する必要があります。sechkey パラメータを使用するには ADMIN 属性が必要です。

重要: 通信の問題を回避するには、CA Access Control コンポーネントを実行するすべてのコンピュータ上で同じ暗号方式を使用します。

このユーティリティの構文は、以下のようになります。

```
sechkey -m -sym {aes128 | aes192 | aes256 | des | tripledes | default} [-s registry_path]
```

-m

暗号化方式を変更するように指定します。

-s *registry_path*

(Windows) CA Access Control プログラムの暗号化鍵が格納されているレジストリのルート パスを指定します。このスイッチは、CA Access Control SDK を使用するサードパーティ プログラムのみで有効です。

-sym

使用する新しい暗号化方式を指定します。

aes128

以下の暗号化方式を使用するように指定します。

(Windows): aes128enc.dll

(UNIX): libaes128.so

aes192

以下の暗号化方式を使用するように指定します。

（Windows）：aes192enc.dll

（UNIX）：libaes192.so

aes256

以下の暗号化方式を使用するように指定します。

（Windows）：aes256enc.dll

（UNIX）：libaes256.so

des

以下の暗号化方式を使用するように指定します。

（Windows）：desenc.dll

（UNIX）：libdes.so

tripledes

以下の暗号化方式を使用するように指定します。

（Windows）：tripledesenc.dll

（UNIX）：libtripledes.so

デフォルト

以下の CA Access Control 専用の暗号化方式を使用するように指定します。

（Windows）：defenc.dll

（UNIX）：libscramble.so

例：対称暗号化方式を AES256 に変更する

以下のコマンドは、対象暗号化方式を AES256 に変更します。

```
sechkey -m -sym aes256
```

詳細情報：

ChangeEncryptionMethod ユーティリティ - 暗号化方式の変更 (P. 33)

sechkey ユーティリティ - X.509 証明書の設定

sechkey ユーティリティは、コンポーネント間の通信を認証するために CA Access Control が使用するルートとサーバの証明書を設定します。

sechkey ユーティリティを使用すると、以下のタスクを実行できます。

- OU パスワード保護されている証明書が含む、サードパーティのルートおよびサーバ証明書を使用する CA Access Control の設定
- サードパーティのルート証明書からのサーバ証明書の作成
- コンピュータ上のパスワード保護されている証明書のパスワードの保存

X.509 証明書を設定するには、sechkey を使用する前に、CA Access Control を停止する必要があります。sechkey パラメータを使用するには ADMIN 属性が必要です。

注: CA Access Control が FIPS のみのモードで動作している場合、パスワード保護されている証明書を使用することはできません。crypto セクションの fips_only 構成トークンの値が 1 の場合、CA Access Control は FIPS のみのモードで動作します。この制限によって、FIPS に準拠していない方式を使用した証明書内でパスワードを暗号化しないようにします。

X.509 ルートまたはサーバ証明書を作成するには、このコマンドを以下の形式で使用します。

```
sechkey -e {-ca|-sub [-priv privfilepath]} [-in infilepath] [-out outfilepath]
[-capwd password] [-subpwd password]
```

OU パスワード保護されているサーバ証明書を使用するには、このコマンドを以下の形式で使用します。

```
sechkey -g {-subpwd password | -verify}
```

-ca

sechkey によって自己署名証明書が作成されるように指定します。この証明書は CA (ルート) 証明書として使用されます。

sechkey は、crypto セクションの ca_certificate 設定で定義されている PEM ファイルに証明書と秘密鍵を格納します。

-capwd *password*

sechkey がサーバ (所有者) 証明書の生成に使用するルート証明書の秘密鍵のパスワードを指定します。

-e

sechkey によって X.509 証明書が作成されるように指定します。

-g

CA Access Control でサードパーティのサーバ証明書を使用するように指定します。crypto セクションの subject_certificate 設定で指定された場所にサードパーティ のサーバ証明書を保存するか、crypto セクションの subject_certificate 設定の値を編集してサードパーティのサーバ証明書へのパスを指定します。

注: 新規ディレクトリにサーバ証明書をインストールした場合は、新規ディレクトリを保護する CA Access Control ファイル ルールを作成する必要があります。

-in *infilepath*

証明書情報を含む入力ファイルを指定します。-in を指定しない場合、sechkey によって標準入力から情報が読み取られます。

sechkey で証明書を作成するには、以下の情報が必要です。

- シリアル番号
- 所有者
- NOTBEFORE（証明書の有効開始日）
- NOTAFTER（証明書の有効終了日）

sechkey では、以下の情報も使用できますが、必須情報ではありません。

- E-MAIL（電子メール）
- URI （通常は URL と呼ばれます）
- DNS 名
- IP アドレス

-out *outfilepath*

証明書情報を記録する出力ファイルを指定します。出力ファイルは入力情報のコピーです。-out を指定しない場合、sechkey では入力情報が複製されません。

-priv *privfilepath*

証明書に関連付けられた秘密鍵を保持するファイルを指定します。このオプションは、-sub オプションと同時に使用した場合にのみ有効になります。

-sub

sechkey によってサーバ(所有者)証明書が作成されるように指定します。

sechkey は、crypto セクションの subject_certificate 設定で定義されている PEM ファイルに証明書と秘密鍵を格納します。

-priv を指定しない場合、crypto セクションの private_key 設定は、この証明書に関連付けられた秘密鍵を保持するファイルを定義します。

パスワード保護されているサーバ証明書を作成する場合、sechkey は証明書を暗号化しません。パスワード保護されていないサーバ証明書を作成する場合、sechkey は AES256 および CA Access Control 暗号化鍵を使用して証明書を暗号化します。

-subpwd *password*

サーバ(所有者)証明書の秘密鍵のパスワードを指定します。sechkey は *ACInstallDir*/Data/crypto ディレクトリにある crypto.dat ファイルにパスワードを格納します。この *ACInstallDir* は CA Access Control をインストールしたディレクトリです。crypto.dat ファイルは非表示であり、暗号化された読み取り専用のファイルです。また、CA Access Control によって保護されます。CA Access Control が停止されている場合、スーパーユーザのみがパスワードにアクセスできます。

-verify

パスワード保護されているサーバ キーを開くために、CA Access Control が保存されたパスワードを使用できることを確認します。

例: OU パスワード保護されたサードパーティのルート証明書からサーバ証明書を作成する

以下のコマンドでは、以下の値を使用して OU パスワード保護されたサードパーティのルート証明書からサーバ証明書を作成します。

- 証明書情報を含む入力ファイルへのパスは、「C:¥Program Files¥CA¥AccessControl¥data¥crypto¥sub_cert_info」です。
- ルート証明書の秘密鍵へのパスは、「C:¥Program Files¥CA¥AccessControl¥data¥crypto¥ca.key」です。
- ルート証明書の秘密鍵のパスワードは、「P@ssw0rd」です。

```
sechkey -e -sub -in "C:¥Program Files¥CA¥AccessControl¥data¥crypto¥sub_cert_info"
-priv "C:¥Program Files¥CA¥AccessControl¥data¥crypto¥ca.key" -capwd P@ssw0rd
```

例: 入力ファイル

証明書情報を含む入力ファイルの例を以下に示します。

```
SERIAL: 00-15-58-C3-5E-4B
SUBJECT: CN=192.168.0.1
NOTBEFORE: “12/31/08”
NOTAFTER: "12/31/09"
E-MAIL: john.smith@example.com
URI: http://www.example.com
DNS: 168.192.0.100
IP:  168.192.0.1
```

sechkey ユーティリティ - メッセージ キューのパスワードの変更

sechkey ユーティリティでは、メッセージ キューのパスワードを変更することができます。クライアントまたはサーバのメッセージ キューのパスワードを変更できます。

sechkey パラメータを使用するには ADMIN 属性が必要です。

このコマンドの形式は以下のようになります。

```
sechkey -t [-server] -pwd password
```

-t

メッセージ キューのパスワードを変更するように指定します。

-server

サーバ メッセージ キューのパスワードを変更するように指定します。

注: このパラメータを指定しない場合、sechkey はクライアント メッセージ キューのパスワードを変更します。

-pwd *password*

新しいパスワードを定義します。

詳細情報:

acuxchkey Utility-暗号化鍵の設定変更 (P. 32)

seclassadm ユーティリティ - CA Access Control クラスの管理

seclassadm ユーティリティは、CA Access Control クラスを管理します。seclassadm は、ローカル データベースに新しいユーザ定義クラスを追加します。seclassadm は、CA Access Control が実行中でないときに、データベースが格納されているディレクトリから（または -p オプションを使用して）起動します。

注: seclassadm の実行により、新しいクラスの情報を含むファイルが seosdb ディレクトリに作成されます。dbmgr -c を指定して新しいデータベースを作成するときに、seos.ini ファイルの CreateNewClasses が「yes」（デフォルト）に設定されている場合は、ユーザ定義クラスが新しいデータベースに作成されます。

このコマンドの形式は以下のようになります。

```
seclassadm -add className [-a access] [{-|+}c] [-d access] ¥
    [-f] [-g] [-o] [-p db_pathname] [-t]

seclassadm -del className

seclassadm -upd className {-|+}c [-p db_pathname]
```

-add *class-name*

既存のデータベースに新しいリソース クラスを追加します。この *class-name* は新しいクラスの名前です。

CA Access Control では、クラス名は大文字で予約されています。クラスを追加する場合は、小文字を最低 1 つ使用します。最大 79 文字のクラス名を指定できます。

新しいクラスを作成した後に、selang の setoptions コマンドを実行してクラスを有効にする必要があります。

-del *class-name*

指定されたリソース クラスをデータベースから削除します。

-upd *class-name*

指定されたリソース クラスをデータベースで更新します。

-a *access*

クラスのアクセス モードを指定します。文字列 *access* は、許可されるアクセスを表します。各アクセスモードは、任意の順序で示される 1 文字のコードで表されます。文字列には空白または英字以外の文字を使用できません。有効なアクセス モードは以下のとおりです。

省略形	説明
C	control
D	delete
E	create
F	ファイル スキャン
M	chmod
O	chown
R	読み取り
S	セキュリティ
T	utime
U	更新
V	rename
W	write
X	execute

-d *access*

クラスのデフォルトのアクセス モードを指定します。アクセス権限を指定せずに authorize コマンドを実行した場合に、CA Access Control によってユーザに割り当てられるアクセス モードです。authorize コマンドで使用されるこの暗黙的なアクセスは、リソースに割り当てられるデフォルトのアクセスとは異なります。使用可能なアクセス モードは、-a オプションで一覧表示されます。

-f

新しいクラス名がすべて大文字の場合でも、CA Access Control で使用できるように指定します。

注: seclassadm ユーティリティでは、すべて大文字のクラス名の作成はデフォルトで許可されていません。CA Access Control のすべて大文字の名前は、定義済みの CA Access Control クラスに予約されています。

--g

新しいクラスを、既存のクラスのメンバをグループ化するリソースとして指定します。既存のクラスと新しいグループ クラスの関係は、データベースの任意のクラスとそのグループ クラス（TERMINAL と GTERMINAL など）の関係と同じです。既存のクラスのメンバをグループ化するリソースは、大文字の G で始まる必要があります。つまり、名前は既存のクラスと同じですが、プレフィクス *G* で始まります。

-o

新しいクラスの *_default* レコードを作成し、そのデフォルト アクセスを設定します。

-p *db_pathname*

ローカル データベースの完全パス名を指定します。

デフォルトでは、seclassadm ユーティリティは、現在のディレクトリ内のデータベースで動作します。このオプションを使用して、データベースが配置されているディレクトリ以外のディレクトリを定義します。

--t

このクラスが Unicenter TNG クラスであることを指定します。

例: データベースへの新しいクラスの追加

以下の例は、seclassadm ユーティリティを使用してデータベースにクラスを追加する方法を示しています。

- *dbfield* という名前のリソース クラスを追加するには、以下のコマンドを使用します。

  ```
  seclassadm -add dbfield
  ```

- READ アクセス権限のみを割り当てた *report* という名前のリソース クラスを追加するには、以下のコマンドを使用します。

  ```
  seclassadm -add report -d R -a R
  ```

- READ、WRITE、および MODIFY アクセス権限を割り当てた *batch_jobs* という名前のリソース クラスを追加し、指定がない場合のデフォルトとして READ アクセス権限を指定するには、以下のコマンドを使用します。

  ```
  seclassadm -add batch_jobs -d R -a RWM
  ```

- オブジェクトが DEPTA クラス内にあるリソースのグループである新しいクラスを、execute アクセス権限および暗黙的な execute アクセス権限付きで追加するには、以下のコマンドを使用します。

  ```
  seclassadm -add DEPTA -d X -a X -g -f
  ```

secompas ユーティリティ - パスワードの比較

UNIX で該当

secompas ユーティリティは、CA Access Control データベースのパスワードを UNIX のパスワード ファイル内のパスワードと比較します。

secompas ユーティリティは、CA Access Control データベースのユーザごとに 1 行を出力します。この行には、ユーザ名、およびそのユーザが UNIX で定義されているかどうか、CA Access Control のパスワードを持っているかどうか、またはパスワードが一致するかどうかを示すメッセージが含まれます。secompas ユーティリティでは、比較したユーザの総数およびパスワードが一致しないユーザの数も表示されます。パスワードが両方の環境に存在し、それらのパスワードが一致しない場合にのみ、総数が追加されます。一方の環境でユーザが定義されていない場合や、一方の環境にパスワードが存在しない場合、不一致パスワードの件数は追加されません。

secompas ユーティリティでは、パスワードを比較するために、/etc/passwd ファイル、shadow password ファイル、および NIS/NIS+ パスワード マップが使用されます。

注: secompas ユーティリティを使用するには、ADMIN 属性を持っている必要があります。

このコマンドの形式は以下のようになります。

```
secompas [-db] [-ok] [-ux]
```

-db

CA Access Control データベースにパスワードを持っていないユーザを表示しないように指定します。

-h

このユーティリティのヘルプ画面を表示します。

-ok

CA Access Control データベースと UNIX で同じパスワードを持っている(パスワード一致)ユーザを表示しないように指定します。

-ux

UNIX に存在しないユーザを表示しないように指定します。

例: ユーティリティの出力

以下の例では、secompas ユーティリティのサンプル出力を示します。

```
Checking root           : No password in Access Control database.
Checking tst_001        : Undefined in UNIX.
Checking tst_002        : No password in UNIX password file
Checking tst_003        : *** PASSWORDS DO NOT MATCH. ***
Checking tst_004        : *** NO MATCH - UNIX DISABLED ***
Checking tst_005        : OK

Total of 6 users found in database.
2 unmatched password(s) found. (1 UNIX DISABLED).
```

上記の出力の各行について、以下で説明します。

```
Checking root           : No password in Access Control database.
```

root ユーザは CA Access Control データベースに定義されていません。または、ユーザは CA Access Control データベースに定義されていますがパスワードがありません。

```
Checking tst_001        : Undefined in UNIX.
```

ユーザ tst_001 は CA Access Control データベースに定義されていますが、UNIX には定義されていません。

```
Checking tst_002        : No password in UNIX password file
```

ユーザ tst_002 は UNIX に定義されていますが、パスワードがありません。

```
Checking tst_003        : *** PASSWORDS DO NOT MATCH. ***
```

CA Access Control パスワードが、ユーザ tst_003 の UNIX パスワードと一致していません。

```
Checking tst_004        : *** NO MATCH - UNIX DISABLED ***
```

UNIX 環境の tst_004 ユーザ アカウントが無効でした。secompas では、/etc/passwd ファイルにあるパスワードの前のアスタリスク(*)によって、無効なユーザ アカウントが識別されます。

```
Checking tst_005        : OK
```

CA Access Control のパスワードが、ユーザ tst_005 の UNIX のパスワードと一致しています。

secons ユーティリティ

secons ユーティリティは、CA Access Control のセキュリティ コンソールです。sepmd ユーティリティを使用すると、以下のタスクを実行できます。

- UNIX の場合
  - 実行時の統計情報の表示 (P. 164)
  - 同時ログイン オプションの管理 (P. 154)
  - CA Access Control トレースの管理 (P. 152)
  - リソース キャッシュ機能の管理 (P. 155)
  - CA Access Control の停止の管理 (P. 149)
  - 構成設定の再ロード (P. 182)
  - XUSER オブジェクトの削除 (P. 161)
  - カーネル テーブルの表示 (P. 169)
  - カーネル キャッシュ テーブルの消去、有効化、無効化 (P. 180)
- Windows の場合
  - 計測ランタイム設定の制御 (P. 182)
  - 実行時の統計情報の表示 (P. 167)
  - ACEE レコードの表示 (P. 162)
  - 同時ログイン オプションの管理 (P. 154)
  - CA Access Control トレースの管理 (P. 152)
  - ネットワーク リソースの IP アドレスの更新 (P. 181)
  - XUSER オブジェクトの削除 (P. 161)
  - 再利用されたアカウントの解決 (P. 164)
  - CA Access Control の停止 (P. 161)
  - ユーザ名およびセキュリティ クレデンシャルの表示 (P. 185)

secons ユーティリティは、セキュリティ管理者でも、その他のユーザでも使用できます。ただし、ADMIN 属性を持たないユーザは、一部のオプションのみを使用できます。使用できるオプションを以下に示します。

-m（トレース管理）、-d-、-d+、-ds（ログイン管理）、および -whoami（ユーザのクレデンシャル）

secons ユーティリティ - UNIX での CA Access Control の停止

UNIX で該当

secons ユーティリティは、CA Access Control および関連付けられているデーモンを停止します。secons ユーティリティを使用して、CA Access Control コードを実行中のプロセスを確認できます。

CA Access Control を停止できるのは、ADMIN または OPERATOR として定義されたユーザのみです。リモート コンピュータ上の CA Access Control を停止できるのは、そのリモート コンピュータで ADMIN または OPERATOR として定義されたユーザのみです。

このコマンドの形式は以下のようになります。

```
secons [-s [hosts | ghosts]] ¥
    [-S [{selogrd | selogrcd | serevu}]] ¥
    [-sc] [-scl] [-sk]
```

-s [*hosts* | *ghosts*]

スペース区切りリストで定義されたリモート ホスト上の CA Access Control デーモンを停止します。ホストを指定しない場合、CA Access Control はローカル ホスト上のサービスを停止します。

ghost レコードの名前を入力することで、ホスト グループを定義できます。このオプションをリモート端末から使用する場合は、ユーティリティによってパスワードの検証が要求されます。また、リモート コンピュータとローカル コンピュータの管理者権限、およびローカル コンピュータでのリモート ホスト データベースに対する書き込み権限も必要です。

-S [{selogrd | selogrcd | serevu}]

デーモンを定義していない場合は、CA Access Control デーモンを停止し、アクティブなデーモン（selogrd、selogrcd、および serevu）の停止を試みます。seos.ini ファイルの [daemons] セクションの selogrd、selogrcd、または serevu の各トークンが *yes* に設定されている場合、CA Access Control がすでに停止していると、実行中の CA Access Control のメイン デーモンに終了要求が送信されるか、または指定されたデーモンに終了シグナルが送信されます。

デーモンを定義している場合、secons は CA Access Control デーモンを停止しません。seos.ini ファイルの [daemons] セクションの該当するトークンが *yes* に設定されている場合、CA Access Control が停止していると、実行中の CA Access Control のメイン デーモンに終了要求が送信されるか、またはそのデーモンに終了シグナルが送信されます。

-sc[l]

CA Access Control コードを実行中のプロセスを表示します。

CA Access Control 上にロードされているアプリケーションに、CA Access Control によってフックされるオープン システム コール（syscall）がある場合は、CA Access Control をアンロードできません。CA Access Control コードを実行中のプロセスを確認した後、これらのプロセスを停止し、CA Access Control カーネル モジュールをアンロードできます。UNIX exit を使用すると、カーネルのアンロード前にこれらのプロセスを自動的に停止してから、カーネルのアンロード後に自動的に再起動できます。

-sc 出力は 2 列のテーブルとして表示されます。1 列目にはシステム コール番号が、2 列目にはプロセス識別子が表示されます。

-scl オプションでは、CA Access Control コードを実行中のプロセスに関して、親プロセス ID（PPID）、UID、時刻、およびプログラム名の情報も示されます。時刻情報により、そのプロセスが CA Access Control をフックしている時間を確認できます。この時間が比較的短い場合、フックは一時的なものと考えることができます。

また、CA Access Control の実行中にこのコマンドを実行すると、アンロードの問題を引き起こす原因を事前に予測するのに役立ちます。ただし、accept コマンドなどでは、CA Access Control コードによってアンロード中にフックが削除される場合があります。これは、CA Access Control の実行中にアクティブなフックが見つかった場合でも、実際にはアンロードに影響しないことがあることを意味します。

注: デフォルトでは、CA Access Control は CA Access Control によってインターセプトされるシステム コールを監視します。CA Access Control がシステム コールを監視しないようにするには、seos.ini ファイルの syscall_monitor トークンを 0（無効）に設定する必要があります。

-sk

すべての CA Access Control デーモンを停止し、CA Access Control カーネル拡張機能をアンロードする準備を行います。

例: CA Access Control の停止

- CA Access Control デーモンを停止するには、以下のように入力します。

  ```
  secons -s
  ```

- リモート ホスト HOST1 および HOST2 上の CA Access Control デーモンを停止するには、以下のように入力します。

  ```
  secons -s HOST1 HOST2
  ```

例: CA Access Control コードを実行中のプロセスに関する情報の表示

- CA Access Control コードを実行中のプロセスに関する基本情報を表示するには、以下のように入力します。

  ```
  secons -sc
  ```

  出力は以下のようになります。

  ```
  CA Access Control secons vX.X.X.xxx - Console utility
  Copyright (c) YYYY CA. All rights reserved.
  Active system calls:

  syscall    5 - PID:  27477
  ```

- CA Access Control コードを実行中のプロセスに関する詳細情報を表示するには、以下のように入力します。

  ```
  secons -scl
  ```

  出力は以下のようになります。

  ```
  CA Access Control secons vX.X.X.xxx - Console utility
  Copyright (c) YYYY CA. All rights reserved.
  Active system calls:

  -Syscall  102 - PID:   2105  PPID:     1 UID:     0 TIME:    4d-4h PROGRAM NAME:
  /usr/sbin/vsftpd
   Syscall    5 - PID:  24269  PPID:   4289 UID:     0 TIME:   2d-21h PROGRAM NAME:
  /bin/bash
  ```

  出力行の先頭のダッシュ(-)は、アンロード時にこのフックによって問題が発生する可能性は低いと CA Access Control が評価していることを意味します。このコマンドを使用する場合、CA Access Control は CA Access Control のアンロードが成功する可能性が高いかどうかを記録する監査ログに行を追加します。たとえば、secons -scl を実行したときに、CA Access Control のアンロードを妨げる可能性があるシステム コールが少なくとも 1 つ存在する場合、以下の監査ログ レコードが作成されます。

  ```
  10 Nov 2008 05:47:22 F CHECK      root      Scan     339  0 SEOS_syscall    unload
  ```

secons ユーティリティ - CA Access Control トレースの管理

secons ユーティリティは、CA Access Control トレースを管理します。トレースを利用すると、オペレーティング システムのイベントを監視できます。CA Access Control によって、オペレーティング システムのイベントをレポートするメッセージがファイルに蓄積され、後で表示できます。

このコマンドの形式は以下のようになります。

```
secons [-t+] [-t-] [-tt] [-ts] [-tc] [-tv [size] [-file fileName]]
```

```
secons -m message
```

```
secons -pupm trace {enable | disable | clear}
```

-m *message*

テキスト メッセージをトレース ファイルに追加します。

-t+

トレースを有効にします。これにより、CA Access Control エンジンである seosd は、その操作およびアクションを指定するメッセージをトレース ファイルにダンプします。

--t-

トレースを無効にします。これにより、CA Access Control エンジンである seosd は、トレース ファイルへのメッセージのダンプを停止します。

-tc

トレース ファイルからすべてのレコードを削除してトレース ファイルの内容を消去します。

注: このオプションは、seosd が実行中かどうかに関係なく使用できます。

-ts

現在のトレース ステータスを表示します。

-tt

トレース ステータスを切り替えます。

-tv [*size*] [-file *fileName*]

リアルタイム トレースの出力を表示します。secons ユーティリティは、トレース ファイルの最後の *size* KB（デフォルトは 2 KB）を表示し、セッションを開いたままにすることで、ファイルに追加された新しいトレース メッセージが表示されるようにします。このユーティリティは、UNIX の tail -f コマンドと似ています。

Ctrl + C キーを使用して、この操作を停止します。

注: このオプションは、seosd が実行中かどうかに関係なく使用できます。full_year 構成設定を使用して、年の表示を 4 桁（デフォルト。yes で設定）とするか下 2 桁とするかを選択できます。

size

表示するファイル部分のサイズ（KB）を、その部分の終端から指定します。トレース ファイル全体を表示するには、0 を指定します。このオプションを指定しない場合、デフォルトの 2 KB が使用されます。

-file *fileName*

ACInstallDir/log/seosd.trace ではなく、*fileName* を読み取ります。

-pupm trace {enable | disable | clear}

特権ユーザ パスワード管理 エージェントに有効

ランタイム中に 特権ユーザ パスワード管理 エージェント上でトレース オプションを指定します。トレース オプションを変更するために CA Access Control を再起動する必要はありません。

制限: 「enable」はトレースを有効にします。「disable」はトレースを無効にします。「clear」はトレース ファイルをクリアします。

重要: 指定するトレース オプションは現在のセッションのみに適用されます。CA Access Control 再起動の後、トレース オプションは PUPMAgent セクション内の OperationMode トークンに従って設定されます。

secons ユーティリティ - 同時ログイン オプションの管理

secons ユーティリティは、同時ログイン オプションを管理します。ユーザが 2 回以上ログインすることを回避するように CA Access Control を構成できます。これにより、すでにログインしているユーザのアカウントで外部からの侵入者がログインすることを防止できます。

このコマンドの形式は以下のようになります。

```
secons [-d+] [-d-] [-ds] [-l+] [-l-] [-ls] ¥
       [-u+ userName] [-u- userName] [-us userName]
```

-d+

コマンドを実行しているユーザに対して同時ログインを有効にします。

-d-

コマンドを実行しているユーザに対して同時ログインを無効にします。このコマンドを使用すると、ローカル コンピュータに対するユーザの同時ログインがすべて無効になります。

注: このコマンドをユーザの .login ファイルまたは .cshrc ファイルに指定して、同時ログインを無効にすることもできます。

-ds

コマンドを実行しているユーザの同時ログイン設定内容を表示します。

-l+

システム全体で同時ログインを有効にします。

注: デフォルトでは、ログインは有効に設定されます。ただし、メンテナンスのためにシステムを停止する必要がある場合は、指定した期間ログインを無効にできます。

--l-

システム全体で同時ログインを無効にします。

-ls

システム全体のログイン ステータス。

-u+ *userName*

定義されたユーザの同時ログインを有効にします。

-u- *userName*

定義されたユーザの同時ログインを無効にします。

-us *userName*

定義されたユーザの同時ログイン設定内容を表示します。

secons ユーティリティ - UNIX でのリソース キャッシュ機能の管理

UNIX で該当

secons ユーティリティは、UNIX 上でリソース キャッシュ機能（ファイル キャッシュ）を管理します。キャッシュ、つまり実行時テーブルには、FILE クラスのリソースについての承認要求に対する以前の応答（許可または拒否）が「記憶」されます。同じ承認が要求されると、その要求はキャッシュ メモリ テーブル内に格納された前回の応答を使用して回答されます。

このコマンドの形式は以下のようになります。

```
secons [-C+] [-C-] [-CA value] [-CC interval] [-CD] ¥
    [-CF value] [-CI init_value] [-CP interval] -CU value]
```

--C+

ファイル認証のキャッシュを有効にします。

-C-

ファイル認証のキャッシュを無効にします。

-CA *value*

テーブル内の認証レコードの最大数を指定します。

デフォルト: 80

制限: 1 ～ 800 の数値

-CC *interval*

キャッシュを消去する間隔（分単位）を指定します。

デフォルト: 60

制限: 0 より大きい数値

--CD

キャッシュ テーブルは標準出力に表示されます。

-CF *value*

テーブル内のファイル レコードの最大数を指定します。

デフォルト: 20

制限: 1 ～ 200 の数値

-CI *init_value*

キャッシュ テーブル内の新規レコードの優先順位の初期値を指定します。

デフォルト: 10

-CP *interval*

キャッシュでの優先順位を付け替える間隔を指定します。

デフォルト: 1（1 レコード）

制限: 1 ～ 10 の数値

-CU *value*

テーブル内のユーザ レコードの最大数を指定します。

デフォルト: 50

制限: 1 ～ 500 の数値

例: キャッシュ設定の変更

以下の例は、キャッシュ内のファイル レコード、ユーザ レコード、および認証レコードの最大数が 60 になるようにキャッシュ設定を変更する方法を示しています。

```
secons -CF 60 -CU 60 -CA 60
```

例: キャッシュ テーブルの表示

以下の例は、secons -CD コマンドの出力を示しています。

```
================================================================================
        FILE CACHE (configuration, statistics, and dispatcher data)
--------------------------------------------------------------------------------
sizes(bytes)       tables:                | max records:      | intervals
cache   head      files    users    auth  | files users auths |clean prio
--------------------------------------------------------------------------------
40244    44        5600     4200    30400 |  20    50    80   |   60   1
================================================================================
table  |statistics        | priority    |min | rec  | average      |pri |init
name   |  hits misses (ok)| maxim  minim|ind | used | usage   life |fact|prio
--------------------------------------------------------------------------------
files  |    5     1   83% |   0      0  |  0 |   1  |              |    |
users  |    5     1   83% |  10      2  |  0 |   1  |  0       0   |  1 | 10
auths  |    4     2   66% |   2         |  0 |   2  |              |    |
================================================================================
FILE TABLE
--------------------------------------------------------------------------------
No  type    pid priority user                                  file name
--------------------------------------------------------------------------------
0   EXPL    372      0    0                                      /etc/shadow
================================================================================
USER TABLE
--------------------------------------------------------------------------------
No   user name     prio   life   used   UID  EUID  RUID auth prev(file)next
--------------------------------------------------------------------------------
0    root           2       2      7     0    0     0    0    50(   0)  50
================================================================================
AUTHORIZATION RESULT TABLE  (R - Result: 'P'-permit, 'D'-deny ...)
--------------------------------------------------------------------------------
No  R ACEE acc  Log stage prv(usr)nxt time       terminal  program
--------------------------------------------------------------------------------
0   P   6  read  0  00036 80(  0)  1   07:48:25            /usr/bin/login
================================================================================
```

上記の出力について、以下で説明します。

この出力は、以下に示す 5 つの部分で構成されています。

- キャッシュの構成。含まれるフィールドは以下のとおりです。
  - キャッシュのサイズ（バイト単位）
  - キャッシュ ヘッダのサイズ（バイト単位）
  - ファイル テーブルのサイズ（バイト単位）
  - ユーザ テーブルのサイズ（バイト単位）
  - 結果テーブルのサイズ（バイト単位）
  - ファイル レコードの最大数
  - ユーザ レコードの最大数
  - 結果レコードの最大数
  - 統計情報：テーブルでのヒット数
- ファイル レコードのテーブル。含まれるフィールドは以下のとおりです。
  - レコードのシーケンス番号
  - ファイルの種類（EXPLICIT、IMPLICIT）
  - プロセス ID 番号
  - レコードの優先順位（ユーザの優先順位値の合計）
  - ユーザのテーブルで対応するユーザ レコード番号
  - ファイルの名前

- ユーザのテーブル。含まれるフィールドは以下のとおりです。
  - レコードのシーケンス番号
  - ユーザ名
  - レコードの優先順位
  - レコードの有効期限のカウンタ
  - レコードの使用カウンタ
  - ユーザ ID、実効ユーザ ID、セキュリティ ID によって実際に使用される ID（実 UID）
  - 認証テーブルで対応する認証レコード番号
  - ユーザ チェーンの前のユーザ レコード番号
  - 対応するファイル レコード番号
  - ユーザ チェーンの次のユーザ レコード
- 認証結果のテーブル。含まれるフィールドは以下のとおりです。
  - Terminal
  - 段階
  - 許可段階
  - 結果 - 認証結果（P または D）
  - ACEE 番号
  - アクセス タイプ
  - ログ記録オプションのフラグ値
  - 決定が行われた段階の番号
  - レコード チェーンの前の認証レコード番号
- 対応するユーザ レコード番号
  - レコード チェーンの次の承認レコード番号
  - 統計情報: テーブルに存在しないレコード数
  - 承認クラス
  - （via パラメータで指定した）プログラム名
  - 通知文字列
  - 更新時刻（GMT）

- ディスパッチャのデータ。含まれるフィールドは以下のとおりです。
  - 統計情報: テーブルに存在しないレコード数
  - 統計情報: テーブルでのヒット数
  - テーブル内の最大優先順位
  - テーブル内の最小優先順位
  - 最小優先順位を持つエントリ数
  - 使用されたレコード数
  - 平均使用状況(ユーザ テーブルの場合のみ)
  - 平均有効期間(ユーザ テーブルの場合のみ)
  - 優先順位の算出要因(ユーザ テーブルの場合のみ)
  - レコードの優先順位の初期値(ユーザ テーブルの場合のみ)

secons ユーティリティ - Windows での CA Access Control の停止

Windows で該当

secons ユーティリティは、CA Access Control エンジン、およびローカル端末上または 1 つ以上のリモート端末上にあるその他のすべての CA Access Control サービスを停止します。

CA Access Control を停止できるのは、ADMIN または OPERATOR として定義されたユーザのみです。リモート コンピュータ上の CA Access Control を停止できるのは、そのリモート コンピュータで ADMIN または OPERATOR として定義されたユーザのみです。

このコマンドの形式は以下のようになります。

```
secons -s [hosts | ghosts]
```

-s [*hosts* | *ghosts*]

スペース区切りで定義された複数のリモート ホスト上の CA Access Control サービスを停止します。ホストを指定しない場合、CA Access Control はローカル ホスト上のサービスを停止します。

ghost レコードの名前を入力することで、ホスト グループを定義できます。このオプションをリモート端末から使用する場合は、ユーティリティによってパスワードの検証が要求されます。また、リモート コンピュータとローカル コンピュータの管理者権限、およびローカル コンピュータでのリモート ホスト データベースに対する書き込み権限も必要です。

secons -dbclean - CA Access Control データベースからの XUSER オブジェクトの削除

secons ユーティリティは、CA Access Control データベースからネイティブ セキュリティ識別子（SID）に解決されない XUSER オブジェクトを削除します。すでにネイティブ環境に存在しない XUSER オブジェクトを削除するには、secons -dbclean コマンドを使用します。

このコマンドの形式は以下のようになります。

```
secons –dbclean <osuser>
```

-dbclean

CA Access Control データベースから解決されない XUSER オブジェクトをすべて削除するように指定します。

<osuser>

ネイティブ ユーザ アカウント名を指定します。

secons -acee 機能 - Windows での ACEE レコードの表示

Windows で該当

secons ユーティリティを使用すると、認証エンジンでアクセサをキャッシュする ACEE（アクセサ エレメント エントリ）テーブルを監視できます。ACEE には、以下のユーザに関する情報が格納されています。

- **ログインしたユーザ** - オペレーティング システムにログインしたユーザです。このタイプのユーザには、以下の ACEE 属性を指定します。
  - ログイン セッション ID
  - ログイン セッション タイプ
- **管理ユーザ** - LCA 接続を使用して、CA Access Control 管理アプリケーションにログインしたユーザです。例: selang
- **Authorization API ユーザ** - SEOSROUTE_* API で参照されるユーザです。
- **SPECIALPGM 論理ユーザ** - 1 つ以上の SPECIALPGM レコードで参照されるユーザです。このタイプのユーザ用の特別な ACEE 属性を以下に示します。
  - SPECIALPGM レコードと関連付けられた ACEE
- **組み込みユーザ** - CA Access Control に組み込まれているユーザです。例: *_undefined*

注: CA Access Control 管理者のみが、このコマンドを使用できます。

このコマンドの形式は以下のようになります。

```
secons -acee [handle | all | list]
```

all

すべての ACEE レコードを表示します。

handle

表示する ACEE ハンドルを定義します。

list

すべての ACEE レコードの（詳細情報が含まれない）サマリリストを表示します。

例: ACEE レコードの表示

- 以下の例は、ACEE のハンドル リストを表示します。

  ```
  secons -acee list
  ```

  secons の出力は、以下のようになります。

  ```
  ACEE handle '0' represents 'Logged on User': NT AUTHORITY¥ANONYMOUS LOGON (OS
  User)
  ACEE handle '1' represents 'Logged on User': NT AUTHORITY¥NETWORK SERVICE (OS
  User)
  ACEE handle '2' represents 'Logged on User': COMP1-SRV-X86¥John
  ACEE handle '3' represents 'Logged on User': NT AUTHORITY¥LOCAL SERVICE (OS User)
  ACEE handle '4' represents 'Logged on User': NT AUTHORITY¥SYSTEM (OS User)
  ACEE handle '5' represents 'Management User': COMP1-SRV-X86¥John
  ACEE handle '6' represents 'SPECIALPGM Logical User': logicaluser
  ```

- 以下の例は、ACEE のハンドル 6 を表示します。

  ```
  secons -acee 6
  ```

  secons の出力は、以下のようになります。

  ```
  ACEE handle '6' represents 'SPECIALPGM Logical User': logicaluser
  ACEE was created at: Wed Feb 20 17:35:52 2008
  ACEE was last accessed at: Wed Feb 20 17:35:52 2008
  ACEE user role is: Regular
  ACEE audit mode is: Failure, Login Success, Login Failure; Originated from User
  definition
  ACEE user is a member of 0 'CA Access Control' groups
  ACEE user is associated with 1 SPECIALPGM records
      1. C:¥WINDOWS¥system32¥calc.exe
  ```

secons -checkSID 機能 - Windows での再使用されたアカウントの解決

Windows で該当

secons ユーティリティは、各企業アカウント(XUSER および XGROUP リソース)のセキュリティ識別子(SID)を、ネイティブ Windows アカウント SID と比較し、再使用されたアカウントのバックアップを作成します。CA Access Control での認証は SID に基づいており、CA Access Control アクセサリソースの SID はネイティブ アカウント SID(再使用されたアカウント)とは異なります。このため、secons ユーティリティは、新しいアカウント(古いアカウントと同じ名前を持つ)を作成し、命名規則 *SID* (*accountName*) を使用して古いリソースをバックアップします。

注: 再使用された企業ストア アカウントの詳細については、「*Windows エンドポイント管理ガイド*」を参照してください。

このコマンドの形式は以下のようになります。

```
secons -checkSID {-groups | -users} [accountName [,accountName...]]
```

-groups

secons が企業グループ レコードを確認するように指定します。

-users

secons が企業ユーザ レコードを確認するように指定します。

accountName

secons が検索するユーザまたはグループの名前を指定します。*accountName* を省略した場合、secons はすべてのグループまたはユーザを検索します。

secons -i 機能 - UNIX での実行時の統計情報の表示

UNIX で該当

secons ユーティリティは、システムの動作に関する CA Access Control 実行時の統計情報を表示します。この情報を使用して、ネットワーク接続要求、監査およびエラー ログ キューのサイズ、キャッシュされたテーブルのサイズ、データベースのサイズ、およびデータベースの各部分のレコード数を把握できます。

このコマンドの形式は以下のようになります。

```
secons -i
```

-i

実行時の統計情報をフォーマットされたテキストで表示します。

例: 実行時データの表示

以下の例は、secons -i コマンドの出力を示しています。

```
Runtime Statistics:
          --------------------
          INet statistics:
                Requests denied   : 0
                Requests granted  : 17
                Errors found      : 0
          Queues size:
                Audit log: 0
                Error log: 0
          Cached tables info:
                ACEE handles      :      11
                Protected clients :      0
                Trusted programs  :      77
                Untrusted programs:      3
          Database info: (Record count & first free ID)
                Classes     :    235 ( CID     0x00f0 )
                Properties  :   4829 ( PID     0x1346 )
                Objects     :    842 ( OID 0x0000035a )
                PropVals    :   4109 ( N/A )
```

上記の出力の各行について、以下で説明します。

```
INet statistics:
      Requests denied   : 0
      Requests granted  : 17
      Errors found      : 0
```

CA Access Control によって実行されたネットワーク アクセス認証に関する統計情報を表示します。ネットワーク要求の認証時に拒否された要求、許可された要求、および検出されたエラーの数がまとめて表示されます。

```
Queues size:
      Audit log: 0
      Error log: 0
```

CA Access Control では、ファイルをロックした状態でログが作成されるため、特定のイベントをメモリ内に保持し、後でログ ファイルに書き込むことが可能です。これらの値が 10 を超えると、エラーが発生してのログ機能が正常に機能しなくなる場合があります。

```
Cached tables info:
      ACEE handles      :      11
      Protected clients :      0
      Trusted programs  :      77
      Untrusted programs:      3
```

CA Access Control が使用する、キャッシュされたテーブルのサイズに関する以下の情報を表示します。

- *ACEE*（アクセサ エレメント エントリ）とは、ログイン プロセスを保持しているテーブルです。
- *Protected clients*（保護クライアント）は、キャッシュされたクライアント数を示します。通常、この値は 0 です。
- *Trusted Programs*（Trusted プログラム）は、メモリにキャッシュされた PROGRAM クラスのエントリ数を示します。通常は、すべてのプログラムが trusted としてキャッシュされます。
- *Untrusted Programs*（Untrusted プログラム）は、untrusted として識別されたプログラム数を示します。

```
Database info: (Record count & first free ID)
      Classes     :    235 ( CID     0x00f0 )
      Properties  :   4829 ( PID     0x1346 )
      Objects     :    842 ( OID 0x0000035a )
      PropVals    :   4109 ( N/A )
```

データベースのサイズ、およびデータベースの各部に含まれるレコード数についての全般的な情報です。

secons -i 機能 - Windows での実行時の統計情報の表示

Windows で該当

secons ユーティリティは、CA Access Control 実行時の統計情報および内部カウンタを表示します。システムの動作に関する統計情報を使用して、以下のことを把握します。

- 各インターセプト タイプについて、トリガされたイベントの数
- キャッシュされたイベントの数と、完全に承認されたイベントの数の比較による、各カーネル キャッシュの有効率

注: 監査キューのアクティビティが活発になる時期に、監査キューのサイズが増加するのは問題ではありません。しかし、キューへのロードが平常の状態に戻ったら、キュー サイズは減少するはずです。

このコマンドの形式は以下のようになります。

```
secons -i [-reset]
```

-i

実行時の統計情報をフォーマットされたテキストで表示します。

-reset

(オプション) 実行時カウンタを 0 にリセットします。

例: 実行時データの表示

secons -i コマンドの出力のうち、名前だけでは内容がわかりにくい情報について、以下に説明します。

データベース実行時データ

CA Access Control データベース内のクラス、オブジェクト、プロパティの数、および最後に作成されたクラス、オブジェクト、プロパティの ID を表示します。また、プロパティ値の数も表示します。

この情報は、データベースのサイズを評価するために使用します。使用されるオブジェクトとプロパティの数が多くなるほど、データベースのサイズは大きくなります。

カーネル実行時データ

各カーネル キャッシュ(ファイル、レジストリ、サロゲート)について、その作成日時、サイズ、および使用率を表示します。使用率は、全イベント数における、監査イベントの数の割合です。残りのインターセプト イベントは、認証プロセスに準じます。

この情報は、各カーネル キャッシュの必要性および使用率を評価するために使用します。

カーネル監査情報

現在のカーネル監査キューのサイズ、およびその最大サイズ、および最大サイズへの到達時期を表示します。

この情報は、監査キューの動作を評価するために使用します。監査キューが、割り当てられている最大キュー サイズを超えないように注意する必要があります。このサイズは、FsiDrv¥MaxAuditRecordLimit CA Access Control レジストリ エントリで設定します。この制限を超えると、CA Access Control が監査イベントを生成するスピードは、キューを解決する必要があるため遅くなります。

ユーザ モード強制実行時データ

Full Enforcement モードで、インターセプトされたファイル、レジストリ、ログオン、強制終了、および Windows サービス イベントに関する情報を表示します。認証エンジンによって認証されるイベントの数、および各クラスの認証プロセスに要する最大時間および平均時間がわかります。

この情報は、実際に稼動しているシステムにおける問題の解決に使用してください。これにより、CA Access Control を停止することなく、いくつかの有用な初期データが提供されます。

ユーザ モード監査実行時データ

監査イベント(キャッシュされたインターセプト イベント)に関する情報を表示します。

この情報は、ユーザ モードでの監査キューの動作を監視するために使用します。監査キューの最大サイズが一貫して増加する場合は、CA Access Control が監査ログ ファイルに書き込むことができるかどうかを確認する必要があります。システムがディスク領域を使い切ってしまった場合、または CA Access Control にファイルに対するネイティブなアクセス権限がない場合、CA Access Control はファイルに書き込みできない場合があります。

注: 監査キューのアクティビティが活発になる時期に、監査キューのサイズが増加するのは問題ではありません。しかし、キューへのロードが平常の状態に戻ったら、キュー サイズは減少するはずです。

secons -kt 機能 - UNIX でのカーネル テーブルの表示

UNIX で該当

secons ユーティリティはカーネル テーブルを表示します。

このコマンドの形式は以下のようになります。

```
secons -kt tableNumber
```

-kt

指定されたカーネル テーブルを表示します。

tableNumber

表示するカーネル テーブルを指定します。*tableNumber* は以下の値のいずれかにします。

1

SpecPgm カーネル テーブルの表示を指定します。

2

TrustPg カーネル テーブルの表示を指定します。

3

LoginPg カーネル テーブルの表示を指定します。

4

DBfiles カーネル テーブルの表示を指定します。

5

FRegExp カーネル テーブルの表示を指定します。

6

DCMfile カーネル テーブルの表示を指定します。

7

AC pids カーネル テーブルの表示を指定します。

8

InoCach カーネル テーブルの表示を指定します。

注: Linux では有効ではありません。

9

F キャッシュ カーネル テーブルの表示を指定します。

10

NetwDCM カーネル テーブルの表示を指定します。

11

MntDirs カーネル テーブルの表示を指定します。

12

F inode カーネル テーブルの表示を指定します。

13

STOPbyp カーネル テーブルの表示を指定します。

注: STOP が有効にならない場合、このカーネル テーブルは表示できません。

14

STOPexp カーネル テーブルの表示を指定します。

注: STOP が有効にならない場合、このカーネル テーブルは表示できません。

15

Family カーネル テーブルの表示を指定します。

16

DbgProt カーネル テーブルの表示を指定します。

17

TCPport カーネル テーブルの表示を指定します。

18

TCPoutp カーネル テーブルの表示を指定します。

19

ProcSrv カーネル テーブルの表示を指定します。

例: DBfiles カーネル テーブルの表示

以下は、DBfiles カーネル テーブルを表示する場合の出力例です。

```
secons -kt 4
DBfiles
file    ID      i-node  device  program name
1       29      280391  356515  /opt/CA/AccessControl/seosdb/seos_ids.dat
2       3       0       0       /opt/CA/AccessControl/etc/privpgms.init
```

カーネル テーブル

カーネル テーブルは、CA Access Control のパフォーマンス改善を支援するために頻繁にアクセスされた情報を一覧表示します。カーネル テーブルが一覧表示するイベントの許可、拒否、解決について、CA Access Control がデータベースを確認する必要はないため、カーネル テーブルによってパフォーマンスが改善されます。

CA Access Control は以下のタイプのカーネル テーブルを含んでいます。

- キャッシュ テーブル - 前のリソース アクセス要求の結果、解決した inode 数、受け入れた TCP 着信 要求を一覧表示します。
- 保護されているリソーステーブル - アクセス要求時に、CA Access Control が常に CA Access Control エンジンへ認証要求を送信するリソースを一覧表示します。
- バイパス テーブル - アクセス要求時に、CA Access Control が認証要求を CA Access Control エンジンへ送信せずにアクセスを許可しているリソースを一覧表示します。
- プロセス テーブル - システムで実行中のすべてのプロセスに関する情報を一覧表示します。

以下のテーブルに、各カーネル テーブルに関する情報を示します。

テーブル名	タイプ	リスト	列名	環境設定
SpecPgm	保護されているリソース	SPECIALPGM クラスのすべてのオブジェクト	flags; user; oid; i-node; device; program	SPECIALPGM クラス レコード
TrustPg	保護されているリソース	PROGRAM クラスのすべてのオブジェクト	flags; i-node; device; program	PROGRAM クラス レコード

テーブル名	タイプ	リスト	列名	環境設定
LoginPg	保護されているリソース	LOGINAPPL クラスのすべてのオブジェクト	flags; i-node; device; program name	LOGINAPPL クラス レコード
DBfiles	保護されているリソース	FILE クラスのすべてのオブジェクト	file ID; i-node; device; program	FILE クラス レコード **注**: このテーブル内のレコードの最大数は seos.ini ファイルの SEOS_syscall セクションにある max_regular_file_rules によって定義されます。
FRegExp	保護されているリソース	FILE クラスの中で定義される包括的なファイル アクセス ルール	fid; expression	FILE クラスレコードでの包括的なルールによって定義されました。 **注**: このテーブル内のレコードの最大数は seos.ini ファイルの SEOS_syscall セクションにある max_general_file_rules によって定義されます。
DCMfile	バイパス	GAC を使用して定義する do-not-call-me ファイル	fid; user; type; access	GAC.init ファイル
ACpids	バイパス	CA Access Control デーモン用のプロセス ID	pid; service; contractID	-
InoCach	キャッシュ	キャッシュされた inode	i-node; device; priority; entry	seos.ini ファイルの SEOS_syscall セクションにある cache_enabled

テーブル名	タイプ	リスト	列名	環境設定
F キャッシュ	キャッシュ	キャッシュされたファイル アクセス認証結果	file ID; access; acee; answer; phash; prio	-
NetwDCM	キャッシュ	承認済みの受信 TCP 接続をキャッシュしました。	peer; port; local port; flag; prio	seos.ini ファイルの SEOS_syscall セクションにある UseNetworkCache
MntDirs	保護されているリソース	CA Access Control がマウントから保護するディレクトリ	dir ID; i-node; device; mount point	-
F inode	保護されているリソース	FILE クラス中のオブジェクトの Inode およびデバイス番号	file ID; i-node; device; links	-
STOPbyp	バイパス	CA Access Control が STOP 保護を提供しない PROGRAM クラスの中のオブジェクト	i-node; device; program	STOP が有効な場合、このテーブル内のオブジェクトにはプロパティ pgmtype (STOP) を持つ SPECIALPGM レコードがあります。
STOPexp	バイパス	CA Access Control が STOP 保護を提供しない PROGRAM クラスにオブジェクトを定義する正規表現	priority; n-chars; expression	STOP が有効な場合、このテーブル内のオブジェクトは、プロパティ pgmtype (STOP) を持つ SPECIALPGM レコードでの包括的なルールによって定義されます。
Family	バイパス	CA Access Control デーモン	service; pid; contractID	-
DbgProt	保護されているリソース	CA Access Control がデバッグから保護する CA Access Control バイナリ	pid; access; name in proc	-

テーブル名	タイプ	リスト	列名	環境設定
TCPport	バイパス	seos_syscall が seosd へのイベントを渡さないポート	TCP port	seos.ini ファイルの SEOS_syscall セクションにある bypass_TCPIP
TCPoutp	バイパス	seos_syscall が seosd への外部接続イベントを渡さないポート	TCP port	seos.ini ファイルの seosd セクションにある bypass_outgoing_TCPIP
ProcServ	プロセス	システムにおいて実行中のすべてのプロセスに関する情報を一覧表示します。	#n; pid; ppid; acee; flags; uid; euid; zone; arg0; ACuser **注**: このテーブルには、secons ユーティリティによって表示されないさらに多くの内部列があります。	-

カーネル テーブルの列名

以下のリストでカーネル テーブルの列名について説明します。

#n

カーネル テーブル内のエントリ番号。

形式

CA Access Control が許可するアクセスのタイプ、またはユーザの要求するアクセスのタイプを定義します。値はアクセス タイプの合計です。

1 - read
2 - write
4 - chown
8 - chmod
16 - rename
32 - unlink
64 - utimes
128 - chattr
256 - link
512 - chdir
1024 - create

acee

アクセス 要求を行うユーザの ACEE を定義します。

ACuser

ユーザの CA Access Control ユーザ名を定義します。

answer

アクセス要求に対する CA Access Control の応答（許可または拒否）を定義します。有効な値は以下のとおりです。

0 - 拒否

1 - 許可

arg0

プログラムの実行時に、引数 0 として定義されるプログラム名を定義します。

contractID

（Solaris 10 のみ）契約プロセス ID を定義します。

device

ファイルが存在する論理ディスクを定義します。

dir ID

ディレクトリ ID を定義します。

entry

inode の文字列値を定義します。

euid

有効なユーザ ID を定義します。

式

エントリが適用されるリソースを指定する式（文字列マッチングに使用されるテキスト パターン）を定義します。

fid *または* file ID

ファイルを識別するために CA Access Control が使用するファイル ID を定義します。

flags

エントリのビット マスク フラグを定義します。

i-node

inode 番号を定義します。

links

ファイルのハード リンクの数を定義します。

local port

TCP 受信接続を受け入れるローカル ホスト上のポートを定義します。

mount point

ディレクトリ内でマウントから保護するべき場所を定義します。

n-chars

式の中での文字数を定義します。

name in proc

/proc ファイル システムにプロセス名前を定義します。

注: /proc ファイル システムでは、プロセスはそれぞれファイルとして表されます。また、ファイル名はプロセス番号です。

oid

オブジェクト ID を定義します。

peer

ピア ホスト アドレスを定義します。

phash

パス文字列のハッシュ値を定義します。

pid

プロセス ID を定義します。

port

着信 TCP 接続が発信されたポートを定義します。

ppid

親プロセス ID を定義します

prio *または* priority

カーネル テーブルにエントリの優先度を定義します。カーネル テーブルが一杯の場合は、CA Access Control がカーネル テーブルに新しいエントリを書き込む場合に、優先度が最低のエントリが削除されます。

program *または* program name

プログラムの名前を定義します。

service

CA Access Control サービス(デーモン)の名前を定義します。

TCP port

エントリが適用する TCP ポートを定義します。

type

保護されたファイル タイプを定義します。

uid *または* user

ユーザ ID を定義します。

zone

(Solaris 10 のみ) ゾーン ID を定義します。

注: この列の値は、Solaris 10 以外の コンピュータの場合は常に 0 です。

キャッシュ テーブル

3 つのタイプのカーネル キャッシュ テーブルがあります。

- **F キャッシュ** - ファイル キャッシュ テーブルは、前の認可要求の結果をキャッシュします。

  同じ承認が要求されると、CA Access Control はその要求に対し、ファイル キャッシュ テーブルに格納された前回の応答を使用して回答します。

  注: ファイル キャッシュ テーブルの消去は、30 分毎と以下のクラスのレコードが変更された場合に必ず実行されます - CALENDAR、CONTAINER、FILE、GFILE、GROUP、HOLIDAY、PROGRAM、SECLABEL、SECLEVEL、SHIFT および USER。

- **InoCach** - inode キャッシュ テーブルは解決された i-node 数をキャッシュします。

  CA Access Control がファイル名に対する i-node 数を解決する必要がある場合、InoCach テーブルを確認してから、ファイル システムを確認します。

- **NetwDCM** - ネットワーク キャッシュ テーブルは受け入れた TCP 着信要求を格納します。

  CA Access Control がネットワーク キャッシュ中のリクエストと同一の TCP 着信要求を受け取る場合、CA Access Control は自動的にリクエストを許可します。

secons ユーティリティを使用して、カーネル キャッシュ テーブルの表示、消去、有効化、無効化ができます。

保護されているリソーステーブル

CA Access Control が認証要求をインターセプトする場合、アクセスが要求されるリソースがカーネル中の保護されているリソーステーブルにリストされているかどうか確認します。

リソースが保護されているリソーステーブルにリストされていれば、CA Access Control は常に CA Access Control エンジンへ認証要求を送ります。リソースが保護されているリソーステーブルにリストされていないと、CA Access Control エンジンに認証要求を送信しない場合がありますが、代わりにカーネル中でアクセス要求を解決します。

バイパス テーブル

CA Access Control が認証要求をインターセプトする場合、アクセスの要求されるリソースがカーネル中のバイパス テーブルにリストされているかどうか確認します。

リソースがバイパス テーブルにリストされていれば、CA Access Control はアクセス要求を許します。バイパス テーブル内にリソースがリストされていない場合、CA Access Control は CA Access Control 認証エンジンに対してさらにアクセス確認するよう要求を送ります。

secons -ktc 機能 - UNIX 上のカーネル キャッシュ テーブルの消去、有効化、無効化

UNIX で該当

secons ユーティリティはカーネル キャッシュ テーブルを消去、有効化、または無効化します。

このコマンドの形式は以下のようになります。

`secons -ktc optionNumber`

-ktc

カーネル キャッシュ テーブルの消去、有効化、または無効化を指定します。

optionNumber

実行するアクションを指定します。*optionNumber* は、必ず以下のいずれかにしてください。

1

F キャッシュ テーブルを消去します。

2

F キャッシュ テーブルを有効化します。

3

F キャッシュ テーブルを無効化します。

4

NetwDCM テーブルを消去します。

5

NetwDCM テーブルを有効化します。

6

NetwDCM テーブルを無効化します。

7

F inode テーブルを消去します。

注: Linux では有効ではありません。

8

F inode テーブルを有効化します。

注: Linux では有効ではありません。

9

F inode テーブルを無効化します。

注: Linux では有効ではありません。

例: F キャッシュ テーブルの消去

以下の例では F キャッシュ テーブルを消去します。

```
secons -ktc 1
```

secons -refIP 機能 - ネットワーク リソースの IP アドレスの更新

Windows で該当

secons ユーティリティは、データベース ネットワーク リソースの IP アドレスを更新します。特定のホストで更新を機能させるには、そのホスト上で DNS がすでに更新されている必要があります。以下の Windows コマンドを使用して、DNS を手動で更新します。

```
ipconfig /flushdns
```

このコマンドの形式は以下のようになります。

```
secons -refIP [hosts]
```

-refIP [*hosts*]

(Windows のみ) CA Access Control によってネットワーク リソースの IP アドレスを更新するホストを、スペース区切りのリストで定義します。ホストを定義しない場合、ローカル ネットワーク リソースが更新されます。

このオプションを使用して、現在の IP アドレスで CA Access Control リソースを更新できます。このため、IP アドレスが動的に割り当てられる DHCP 環境で特に役立ちます。

secons -rl 機能 - UNIX での環境設定の再ロード

UNIX で該当

secons ユーティリティは、seos.ini ファイルを再ロードします。secons ユーティリティを使用すると、CA Access Control を停止せずに構成設定を更新できます。

このコマンドの形式は以下のようになります。

```
secons -rl
```

--rl

(UNIX のみ) CA Access Control を停止せずに seos.ini 設定ファイルおよび更新設定を再ロードします。

secons -v 機能 - Windows での計測ランタイム設定の制御

Windows で該当

secons ユーティリティは、CA Access Control 計測のランタイム設定を制御します。このユーティリティを使用すると、外部 DLL ライブラリをアクティブなプロセスにロードし、CA Access Control 計測プラグインのランタイムトレース設定を変更できます。このコマンドを実行するには、ADMIN または OPERATOR 属性が必要となります。

このコマンドで DLL ライブラリをロードするための形式は以下のとおりです。

```
secons -v target load "dll_name"
```

このコマンドで CA Access Control 計測プラグインのトレースを有効または無効にするための形式は以下のとおりです。

```
secons -v target trace plugin_name
{trace:enable|trace:disable}:{file:"tracefile_path"|debug}
```

注: トレースが適切に設定されるまで、CA Access Control はトレースを開始しません。

このコマンドで CA Access Control 計測プラグインのトレースを設定するための形式は以下のとおりです。

```
secons -v target trace plugin_name trace:option:{sources:{1 | 4} | filtering:value
| filecyclic:{0 | 1} | filelimit:value }
```

debug

コマンドがデバッグ出力チャネルへのトレースを有効または無効にするように指定します。

file:"*tracefile_path*"

CA Access Control がトレースを書き込むファイルのフル パスを定義します。

注: trace:disable パラメータを指定する場合、CA Access Control は file:"*tracefile_path*" パラメータに指定された値を無視します。

filecyclic:{0 | 1}

循環ファイル トレースを有効にするかどうかを指定します。循環ファイル トレースを有効にした場合、トレース ファイルのサイズが指定の最大サイズに達すると、CA Access Control はトレース ファイルの最初に戻ってトレースの書き込みを続行します。

このパラメータには、以下の値を設定できます。

0 - 循環ファイル トレースを無効にします

1 - 循環ファイル トレースを有効にします

filelimit:*value*

トレース ファイルの最大サイズをバイト単位で定義します。値が 0 の場合、トレース ファイルの最大サイズは指定されません。

filtering:*value*

指定された計測プラグインのトレースをフィルタするビット単位のフィルタ マスクを定義します。CA Access Control は、フィルタされたイベントをトレース ファイルに書き込みません。

注: フィルタなし(CA Access Control がすべてのイベントをトレース ファイルに書き込む)を指定するには、0xFFFFFFFF を使用します。このパラメータの他のすべての値は、指定するプラグインに依存します。

load "*dll_name*"

指定された DLL をターゲット プロセスにをロードするように指定します。DLL の動作環境とターゲット プロセスの動作環境は同一である必要があります。たとえば、ターゲット プロセスとして 32 ビットプロセスを指定した場合、DLL も 32 ビットである必要があります。

重要: DLL は、*ACInstallDir*¥bin フォルダに存在する必要があります。

sources:{1 | 4}

CA Access Control がどこへトレースを出力するかを指定します。

このパラメータには、以下の値を設定できます。

1 - ファイルに出力します

4 - デバッグ API トレースに出力します

target

ターゲット プロセス(複数可)を定義します。このパラメータには、以下のいずれかの値を設定できます。

all_32bit

コンピュータで実行されているすべての 32 ビット プロセスにコマンドを送信するように指定します。

all_64bit

コンピュータで実行されているすべての 64 ビット プロセスにコマンドを送信するように指定します。

PID

ターゲット プロセスのプロセス ID を定義します。ターゲット プロセスはコンピュータ上で実行されている必要があります。

process_name

ターゲット プロセスの名前を識別するマスクを定義します。ターゲット プロセスはコンピュータ上で実行されている必要があります。たとえば、このパラメータに cmd.exe を指定し、cmd.exe の 3 つのインスタンスがコンピュータ上で実行されている場合、CA Access Control は 3 つのプロセスすべてにコマンドを適用します。

trace *plugin_name*

CA Access Control 計測プラグイン *module_name*（cainstrm、stopplg など）のランタイム トレース設定を変更するように指定します。.

注: プラグインの DLL 名を指定する必要があります。計測プラグインをアップグレードし、そのプラグインの DLL の名前が変更された場合、新しい DLL の名前をコマンドに指定する必要があります。たとえば、cainstrm プラグインをアップグレードし、そのアップグレードされた DLL の名前が cainstrm2.dll である場合は、*plugin_name* として cainstrm2 を指定する必要があります。

trace:disable

ターゲット プラグインのトレースの有効化を指定します。

trace:enable

ターゲット プラグインのトレースの無効化を指定します。

注: このパラメータは、トレース有効化フラグのステータスを実行時に変更します。CA Access Control はトレースが適切に設定されるまでトレースを開始しません。

trace:option

ターゲット プラグインのトレースを設定するように指定します。

例: デバッグ出力チャネルへのトレースの有効化

以下のコマンドは、コンピュータ上で実行されている 32 ビットプロセスである stopplg プラグインのすべてのファイルのトレース有効化フラグのステータスを実行時に変更します。CA Access Control は、トレースが適切に設定されるまでトレースを開始しません。

```
secons -v all_32bit trace stopplg trace:enable:debug
```

例: トレース フィルタ マスクのプラグインへの適用

以下のコマンドは、PID 362 のプロセスで、cainstrm プラグインのすべてのファイルにトレース フィルタリング マスクを適用します。

```
secons –v 362 trace "cainstrm trace:option:filtering:4294967295"
```

secons -whoami 機能 - ユーザ名およびセキュリティ クレデンシャルの表示

Windows で該当

secons ユーティリティを使用して、CA Access Control 認証エンジンで認識されるユーザ名を表示します。この情報は、ACEE (アクセサ エレメント エントリ) テーブルに格納されています。ACEE には、以下のユーザに関する情報が格納されています。

- **ログインしたユーザ** - オペレーティング システムにログインしたユーザです。このタイプのユーザには、以下の ACEE 属性を指定します。
  - ログイン セッション ID
  - ログイン セッション タイプ
- **管理ユーザ** - LCA 接続を使用して、CA Access Control 管理アプリケーションにログインしたユーザです。例: selang
- **Authorization API ユーザ** - SEOSROUTE_* API で参照されるユーザです。

- **SPECIALPGM 論理ユーザ** - 1 つ以上の SPECIALPGM レコードで参照されるユーザです。このタイプのユーザ用の特別な ACEE 属性を以下に示します。
  - SPECIALPGM レコードと関連付けられた ACEE
- **組み込みユーザ** - CA Access Control に組み込まれているユーザです。例: *_undefined*

このコマンドの形式は以下のようになります。

```
secons -whoami
```

例: ユーザ名およびセキュリティ クレデンシャルの表示

以下の例は、CA Access Control 認証エンジンで認識されているユーザ名およびセキュリティ クレデンシャルを表示します。

```
secons -whoami
```

secons の出力は、以下のようになります。

```
ACEE handle '2' represents 'Logged on User': COMP1-SRV-X86¥John
ACEE was created at: Wed Feb 20 17:34:47 2008
ACEE was last accessed at: Wed Feb 20 17:36:49 2008
ACEE user role is: Auditor, Administrator
ACEE audit mode is: Failure, Login Success, Login Failure; Originated from User
definition
ACEE user is a member of 0 'CA Access Control' groups
ACEE's Logon session ID is: 0:68737
ACEE's Logon session type is: Interactive
```

詳細情報:

sewhoami ユーティリティ - UNIX での CA Access Control ユーザ名およびセキュリティ クレデンシャルの表示 (P. 265)

secrepsw ユーティリティ - Policy Model ファイルおよび shadow ファイルの作成

UNIX で該当

secrepsw ユーティリティは、すべてのユーザのパスワード レコードを /etc/passwd ファイルに作成します。secrespw は、UNIX 環境で動作する PMDB によって定義されたユーザを管理する場合に必要です。secrepsw ユーティリティは、shadow ファイルを作成および削除することもできます。

注: このユーティリティは lbin ディレクトリに配置されており、root ユーザのみが使用できます。secrepsw ユーティリティを使用するには、pmd.ini ファイルにある shadow トークンを *yes* に変更する必要があります。

このコマンドの形式は以下のようになります。

```
secrepsw [-h] [-c] [-r PolicyModel] [-s PolicyModel]
```

-c

ローカル コンピュータの /etc/passwd ファイルおよび /etc/shadow ファイルから新しい Policy Model パスワード ファイルを作成します。

-h

このユーティリティのヘルプ画面を表示します。

-r *PolicyModel*

ユーザ名およびパスワードを Policy Model の shadow ファイルから元の Policy Model パスワード ファイル（passwd）に転送して戻します。

-s *PolicyModel*

ユーザ名およびパスワードを Policy Model のパスワード ファイル（passwd）から Policy Model の shadow ファイルに転送します。

sedbpchk ユーティリティ - データベースのバックアップ

UNIX で該当

sedbpchk ユーティリティは、データベースのバックアップ コピーを作成します。sedbpchk は、実行時データベースを一時的な場所にコピーし、その一時データベースに対してさまざまな整合性チェックを行います。整合性チェックで問題がなかった場合は、一時データベースをバックアップの保存場所にコピーします。

データベースの整合性に問題があった場合、sedbpchk は、コピー中に更新内容がデータベースに適用されたかどうかを確認します。更新内容が適用されている場合、データベースは壊れていない可能性があります。

データベースのコピー中に更新の適用がなかった場合は、データベースが壊れている可能性があります。この場合は、システム管理者に電子メール メッセージが送信されるため、システム管理者は、バックアップ ディレクトリを使用して、壊れている実行時データベースを上書きすることができます。

注: このスクリプトを使用するときは十分な注意が必要です。データベースが壊れていないのに壊れていると誤って判断される可能性があります。ただし、データベースに問題がないという判断については、常に正しい判断となります。

このスクリプトを実行するには、root 権限と ADMIN 権限が必要です。sedbpchk を使用する前に、*ACInstallDir*/lbin にあるこのスクリプトを確認し、以下のフィールドの値がサイトのニーズに合っていることを確認することをお勧めします。

MAIL_TO

データベースが壊れていることを通知するメッセージが送信されるユーザの名前を指定します。

RETRIES

データベースが壊れている可能性がある場合、通知を送信する前に、sedbpchk ユーティリティでデータベースをチェックする回数を指定します。

ACInstallDir

CA Access Control インストール ディレクトリの場所を指定します。

SE_BINDIR

CA Access Control バイナリ ファイル ディレクトリの場所を指定します。

SE_DB_DIR

CA Access Control 実行時データベース ディレクトリの場所を指定します。

SE_BCKDIR

バックアップ データベース ディレクトリの場所を指定します。

SE_TMPDIR

一時データベース ディレクトリの場所を指定します。

注: sedbpchk ユーティリティはスクリプト ファイルとして提供されているため、実行するには .sh 拡張子を指定する必要があります。

このコマンドの形式は以下のようになります。

```
sedbpchk
```

seerrlog ユーティリティ - エラー ログ レコードの表示

UNIX で該当

seerrlog ユーティリティは、CA Access Control エラー ログのレコードを一覧表示します。。エラー ログ ファイルを読み取るための権限があるか、またはエラー ログ ファイルを読み取ることができるグループ (error_group 構成設定で定義されたグループ) のメンバであることが必要です。

このコマンドの形式は以下のようになります。

```
seerrlog [-h] [-s date] [-e date] [-d] [-f filename]
```

-s *date*

リストの開始日を指定します。定義された日付以降に書き込まれたレコードが一覧表示されます。

制限: 日付は dd-mm-yyyy の形式にする必要があります。

-e *date*

リストの終了日を指定します。定義された日付までに書き込まれたレコードが一覧表示されます。
制限: 日付は dd-mm-yyyy の形式にする必要があります。

-d

エラーに関する詳細情報を出力しないように指定します。

-h

このユーティリティのヘルプ画面を表示します。

-f *filename*

読み取るエラー ログ ファイルを指定します。

デフォルトでは、seerrlog は *ACInstallDir*/log/seos.error ファイルを読み取ります。このファイルをデータベースに定義することはできず、CA Access Control のみがこのファイルに書き込むことができます。

例

- 2006 年 1 月 3 日以降に書き込まれたすべてのエラー レコードを一覧表示するには、以下のように入力します。

```
seerrlog -s 03-Jan-2006
```

- 2006 年 1 月 3 日から 2007 年 1 月 1 日までの間に書き込まれたすべてのエラー レコードを一覧表示するには、以下のように入力します。

```
seerrlog -s 03-Jan-2006 -e 01-Jan-2007
```

segrace ユーティリティ - ユーザのログイン情報の表示

segrace コマンド ライン ユーティリティは、ユーザに許可されている猶予ログインの残りの回数、ユーザの現在のパスワードが期限切れになるまでの残り日数、およびユーザが最後にログオンした日時と端末を表示します。

注: ユーザの猶予ログイン プロパティの詳細については、お使いの OS に対応する「*エンドポイント管理ガイド*」を参照してください。

segrace を起動する前に、システム管理者は以下の selang コマンドを入力して、CA Access Control のパスワード チェック機能を有効にする必要があります。

```
setoptions class+(PASSWORD)
```

これ以降は、ユーザのパスワードが変更されるたびに、新しいパスワードが、データベースに設定されているパスワードの品質ルールと照合されるようになります。

segrace ユーティリティ - UNIX でのユーザ ログイン設定の表示

UNIX で該当

segrace ユーティリティは、ユーザのログイン設定を表示します。ユーザがログインするたびに segrace コマンドを実行することをお勧めします。このためには、このコマンドを /etc/profile および /etc/csh.login（Solaris の場合は /etc/.login）に追加します。

segrace で猶予ログインの回数をカウントするには、sepass ユーティリティを使用してパスワードを変更する必要があります。ユーザに猶予ログインの回数が残っていない場合、segrace は sepass ユーティリティを起動します。これにより、ユーザによるパスワード変更が要求されます。sepass ユーティリティの代わりに実行するコマンドをサイトで決定するには、seos.ini ファイルの segrace セクションにある sepass_command トークンに他のユーティリティを指定します。

このコマンドの形式は以下のようになります。

```
segrace [-h] [-d days] [-l] [-p] [userName]
```

-d *days*

ユーザの現在のパスワードが期限切れになるまでの残り日数を表示します。この数値は、*days* パラメータに指定した日数が CA Access Control オプションの設定値以上である場合にのみ表示されます。*days* パラメータを省略すると、デフォルトの 7 日間が使用されます。このオプションは、ユーザのパスワードが sepass を使用して変更された場合にのみ有効です。

-h

このユーティリティのヘルプ画面を表示します。

--l

ユーザが最後にログインした日時およびログインした端末を表示します。

-p

ユーザのパスワードが期限切れになったときに、新しいパスワードの入力を促すメッセージを表示します。

userName

ユーザ名を指定した場合、要求したユーザに ADMIN 属性があれば、segrace によって、指定したユーザに必要なログイン情報が表示されます。

ユーザ名を指定しない場合は、現在のユーザのログインの詳細が表示されます。

詳細情報:

sepass ユーティリティ - パスワードの設定または変更 (P. 219)

segrace ユーティリティ - Windows でのユーザ ログイン設定の表示

Windows で該当

segrace ユーティリティは、ユーザのログイン設定を表示します。segrace ユーティリティは、リモート マシンからスタンドアロン モジュールとして実行できます。

注: パラメータを指定せずに segrace を起動し、ユーザに猶予ログインがない場合は、何も表示されません。

このコマンドの形式は以下のようになります。

```
segrace [-h] [-d days] [-l] [-p] [-s host] [userName]
```

-d *days*

サーバに設定されているデフォルト値とは異なる警告 *日数*パラメータを設定します。

-h

このユーティリティのヘルプ画面を表示します。

--l

ユーザが最後にログインした日時およびログインした端末を表示します。

-p

*警告日数*期間が到来したためパスワードの有効期限が切れることを警告する場合、またはユーザに猶予回数がある場合に、パスワードの入力を促すメッセージを表示します。

-s *host*

CA Access Control データベースが使用されるリモート サーバ名を指定します。

userName

ユーザ名を指定した場合、要求したユーザに ADMIN 属性があれば、segrace によって、指定したユーザに必要なデータが表示されます。

ユーザ名を指定しない場合は、現在のユーザのログインの詳細が表示されます。

segracex ユーティリティ - UNIX でのパスワードの有効期限の確認

UNIX で該当

segracex ユーティリティは、X Window 環境で新しいパスワードを設定します。segracex ユーティリティは、ユーザのパスワードが有効期限切れかどうかをチェックします。有効期限切れの場合は、パスワードを変更できるウィンドウが表示されます。

segracex ユーティリティは、ユーザがデスクトップ環境にログインした後に起動されるユーザ初期化スクリプトにリンクするように設計されています。

このユーティリティは、ユーザの CA Access Control での猶予ログイン属性をチェックします。猶予ログインの残りの値に応じて、以下の処理が実行されます。

- 0 の場合は、パスワードの変更を強制します。
- 正の数であっても、ユーザの猶予パラメータまたはグローバルな猶予設定（設定されている場合）で指定された値未満である場合は、パスワードの変更を推奨するメッセージを表示します。
- ユーザの猶予パラメータまたはグローバルな猶予設定（設定されている場合）で指定された値以上の場合は、何も行われません。

パスワードを変更する場合は、古いパスワードの入力を促すメッセージが表示されます。次に、新しいパスワードの入力を促すメッセージが表示されます。

- CA Access Control のパスワード チェックが有効になっている場合は、データベースに設定されているパスワード ルールに新しいパスワードが準拠しているかどうかがチェックされます。新しいパスワードが品質チェックの基準を満たす場合は、新しいパスワードの再入力を促すメッセージが表示されます。
- パスワード チェックが無効になっている場合は、新しいパスワードの再入力を促すメッセージがただちに表示されます。

  新しいパスワードが 2 回入力されると、2 つの新しいパスワードが比較されます。これらのパスワードが一致しない場合は、新しいパスワードの入力を促すメッセージが再度表示されます。

2 つの新しいパスワードが一致する場合、パスワードは以下の方法で更新されます。

- ローカル ホストのパスワード ファイル(/etc/passwd とセキュリティ ファイル)およびローカル データベースが更新されます。
- seos.ini ファイルの [seos] セクションの passwd_pmd トークンまたは parent_pmd トークンに値が定義されている場合は、適切な PMDB が更新され、その更新内容が UNIX 環境およびデータベースの両方のサブスクライバに伝達されます。seos.ini ファイルの [passwd] セクションの nis_env トークンに値(nis または nisplus)が設定されている場合は、NIS または NIS+ サーバが更新されます。マスタ NIS サーバにパスワードが設定されている場合は、NIS パスワード マップが自動的に再作成されます。

色やフォントなどのカスタマイズ可能なリソースは、segracex ファイルに格納されています。CA Access Control の標準インストールの際に、このファイルは以下のディレクトリに格納されます。

- Sun Solaris を除くすべてのプラットフォームの場合

  ```
  /usr/lib/X11/app-defaults
  ```

- Sun Solaris プラットフォームの場合

  ```
  /usr/lib/openwin/app-defaults
  ```

BigTradeMark_BW.xpm ファイルには CA Access Control の商標アイコンが格納されています。インストール後、このファイルを *ACInstallDir*/data/segracex ディレクトリに格納する必要があります。

このコマンドの形式は以下のようになります。

```
segracex [-user userName]
```

userName

ユーザ名を指定した場合、要求したユーザに ADMIN 属性があれば、segracex が指定したユーザに対して実行されます。

ユーザ名を指定しない場合、*segracex* は現在のユーザに対して実行されます。

SegraceW ユーティリティ - Windows でのパスワードの有効期限の確認

Windows で該当

Windows GUI 猶予ユーティリティは、ユーザのパスワードの有効期限が切れているかどうか、またはユーザに猶予ログイン回数があるかどうかを確認します。該当する場合は、パスワードを変更できるウィンドウが表示されます。

SegraceW は、CA Access Control 以外の環境のスタンドアロン モジュールとして実行できます。このため、SegraceW ユーティリティはドメイン内のあらゆるワークステーションに適用できます。

SegraceW は、最初にプライマリドメイン コントローラへの接続を試みます（NT 4.0 環境の場合）。この試みが失敗した場合にのみ、バックアップ ドメイン コントローラを探します。Windows 2000 以降の環境では、SegraceW は最初に見つかったドメイン コントローラへの接続を試みます。

注: リモート ホストが SegraceW の実行オプションで明示的に指定されている場合、SegraceW はそのリモート ホストにのみ接続します。

SegraceW ユーティリティは、ドメイン コントローラの NETLOGON 共有にあるログイン バッチ ファイルから呼び出されるように設計されています。

SegraceW ユーティリティは、ユーザのパスワードの有効期限が切れているかどうか、またはユーザに猶予ログイン回数があるかどうかを確認します。

ユーザに猶予ログイン回数属性がある場合は、以下の処理が実行されます。

- ユーザの猶予ログインの残りの回数が 0 の場合は、パスワードの変更を強制します。
- ユーザの猶予ログインの残りの回数が正の値の場合は、パスワードの変更を推奨するメッセージを表示します。

ユーザに猶予ログイン回数がない場合は、SegraceW によってパスワードの期限切れステータスがチェックされます。

- パスワードの期限が切れる期間が、サーバ側で設定された警告日数パラメータの値よりも多い場合、SegraceW は何も行いません。
- パスワードの期限が切れる期間が、サーバ側で設定された警告日数パラメータの値以下である場合は、SegraceW によってパスワードの変更を推奨するメッセージが表示されます。
- パスワードの有効期限が切れている場合、SegraceW はパスワードの変更を強制します。

パスワードを変更する場合、SegraceW によって、古いパスワード、新しいパスワード、および新しいパスワードの確認を入力するように促す「パスワードの変更」メッセージが表示されます。

確認チェックに成功すると、パスワードはドメイン コントローラの SAM データベースで更新されます。

このコマンドの形式は以下のようになります。

```
segracew [d] [-s remoteHost]
```

d

サーバに設定されているデフォルト値とは異なる*警告日数*パラメータを設定します。

-s *remoteHost*

情報を取得するために、指定したリモート ホストに接続します。

注: リモート ホストに接続する前に、暗号化ライブラリをリモート ホストからローカル ホストにコピーして、その名前を defence.dll に変更します。

seini ユーティリティ - 環境設定ファイルの管理

UNIX で該当

seini ユーティリティは、CA Access Control データベースおよびすべてのホストの初期設定ファイルを管理します。ホストに対して以下の処理を行います。

- CA Access Control データベースのパスを表示します。
- 初期設定ファイル（.ini）のパスを表示します。
- 初期設定ファイルのトークンの内容を表示します。
- 初期設定ファイルの特定のセクションに、特定のトークンの値を設定します。
- 初期設定ファイルの特定のセクションから、特定のトークンを削除します。

seini ユーティリティは、その他の .ini ファイルのトークンもすべて表示します。初期設定ファイルの名前は、常に拡張子 *.ini* で終わる必要があります。WRITE 権限および ADMIN 権限が割り当てられている限り、任意のリモート ホストから .ini ファイルを操作できます。

スイッチを指定しない場合は、データベースおよび seos.ini ファイルのパスが表示されます。

注: : seosd が実行中でない場合、またはデータベースのルールによって明示的に許可されている場合にのみ、seini ユーティリティで seos.ini ファイルを更新できます。

seos.ini ファイルに特定のトークンを追加することによって、seini でトークンおよびセクションのインテリジェント検索を実行できます。この機能では、完全一致または部分一致（25% 以内の許容誤差）が見つかるまで、各トークンまたは各セクションを、指定したトークンまたはセクションと比較することによって、スペル エラーがチェックされます。該当するトークンまたはセクションが見つかると、指定した操作が実行されます。それ以外の場合は、エラー メッセージが表示されます。

注: インテリジェント検索機能は、seini ユーティリティを起動したホストでのみ実行できます。

このコマンドの形式は以下のようになります。

```
seini [-d] [host]

seini [-i] [host]

seini [-H host] ¥
    {[-f [host.]section.token [ini_file]] | ¥
    [-r [host.]section.token [ini_file]] | ¥
    [-s [host.]section.token value [ini_file]] | ¥
    [-sn [host.]section.token value [ini_file]]}
```

-d [*host*]

リモート ホスト上のデータベースのパスを表示します。ホストを指定しない場合は、ローカル ホストのパスが表示されます。

-f [*host*.]*section*.*token* [*ini_file*]

指定したホスト上の指定した初期設定ファイルのセクションにあるトークンの値を表示します。 指定したセクションまたはトークンが見つからない場合は、空の行が表示されます。ホスト、セクション、およびトークンの名前は、ピリオド(.)で区切る必要があります。*ini_file* を指定しない場合は、seos.ini ファイルのセクションおよびトークンが検索されます。ローカル コンピュータの情報を表示するには、*host* パラメータを省略します。

-g *section*

定義したセクションのトークンを一覧表示します。

-h

このユーティリティのヘルプ画面を表示します。

-H [*host*]

-f、-r、-s、および -sn の各フラグを指定して、使用するリモート ホストを指定します。

-i [*host*]

初期設定ファイル seos.ini のパス名を指定します。ホストを指定しない場合は、ローカル ホストのパス名が表示されます。

-r [*host.*]*section.token* [*ini_file*]

指定したホストの**初期設定ファイル**のセクションからトークンを削除します。*ini_file* を指定しない場合、seos.ini ファイルからトークンが削除されます。

ローカル コンピュータの情報を削除するには、セクション名とトークン名のみを指定します。

-s [*host.*]*section.token value* [*ini_file*]

指定したホストの**初期設定ファイル**のセクションにあるトークンの値を設定します。*ini_file* パラメータを指定しない場合、seos.ini ファイルに値が設定されます。セクションまたはトークンが存在せず、リモート ホストを指定している場合は、そのセクションまたはトークンが作成されます。

ローカル コンピュータにセクションまたはトークンを作成するには、-sn スイッチを使用します。

-sn [*host.*]*section.token newValue* [*ini_file*]

指定したホストの**初期設定ファイル**のセクションにあるトークンの値を設定します。*ini_file* パラメータを指定しない場合、seos.ini ファイルに値が設定されます。セクションまたはトークンが存在せず、ローカル ホストを指定している場合は、そのセクションまたはトークンが作成されます。

リモート コンピュータにセクションまたはトークンを作成するには、-s スイッチを使用します。

例: seini の使用

- seos.ini 初期設定ファイルがローカル コンピュータのどこに格納されているかを見つけるには、以下のコマンドを使用します。

  ```
  seini -i
  ```

- [seosd] セクションの *trace* 構成設定の値を見つけるには、以下のコマンドを使用します。

  ```
  seini -f seosd.trace_file
  ```

- [seosd] セクションの *trace_to* 構成設定の値を設定するには、以下のコマンドを使用します。

  ```
  seini -s seosd.trace_to file
  ```

  このコマンドの出力は、以下のようになります。

  ```
  The token seosd.trace_to now set to file (was file,stop)
  ```

selang ユーティリティ - CA Access Control コマンドラインの実行

selang ユーティリティは、CA Access Control データベースおよびネイティブ環境にアクセスできるコマンド シェルを起動します。このコマンド シェルから selang のコマンドを発行することで、データベースが動的に更新されます。

注: -o オプションを指定した場合を除き、コマンドの実行結果は標準出力に送信されます。

UNIX でのこのコマンドの形式は、以下のようになります。

```
selang [{-c command|-f file}] [{-d path|-p pmdb}] [-o file] [-r file] [-s] ¥
[-u user pass]
selang [-l] [-o file] [-r file] [-s] [-u user pass]
```

Windows でのこのコマンドの形式は、以下のようになります。

```
selang [{-c command|-f file}] [{-d path|-p pmdb}] [-o file] [-r file] [-s] [-v]
selang [-l] [-o file] [-r file] [-s] [-v]
```

-c *command*

実行する selang コマンドを指定します。指定したコマンドの実行後に、selang が終了します。

command に空白が含まれる場合は、文字列全体を引用符で囲みます。以下に例を示します。

```
selang -c "showusr rosa"
```

-d *path*

定義したパスのデータベースが更新されるように指定します。

注: ローカル データベースのみを指定できます。

-f *file*

端末の標準入力からではなく、指定されたファイルから selang コマンドが読み取られるように指定します。

入力ファイルのコマンドが実行されると、実行中のコマンドの行番号が画面に表示されます。selang のプロンプトは表示されません。*file* に指定されたコマンドの実行後に、selang が終了します。

-h

このユーティリティのヘルプ画面を表示します。

--l

デフォルトのローカル データベースが更新されるように指定します。通常、このデータベースは *ACInstallDir*/seosdb です（*ACInstallDir* は CA Access Control をインストールしたディレクトリです）。

このオプションを -d または -p と同時に指定する必要はありません。

注: このオプションは selang に取って代わるものです。これは seosd が実行されていないときにのみ有効です。また、データベース ファイルを更新するための十分なネイティブ権限を持った CA Access Control 管理者のみ実行できます。

-o *file*

selang の出力が指定されたファイルに書き込まれるように指定します。selang を起動するたびに、新しい空のファイルが作成されます。既存のファイル名を指定した場合は、そのファイルの現在の情報が上書きされます。

-p *pmdb*

定義した PMDB のデータベース（PMDB サブディレクトリ内のデータベース）が更新されるように指定します。この場合、PMDB はローカル端末上に存在する必要があります。このデータベースに対する変更内容は、サブスクライバには伝達されません。

注: このオプションは、指定された PMDB 上で sepmdd または seosd のいずれかが実行されている場合は無効となります。また、*hosts* コマンドの使用とは異なります。

重要: サブスクライバへの伝達が必要な変更はこのモードで行わないでください。更新の作成時にネイティブ モードを使用すると、CA Access Control 設定オプションで定義されているように、ネイティブ ホスト ファイルのみが更新されます。

-r *file*

定義したファイルからコマンドが読み取られるように指定します。このファイルでは、標準の selang 構文で記述されたコマンドがセミコロンまたは改行記号で区切られている必要があります。*file* 内のコマンドが実行された後、ユーザに入力を促すメッセージが表示されます。

このオプションでファイルを定義しない場合は、ホーム ディレクトリの .selangrc ファイルが使用されます。

-s

selang がサイレント モードで開かれるように指定します。著作権に関するメッセージは表示されません。

-u *user pass*

（UNIX のみ）selang を実行するユーザ名およびパスワードを指定します。

このオプションを使用するには、seos.ini ファイルの check_password トークンを yes に設定する必要があります。これにより、selang -u を実行するときに、「パスワードを入力してください」というメッセージが表示されます。試行することができるログインは 3 回までです。

seos.ini ファイルの [lang] セクションにある no_check_password_users トークンには、selang へのログイン中にパスワード チェックを省略するユーザのリストが含まれます。

注: check_password トークンが no（デフォルト）に設定されている場合、パスワードの入力は要求されません。

-v

（Windows のみ）出力にコマンド ラインを書き込みます。

使用上の注意

- -h が使用されると、他のオプションはすべて無視されます。
- -c オプションを -f オプションと同時に使用することはできません。
- -d オプションを -p オプションと同時に使用することはできません。
- -d または -p を指定した場合、-l を指定する必要はありません。

seldapcred ユーティリティ - クレデンシャルの暗号化および格納

UNIX で該当

seldapcred ユーティリティは、提供したクレデンシャルを暗号化および格納します。クレデンシャルは、LDAP 対応の CA Access Control ユーティリティ（sebuildla など）で LDAP ディレクトリ情報ツリー（DIT）からデータを取得するために使用します。seos.ini ファイルの [seos] セクション内の ldap_userdn トークンの値と共に使用すると、LDAP サービスに対する認証を実行できます。認証を単純化するために、クレデンシャルは ldap_userdn 値に対応するパスワードとなります。SASL 認証の場合、クレデンシャルは異なる意味を持ちます。

暗号化されたクレデンシャルは、*ACInstallDir*/etc/ldapcred.dat に書き込まれます。

このコマンドの形式は以下のようになります。

```
seldapcred [-h] [-w [credential]]
```

-h

このユーティリティのヘルプ画面を表示します。

-w [*credential*]

暗号化および格納するクレデンシャルを指定します。指定しないと、値の入力を求めるメッセージが表示されます。このように対話モードを使用することで、他のユーザにクレデンシャルが公開されないようにすることができます。

詳細情報:

sebuildla ユーティリティ - lookaside データベースの作成 (P. 128)

seload ユーティリティ - CA Access Control のロードおよび起動

UNIX で該当

seload ユーティリティは、CA Access Control 拡張機能を UNIX カーネルにロードし、CA Access Control デーモンを起動します。seload ユーティリティを使用すると、CA Access Control デーモンをローカルまたはリモートでロードできます。また、UNIX カーネルに対する CA Access Control 拡張機能が、指定されたホストにロードされているかどうかも確認します。seosd が実行されていない場合、seload は指定されたホストのデーモンを起動します。-r スイッチおよびパラメータを省略すると、ローカル ホストで seosd デーモンが実行されます。

seosd、selogrd、selogrcd、または serevu のいずれかのデーモンをリモート ホストにロードするように指定できます。このプロセスは、トークンによって異なります。

CA Access Control がサーバ端末のブート シーケンスに指定されている場合は、seload を使用します。

注:

- CA Access Control のインストール時に、CA Access Control がサポートする各オペレーティング システムのサンプル初期設定ファイルが、*ACInstallDir*/samples/system.init ディレクトリに格納されます。システム初期化プロセスの一部として CA Access Control を起動する場合は、これらのファイルを使用します。
- seload ユーティリティでは、実行可能ファイル se_loadtest が *ACInstallDir*/lbin に格納されている必要があります (*ACInstallDir* はインストール ディレクトリ)。このプログラムは、UNIX カーネルに CA Access Control 拡張機能がロードされているかどうかを確認します。
- seload ユーティリティをリモートで操作する場合は、以下の条件を満たしている必要があります。
  - 実行可能ファイル rseloadd が CA Access Control の dir/lbin にあること。このプログラムは、リモート ホスト上で実行され、seload をアクティブにします。
  - ファイル /etc/services に seosload サービスが含まれていること。CA Access Control のインストール時に、このファイルを追加する必要があります。
  - ファイル /etc/inetd.conf に rseloadd プログラムが含まれていること。CA Access Control のインストール時に、このプログラムを追加できます。

このコマンドの形式は以下のようになります。

```
seload [-c] [-nopmd]  [-r host [daemon]]
```

-c

sechkey -r コマンドを実行して設定された暗号化鍵を変更します。

--nopmd

-c スイッチと -nopmd スイッチの両方を指定すると、Policy Model 更新ファイルが新しい鍵で更新されません。

-r *host* [*daemon*]

seosd デーモン、および seos.ini ファイルの [daemons] セクションに指定されている他のデーモンをロードします。

daemon を指定すると、そのデーモンのみが起動され、seos.ini のトークンは無視されます。デーモンの完全パスを指定する必要があります。

[daemons] セクションの seos.ini トークンは、値を指定した場合にのみ使用されます。デフォルト値はありません。値を指定すると、指定されたユーティリティまたはプログラムの標準値が、トークンの値に置き換わります。たとえば、selogrd の値を yes に指定すると、seosd デーモンの起動後に selogrd デーモンが自動的に起動します。

selock ユーティリティ - X 端末画面のロック

UNIX で該当

selock ユーティリティは、作業場所から離れている間、常に X 端末または端末を保護します。selock には、以下の 3 つの操作モードがあります。

- モニタ モード
- セーバ モード
- ロック モード

selock のデフォルト設定は、セーバ モードとロック モードの組み合わせです。

注: selock によるアイドル状態の端末のロックの詳細については、「*UNIX エンドポイント管理ガイド*」を参照してください。

このコマンドの形式は以下のようになります。

```
selock [-delay period] [-display hostname:display#.screen#] [-fodelay factor] ¥
    [-folevels levels] [-idelay seconds] [-lock-timeout minutes] ¥
    [-pixmapFile fileName] [-pw-timeout seconds]
```

-delay *period*

画面上のある位置にシステム アイコンを表示する時間の長さを指定します。この時間が経過すると、システム アイコンは消え、画面上の他の位置に移動します。これは標準のスクリーン セーバの動作であり、画面の焼き付きを防ぎます。時間はマイクロ秒で入力します。

時間を定義しない場合は、デフォルト値の 5000000（500 万）が使用されます。

-display *hostname:display#.screen#*

ロックするディスプレイ モニタを指定します。システムの X セッション リストで、ディスプレイおよび画面の番号を確認できます。ここで定義した代替ディスプレイ モニタを現在実行しているユーザの許可が必要です。

このオプションを定義しない場合、使用しているディスプレイがロックされます。

-fodelay *factor*

画面上に表示する各フェードアウト レベルの時間の長さを変更します。これにより、レベルの数を増やさずに、各ステップに費やす時間を延長できます。デフォルト値は 10 です。

-folevels *levels*

システム アイコンのフェードアウト ステップ数を指定します。フェードアウト レベル数を増やすと、フェードアウトの動作が滑らかになりますが、アイコンのフェードアウトに要する時間は長くなります。デフォルトのフェードアウト ステップ数は 20 です。

-help

selock のさまざまなオプションを説明するヘルプ画面を表示します。

-idelay *seconds*

ログインしてから監視を開始するまでの時間の長さ（秒単位）を指定します。selock が .login シェルの一部である場合は、最初にログインしてからシステムが正常に機能するまで、この時間が必要です。デフォルト値は 30 秒です。

-lock-timeout *minutes*

transparent=off の場合は、ロック モードに移行するまでのセーバ モードの時間の長さ(分単位)を指定します。

transparent=on の場合は、ロック モードに移行するまでのモニタ モードの時間の長さ(分単位)を指定します。

デフォルト値は 0 であり、セーバ モードを省略してただちにロック モードを開始します。

-pixmapFile *fileName*

画面がロックされ、transparent=on の場合に、背景に表示される XPM ファイルを指定します。

-pw-timeout *seconds*

パスワードのダイアログ ボックスを画面に表示する時間の長さを指定します。デフォルト値は 30 秒です。設定値が大きすぎると、X サーバで問題が発生するので注意してください。指定した制限時間内に正確なパスワードが入力されなかった場合、パスワード入力のダイアログ ボックスが閉じられ、selock はロック モードになります。

-segrace {on|off}

ユーザおよびパスワードの識別後、selock が segracex を起動するように指定します。ただし、ユーザ ID とパスワードが、seos.ini の [selock] セクションにある unlocking_user トークンに名前が設定されているユーザのものである場合、selock は segrace を起動しません。デフォルト値は off です。

注: segracex ユーティリティは、ユーザのパスワードが有効期限切れかどうかをチェックします。有効期限切れの場合は、新しいパスワードを指定できるダイアログ ボックスが表示されます。詳細については、「segrace ユーティリティ - UNIX でのユーザ ログイン設定の表示」を参照してください。

-timeout *minutes*

モニタ モードからセーバ モードに切り替わるまでの、操作が行われない時間の長さを指定します。デフォルト値は 10 分です。

-transparent {on|off}

ロック モードの場合、画面の内容を表示したままにするかどうかを指定します。「*on*」を指定すると、進行中のプロセスの表示および更新が続行されます。画面がロックされていることを示すには、-pixmapFile オプションで指定されたファイルの内容を表示することによって背景を変更します。
デフォルト値は *off* です。

-user *user-name*

ロック モードでユーザ アクティビティが検出された場合に、パスワードのダイアログ ボックスでパスワードの入力を促すユーザを指定します。デフォルト値は現在のユーザ名です。root のパスワードは、user オプションに指定したユーザ名に関係なく、受け入れられます。

-workhours（*hh*: *mm-hh*:*mm*）

ユーザが画面のロックを解除できる時間帯を指定します。指定された時間帯以外にキーボードやマウスを操作しても、パスワードのダイアログ ボックスは表示されません。

デフォルト値は 00:00-24:00 で、画面のロックはいつでも解除できます。

-xmin *pixels*

システム アイコンが一度に移動する最小水平方向距離をピクセル単位で指定します。デフォルト値は 100 です。

-xmax *pixels*

システム アイコンが一度に移動する最大水平方向距離をピクセル単位で指定します。デフォルト値は 300 です。

-ymin pixels

システム アイコンが一度に移動する最小垂直方向距離をピクセル単位で指定します。デフォルト値は 80 です。

-ymax pixels

システム アイコンが一度に移動する最大垂直方向距離をピクセル単位で指定します。デフォルト値は 250 です。

詳細情報:

segrace ユーティリティ - UNIX でのユーザ ログイン設定の表示 (P. 191)

selockcom ユーティリティ - selock ユーティリティの制御

UNIX で該当

selockcom ユーティリティは、現在アクティブな selock プロセスを制御します。selockcom ユーティリティを使用すると、selock の再起動や停止を行ったり、ロック モード、セーバ モード、およびモニタ モードの切り替えを行うことができます。

注: selock がロードされた場合は、selock と端末に付属しているスクリーン セーバとの間の競合状態または重複状態を避けるために、端末に付属しているスクリーン セーバが無効になります。selockcom に exit スイッチを付けて selock を停止すると、端末上でアクティブなスクリーン セーバはなくなります。標準の X コマンドである xset s on を使用すると selock または端末に組み込まれたスクリーン セーバを再起動できます。xset コマンドの詳細については、UNIX のマニュアルを参照してください。

このコマンドの形式は以下のようになります。

```
selockcom {-activate|-deactivate|-exit|-restart|-lock} ¥
    [-display hostname:display#.screen#]
```

--activate

事前に定義されたタイムアウト制限時間が経過する前に、selock をモニタ モードからセーバ モードに切り替えます。キーボードがロックされ、画面に CA Access Control のロゴが表示されます。

--deactivate

selock をモニタ モードに切り替えます。このスイッチは、selock プロセスへのユーザ入力をシミュレートします。selock が現在ロック モードの場合は、パスワードのダイアログ ボックスが表示されます。モニタ モードに戻るには、パスワードを入力します。selock がセーバ モードの場合は、モニタ モードに戻ります。

-終了

selock プロセスを終了します。sigterm シグナルを送信して selock を終了することもできます。最終手段として、sigkill シグナル(kill -9)を使用することもできます。この場合、selock は正常終了しません。したがって、通常は sigkill シグナル(kill -9)を使用しないでください。仮想 root ウィンドウ マネージャを実行している場合に kill -9 を使用すると、仮想ウィンドウを復元するためにウィンドウ マネージャを再起動する必要があります。

-再起動

selock プロセスを終了した後、以前の実行と同じコマンド ライン オプションで selock プロセスをただちに再開します。これは、selock を最後に起動した後でデータベースが変更された場合に、selock がリソース データベースを再度読み込むための便利な方法です。

-lock

現在の lock-timeout の値に関係なく、selock をロック モードに切り替えます。

-display *hostname*:*display#*.*screen#*

指定されたディスプレイで動作している selock プロセスを制御するように selockcom に指示します。このオプションによって、selock をリモート端末から制御できます。

システムの X セッションリストで、ディスプレイと画面の番号を確認できます。これを行うには、指定されたディスプレイ モニタを現在使用しているユーザの許可が必要です。デフォルトでは、ユーザが自分のディスプレイをロックすることを想定しています。

selogmix ユーティリティ - 監査ログ ファイルの分割および統合

UNIX で該当

selogmix ユーティリティは、CA Access Control の監査ログ ファイルを分割または統合します。

このコマンドの形式は以下のようになります。

```
selogmix {-s|-m} [-fn fileName] [-l fileName1 fileName2] ¥
    [-c weight1:weight2] [-t days] [-d] [-i]
```

-c *weight1*:*weight2*

ファイルを分割する場合にファイル サイズの比率を指定します。*weight1* は最初のファイルの相対的な大きさを示し、*weight2* は 2 番目のファイルの相対的な大きさを示します。このオプションを省略すると、1 対 1 の比率が使用されます。

-d

selogmix をデバッグ モードで実行するように指定します。このモードでは、すべての設定が表示されます。

-fn *fileName*

分割する監査ログ ファイルまたは統合されたファイルの名前を指定します。このオプションを省略すると、seos.ini ファイルの [logmgr] セクションにある audit_log トークンに指定されているファイル名が使用されます。

-h

このユーティリティのヘルプ画面を表示します。

-i

selogmix を対話モードで実行するように指定します。対話モードでは、既存のファイルを上書きする前に確認メッセージが表示されます。対話モードでない場合は、確認メッセージが表示されることなくファイルが上書きされます。

-l *fileName1 fileName2*

統合または分割に使用するファイルを指定します。

このオプションでは、2 つのファイル名を指定する必要があります。統合の場合は、統合する 2 つのファイルの名前を指定します。分割の場合は、分割後の 2 つのファイルの名前を指定します。このオプションを省略すると、seos.ini ファイルの audit_log トークンで指定されたファイル名が使用され、ファイル名の最後にシーケンス番号が追加されます。

-m

2 つの監査ログ ファイルを統合します。

-s

指定された監査ログ ファイルを分割します。

-t *days*

日数を指定します。このオプションは、ファイルを分割する場合にのみ使用できます。ログ記録の終了日からの日数を指定します。指定した日数分のログ記録が別ファイルに書き込まれます。このオプションを省略すると、過去 1 日分のログ記録が別ファイルに書き込まれます。

例

- ログ ファイルを同じサイズの 2 つのファイルに分割するには、以下のコマンドを使用します。

  ```
  selogmix -s
  ```

  元の監査ファイルは *ACInstallDir*/log/seos.audit という名前です。

  分割された新しいファイルは、*ACInstallDir*/log/seos.audit1 および *ACInstallDir*/log/seos.audit2 という名前になります。

- ログ ファイルから過去 2 日間のレコードを分割するには、以下のコマンドを使用します。

  ```
  selogmix -s -t 2
  ```

- 定義した比率でログ ファイルを 2 つのファイルに分割するには、以下のコマンドを使用します。

  ```
  selogmix -s -c 1:2
  ```

- 指定した 2 つのファイルを 1 つのファイルに統合するには、以下のコマンドを使用します。

  ```
  selogmix -m -l seos.audit1 seos.audit2 -fn seos.audit.merge
  ```

詳細情報:

seaudit ユーティリティ - 監査ログ レコードの表示 (P. 118)

semsgtool ユーティリティ - メッセージ ファイルの管理

semsgtool ユーティリティを使用すると、以下のことを実行できます。

- CA Access Control メッセージ ファイルから 1 つのメッセージを表示します。
- メッセージの 1 つのセクション全体を一覧表示します。
- ファイル全体を複数の ASCII ファイルにダンプします。各セクションにつき 1 つの ASCII ファイルが作成されます。
- 新しいメッセージ ファイルを作成します。
- メッセージを新しいメッセージに変更します。
- メッセージ(サブストリングを含む)を一覧表示します。
- メッセージ ファイルを検証します。

semsgtool を実行する場合は、一度に 1 つのコマンドのみを指定できます。

メッセージ ファイルのデフォルトの場所は、*ACInstallDir*/data/seos.msg です。

注: CA Access Control メッセージ ファイルは、セクションとメッセージ番号で構成されます。各セクションには、異なる CA Access Control モジュールまたはサブモジュールのメッセージが保存されています。

このコマンドの形式は以下のようになります。

```
semsgtool {-build|-b} asciiSourceFile OutputMessageFile

semsgtool {-change|-c} [messageFile] {0xerror-code|section# msg#} new-message

semsgtool {-dump|-d} messageFile

semsgtool {-list|-l} [messageFile] sectionNumber

semsgtool {-number|-n} [messageFile] subString

semsgtool {-show|-s} [messageFile] [0xerror-code|section# msg#]

semsgtool {-validate|-v} [messageFile]
```

-build|-b

ASCII ソース ファイルから新しい CA Access Control メッセージ ファイルを作成します。

-number|-n

メッセージ ファイル内の、定義された文字列を持つメッセージを一覧表示します。

-change|-c

messageFile.new という名前の新しいメッセージ ファイルを作成します。このファイルでは、指定されたメッセージに、変更された定義済み文字列が含まれます。

-dump|-d

メッセージ ファイルを複数のファイルにダンプします。1 つのセクションにつき 1 つのファイルが作成されます。作成された ASCII ソース ファイルは、後で新しい CA Access Control メッセージ ファイルを作成する際に使用できます。

-h

このユーティリティのヘルプ画面を表示します。

-list|-l

メッセージ ファイル内の指定したセクションにあるすべてのメッセージを一覧表示します。

-show|-s

特定のメッセージ コードに関連付けられているメッセージを表示します。

-validate|-v

（Windows のみ）重複したメッセージや、割り当てられた境界を越えたメッセージをチェックすることで、メッセージを検証します。

0x*error-code*

表示または変更するメッセージのエラー コードの 16 進数を定義します。

asciiSourceFile

ソース ファイルを ASCII 形式で定義します。そのファイルから新しいメッセージ ファイルが作成されます。

messageFile

メッセージ ファイルの名前を定義します。このオプションを省略すると、構成設定で指定されているメッセージ ファイルが使用されます。

OutputMessageFile

作成する新しいメッセージ ファイルの名前を定義します。

section# msg#

表示または変更するメッセージのエラー コードのセクション番号およびメッセージ番号を定義します。

sectionNumber

すべてのメッセージを一覧表示するセクションのセクション番号を定義します。

例

- エラー コード 0x205 に関連付けられたメッセージを一覧表示するには、以下のコマンドを入力します。

```
semsgtool -s seos.msg 0x205
```

- メッセージをセクション 512 に一覧表示するには、以下のコマンドを入力します。

```
semsgtool -l seos.msg 512
```

- 変更された CA Access Control メッセージ ファイルを作成するには、以下の手順に従います。

  1. 変更されたメッセージを使用して新しいメッセージ ファイルを作成します。

     ```
     semsgtool -c 0x2501 "This is the new message"
     ```

     変更されたメッセージを含む新しいメッセージ ファイル seos.msg.new が作成されます。

  2. この新しいファイルを CA Access Control メッセージ ファイルにコピーします。

     ```
     copy seos.msg.new seos.msg
     ```

     変更されたメッセージを含む新しいメッセージ ファイルをコピーして、古い seos.msg ファイルの上部に追加します。

- エラー コード 0x0205 に関連付けられたメッセージを表示するには、以下のコマンドを入力します。

  ```
  semsgtool -s 0x205
  ```

senable ユーティリティ - 無効なユーザ アカウントの有効化

UNIX で該当

senable ユーティリティは、何らかの理由で無効にされたユーザのログインを、ユーザが無効にされた場所（PMDB を含む）で有効にします。たとえば、ユーザが無効にされる理由として、serevu デーモンによる無効化や、設定されていたユーザ アカウントの一時停止日または失効日による無効化があります。

ユーザ アカウントを有効にした後、senable は sepass ユーティリティを呼び出します。これにより、新しいユーザ パスワードの入力を促すメッセージが表示されます。最後に使用されていたパスワードを復元するには、-n オプションを使用します。

senable ユーティリティは、ローカルの /etc/passwd ファイルから該当するアカウントを削除することによって、未定義のユーザ アカウントを有効にします。

senable をリモートで実行するには、リモート端末にアクセスするための WRITE 権限を与えるルールにユーザのローカル端末を明示的に記述する必要があります。記述がない場合は、リモート端末で CA Access Control の管理を実行することはできません。

注: リモート管理の制限の詳細については、「*UNIX エンドポイント管理ガイド*」を参照してください。

このコマンドの形式は以下のようになります。

```
senable [-host hostname] userNames [-n]
```

-host *hostname*

アカウントを無効から有効に変更するホストを選択します。

-host オプションを使用するには、以下の 2 つのホストで ADMIN 属性または PWMANAGER 属性が必要です。

- アカウントを無効から有効に変更するホスト
- senable コマンドを入力するホスト

-h

このユーティリティのヘルプ画面を表示します。

-n

非対話式でコマンドを実行します。このオプションを使用すると、senable は sepass を呼び出す代わりに、最後に使用されていたパスワードを復元します。

userNames

無効から有効に変更する複数のアカウントのユーザ名を指定する、スペース区切りリストを定義します。

詳細情報:

serevu ユーティリティ - 失敗したログイン試行の処理 (P. 251)

senone ユーティリティ - 権限のないユーザとしてコマンドを実行

UNIX で該当

senone ユーティリティは、上位の権限を持つユーザが発行したコマンドを、権限のないユーザ プロセスとして実行します。

注: このユーティリティは、上位権限を持ち、untrusted プログラムをテストするユーザのみが使用してください。

senone ユーティリティを起動すると、認証デーモンからプロセス クレデンシャルが削除されます。senone は、CA Access Control に定義されていないユーザのクレデンシャルでシェルを実行します。これ以降、このシェルの内部から起動されたプログラムは、CA Access Control ユーザ以外のクレデンシャルで実行されます。senone は起動したユーザの ID を変更しないため、ユーザの UNIX 権限は変わりません。

重要: root ユーザとしてログインした場合は、untrusted プログラムを実行しないことをお勧めします。senone で untrusted プログラムを実行した場合でも、予期しない障害が発生する可能性があります。

コマンドを指定せずに senone を起動すると、/etc/passwd に定義されているユーザのシェルが実行されます。

このコマンドの形式は以下のようになります。

senone [*command*]

-h

このユーティリティのヘルプ画面を表示します。

command

権限のないユーザとして実行するコマンドを指定します。

詳細情報:

sesu ユーティリティ - ユーザの代替 (P. 254)
sewhoami ユーティリティ - UNIX での CA Access Control ユーザ名およびセキュリティ クレデンシャルの表示 (P. 265)

SEOS_load ユーティリティ - CA Access Control インターセプト モジュールのロード

UNIX で該当

SEOS_load ユーティリティは、動的な CA Access Control カーネル モジュール（SEOS_syscall）を制御します。インターセプト モジュールは、CA Access Control ユーティリティを実行する前にロードする必要があります。

注: UNIX exit を使用して、カーネルのロードとアンロードの前および後にプログラムを自動的に実行することができます。

streams がサポートされたプラットフォームでは、SEOS_load ユーティリティは、seos.ini ファイルの [SEOS_syscall] セクションにある SEOS_use_streams トークンに応じて CA Access Control モジュールを streams にロードします。トークンが yes に設定されている場合、モジュールは streams にプッシュされます。

このコマンドの形式は以下のようになります。

```
SEOS_load [-i|-k|-s|-u]
```

-i

（HP-UX および Sun Solaris プラットフォームのみ）CA Access Control のカーネル拡張機能に関する情報を表示します。

-k

（HP-UX および Sun Solaris プラットフォームのみ）CA Access Control モジュールを streams にプッシュせずにカーネルにロードします。

-s

(HP-UX および Sun Solaris プラットフォームのみ) CA Access Control カーネル モジュールを streams に挿入します。このオプションによって、seos.ini ファイルの SEOS_syscall セクションにある SEOS_use_streams トークンが無視されます

-u

CA Access Control のカーネル拡張機能をカーネルからアンロードして、streams からモジュールを削除します。

注: CA Access Control 上にロードされているアプリケーションに、CA Access Control によってフックされるオープン システム コール (syscall) がある場合は、CA Access Control をアンロードできません。*secons -sc* または *secons -scl* を使用して、こうしたプロセスを検出します。検出されたプロセスを停止した後、CA Access Control カーネル モジュールをアンロードできます。また、UNIX exit を使用すると、検出されたプロセスをカーネルのアンロード前に自動的に停止し、カーネルのアンロード後に自動的に再開することができます。

sepass ユーティリティ - パスワードの設定または変更

UNIX で該当

sepass を使用して、ローカル ホスト、Policy Model、または NIS/NIS+ サーバで必要に応じて新しいパスワードを設定したり、既存のパスワードを更新できます。

sepass ユーティリティは、ユーザのパスワードを変更します。また、特権ユーザは、sepass を使用して他のユーザのパスワードを変更することもできます。自分のパスワードを変更する場合は、古いパスワードの入力を促すメッセージが表示されます。

注: seosd が実行されていない場合、sepass はデフォルトのパスワード プログラムを実行します。デフォルトのパスワード プログラムは、seos.ini ファイルの passwd セクションにある DefaultPasswdCmd トークンで指定されます。パスワードは暗号化された状態で保存され、ネットワーク上で転送されます。

このコマンドの形式は以下のようになります。

```
sepass [-d] [-l] [-p] [-s policy_model@hostname] ¥
    [-g number] [-x] [userName]
```

-d

パスワード更新に関するすべての情報が表示されます。更新が正常に行われた端末や、パスワードの品質がチェックされなかった（setoptions class+(PASSWORD) を有効にしなかった場合）などの情報が表示されます。このスイッチは、デバッグ時に有用です。

-g *number*

userName の猶予ログイン回数を定義します。

-h

このユーティリティのヘルプ画面を表示します。

--l

ローカル パスワード ファイル（通常は /etc/passwd）、セキュリティ ファイル、ローカル データベースなどのローカル端末上でのみパスワードを更新します。

NIS/NIS+ 環境では、ユーザはクライアントの /etc/passwd ファイルに通常は定義されません。したがって、クライアント端末上のパスワードは更新されません。

NIS/NIS+ サーバ端末の場合、パスワードはローカルで更新され、NIS/NIS+ サーバによって伝達されます。

このスイッチと -p スイッチおよび -s スイッチは、いずれか 1 つのみを選択できます。

-p

リモート端末およびスイッチで指定されたホストの PMDB 上でのみパスワードを変更します。このスイッチと -l スイッチおよび -s スイッチは、いずれか 1 つのみを選択できます。

-s *policy_model@hostname*

ローカル端末およびスイッチで指定されたホストの PMDB 上でのみパスワードを変更します。このスイッチと -l スイッチおよび -p スイッチは、いずれか 1 つのみを選択できます。

-x

ユーザ *username* が変更した場合と同じようにパスワードを置き換えます。データベースを最後に変更した日時が *更新され*、猶予ログインが終了します。

注: root ユーザが変更したかのように root パスワードを変更するには、RootPwAsOwn を適切に設定する必要があります。seos.ini トークンの詳細については、「リファレンス ガイド」を参照してください。

username

(オプション) sepass によってパスワードが変更されるユーザの名前を指定します。userName を省略すると、自分のパスワードが設定されます。

例

以下の例は、sepass をさまざまな状況で使用する方法を示しています。

- ローカル ホスト上で自分のパスワードを変更するには、以下のコマンドを入力します。

  ```
  sepass -l
  ```

  注: サイトに PMDB が定義されていない場合は、-l スイッチを省略できます。サイトで PMDB が使用中の場合は、-l スイッチを省略すると、PMDB のすべてのサブスクライバ データベースにある自分のパスワードが変更されます。NIS/NIS+ クライアントでは、このスイッチを指定してもパスワードは変更されません。NIS/NIS+ サーバでは、パスワードは変更された後に伝達されます。

- 自分以外のユーザのパスワードをローカル ホスト上でのみ変更するには、以下のコマンドを入力します。

  ```
  sepass -l username
  ```

  username は、/etc/passwd ファイル、適切な UNIX セキュリティ ファイル、およびデータベースに存在するユーザである必要があります。

  NIS/NIS+ クライアントでは、パスワードは変更されません。NIS/NIS+ サーバでは、パスワードは変更された後に伝達されます。

- NIS が使用されていないサイトにある複数端末のユーザのパスワードを変更するには、以下の手順に従います。

  1. PMDB を作成します。

     注: PMDB の作成の詳細については、「*UNIX エンドポイント管理ガイド*」を参照してください。

  2. サブスクライバ コンピュータに詳細情報を配布する必要があるすべてのユーザを PMDB の UNIX 環境および CA Access Control 環境に追加します。

  3. 更新されたパスワードを受け取るすべての端末を PMDB にサブスクライブします。

  4. すべてのサブスクライバで、seos.ini ファイルの [seos] セクションにあるトークンを PMDB の名前に設定します。以下に例を示します。

     ```
     passwd_pmd = PMD1@morocco
     parent_pmd = PMD1@casablanca
     ```

  5. 以下のコマンドを入力します。

     ```
     sepass username
     ```

     sepass の実行が完了すると、すべてのサブスクライバ データベースで、ユーザのパスワードが変更されます。

sepmd ユーティリティ

sepmd ユーティリティは、Policy Model 管理ユーティリティです。

sepmd ユーティリティを使用すると、以下のタスクを実行できます。

- サブスクライバおよび更新ファイルの管理
- デュアル コントロールの管理
- Policy Model のログ ファイルの管理
- PMDB の管理
- PMDB のバックアップ
- PMDB のリストア

注: sepmd ユーティリティは、Policy Model が格納されているホストで実行する必要があります。

詳細情報:

sepmd ユーティリティ - サブスクライバおよび更新ファイルの管理 (P. 223)
sepmd ユーティリティ - デュアル コントロールの管理 (P. 227)
sepmd ユーティリティ - PMDB のバックアップ (P. 229)
sepmd Utility - Policy Model のログ ファイルの管理 (P. 232)
sepmd ユーティリティ - PMDB の管理 (P. 233)
sepmd ユーティリティ - PMDB の管理 (P. 235)

sepmd ユーティリティ - サブスクライバおよび更新ファイルの管理

sepmd ユーティリティは、サブスクライバの作成、削除、および割り当てを実行します。

このコマンドの形式は以下のようになります。

```
sepmd {-C|-de|-l|-L|-p|-R} pmd

sepmd {-n|-r|-u} pmd subscriber

sepmd -s pmd subscriber offset

sepmd -sm pmd mf_subscriber mf_type mf_sysid mf_admin offset

sepmd -t pmd {auto|offset}
```

-C

更新ファイル内のすべてのコマンド、および各コマンドのオフセットを表示します。オフセットは、ファイル内での更新の位置を示します。別のデータベースまたは PMDB をサブスクライブするときにこの位置を指定することができます。

-de

(UNIX のみ)暗号化された updates.dat ファイルの情報の暗号を解除します。updates.dat ファイルのデータは、UseEncryption PMDB 構成設定を yes に設定している場合に暗号化されます。

-l

Policy Model のサブスクライバを一覧表示します。

-L

Policy Model およびそのステータスを一覧表示します。エラーの数、可用性、オフセット、同期モード、次に伝達するコマンドなどの情報が表示されます。更新ファイルには、Policy Model によって伝達する必要がある更新情報、またはすでに伝達済みの更新情報がすべて保存されます。オフセットは、サブスクライバに送信する必要がある次の更新情報の位置を示します。初期オフセットと最新のオフセットも表示されます。

-n

新しいサブスクライバを作成した後、そのサブスクライバを Policy Model に対応して遡及的に更新します。サブスクライバの更新に適用する一般ルールについては、-s オプションの説明を参照してください。

注: このオプションによって、LOGINAPPL オブジェクト(UNIX のみ)および SPECIALPGM オブジェクトを含む PMDB 全体の内容が新しいサブスクライバに送信されます。サブスクライバのオブジェクトが親のオブジェクトと異なる場合は、これらのオブジェクトを除外できます。

-n オプションは、ターゲット サブスクライバ データベース定義上の Policy Model データベース定義を置換せず、代わりに既存の Policy Model に追加します。ターゲット データベースに追加のリソースまたは属性が含まれている場合、サブスクリプションが完了した後、新しい Policy Model がそれらを削除することはしません。

-n を指定して追加されたサブスクライバには、*sync* というマークが付けられます。これは、このサブスクライバが現在同期モードの状態にあり、すべての PMDB ルールを受け取ることを示します。すべてのルールを受け取ったサブスクライバは、同期モードから解放され、標準サブスクライバになります。-n オプションの処理には時間がかかる場合があります。複数の更新情報または矛盾する更新情報がある場合は、最新の更新情報が使用されます。

重要: *sepmd -n* を使用して、CA Access Control エンドポイントまたは PMDB を別の PMDB にサブスクライブする場合は、新しいサブスクライバにすでに存在しているポリシー(POLICY オブジェクト名)を新しい親 PMDB に含めないようにしてください。サブスクライバから既存の各ポリシーをデプロイ解除した後、POLICY オブジェクトおよびリンクされた RULESET オブジェクトをサブスクライバから削除してから、新しい親 PMDB にポリシーをサブスクライブしてください。

UNIX では、seos.ini ファイルにある send_unix_env トークンを yes に設定した場合、-n オプションを設定すると、Policy Model のパスワード ファイルおよびグループ ファイルの内容も送信されます。コマンドを確実に送信するために、dbmgr -export -l を実行してデータベースの内容を確認することをお勧めします。

-p

格納されている Policy Model およびそのステータスを一覧表示します。

-r

sepmdd によって管理されている使用不可のサブスクライバのリストからサブスクライバを削除し、そのサブスクライバをただちに更新できるようにします。通常、サブスクライバが停止状態で、そのため Policy Model から更新情報を受け取れない場合、sepmdd は一定時間待機した後にそのサブスクライバに更新情報を送信します。ただし、このオプションを指定した場合、sepmdd は待機せず、ただちに更新情報をサブスクライバに送信します。

-R

すべてのサブスクライバを実際のオフセットで更新します。

-s

他のデータベースまたは PMDB を Policy Model にサブスクライブします。ホストを Policy Model にサブスクライブする場合は、そのホストが稼動しており、CA Access Control がそのホスト上で実行中であることが必要です。さらに、PMDB は、サブスクライブされるホストの親 PMDB である必要があります。この関係は、サブスクライバの構成設定の parent_pmd トークンで設定します。このトークンでは、ホストをサブスクライブする PMDB の名前を指定する必要があります。

Policy Model を別の Policy Model にサブスクライブする場合は、以下の要件を満たす必要があります。

- サブスクライブされる Policy Model の pmd.ini ファイルの parent_pmd トークンに、サブスクライブ先の Policy Model（その親 Policy Model）の名前が指定されていること。
- サブスクライブされるポリシーが格納されているホスト上で CA Access Control が実行中であること。

通常、PMDB の親は 1 つだけ設定します。複数の親を持つ Policy Model を設定する場合は、親 Policy Model のリストを含むファイルの名前を parent_pmd トークンに指定します。ただし、複数のソースからの信頼性の低い情報がデータベースに氾濫するおそれがあるため、複数の親を設定しないことをお勧めします。

-sm

メインフレーム サブスクライバを Policy Model に割り当てます。

-t

更新ファイルからエントリを削除することで、更新ファイルを切り捨てます。

注: UNIX では、force_auto_truncate PMDB 設定が no に設定されている場合、sepmd -t を指定しても更新ファイルは切り捨てられません。このトークンが yes に設定されていると、Policy Model のサブスクライバが存在しない場合でも、更新ファイルが切り捨てられます。

- *offset* (手動による切り捨て)を使用している場合は、-L パラメータ付きで sepmd を実行するとオフセットを検索できます。

  注: ファイルを切り捨てるには、開始オフセットから減算した結果のオフセットではなく、-L パラメータによって取得した正確なオフセットを使用する必要があります。

- auto を使用している場合は、まだ伝達されていない最初のエントリのオフセットが計算され、その前にあるすべてのエントリが削除されます。auto を使用すると、-L パラメータを指定してユーティリティを実行する手順を省くことができます。

サブスクライバが、指定されたオフセットより前にあるすべての更新情報の一部しか受け取れなかった場合は、エラー メッセージが表示され、ファイルの切り捨ては行われません。すべての場合にファイルの切り捨てを実行する場合は、以下の操作を実行します。

- 更新されなかったホストのサブスクライブを解除します。
- ファイルを切り捨てます。
- ホストを Policy Model に再度サブスクライブします。

この操作を行った場合、サブスクライバは、Policy Model からの更新の受け取りに 1 回以上失敗します。サブスクライバのオフセットは、更新ファイルの最後のオフセットに変更されます。

-u

Policy Model のサブスクライバ リストからサブスクライバを削除します。

auto

まだ伝達されていない最初のエントリのオフセットを計算し、その前にあるすべてのエントリを削除するように sepmd に指示します。

offset

-s オプションまたは -sm オプションと同時に使用して、新たに追加されたサブスクライバが更新の受け取りを開始する更新ファイル内のポイントを指定します。

-t オプションと同時に使用して、更新ファイルの先頭から特定のサブスクライバの位置までの距離を指定します。

有効な更新オフセットを表示するには、-C オプションを使用します。更新中のオフセットを指定した場合、そのオフセットは次の更新の先頭に移動します。無効なオフセット(最初のオフセットよりも小さいか、最後のオフセットよりも大きい)を指定した場合、エラー メッセージが表示されます。

pmd

Policy Model の名前を指定します。

subscriber

サブスクライバ端末、またはサブスクライバ PMDB のホストを指定します。

sepmd ユーティリティ - デュアル コントロールの管理

UNIX で該当

sepmd ユーティリティは、デュアル コントロール トランザクションを管理します。このユーティリティは、トランザクションの作成時に各トランザクションに一意の ID 番号を割り当てます。

注: デュアル コントロールの詳細については、「*UNIX エンドポイント管理ガイド*」を参照してください。

デュアル コントロールを使用する場合は、PMDB の名前を *maker* とする必要があります、また、PMDB および CA Access Control の両方に関して、is_maker_checker 構成設定の値を yes に設定する必要があります。

このコマンドの形式は以下のようになります。

```
sepmd -m {l|la|lo}

sepmd -m {d|r} transactionId

sepmd -m p transactionId code
```

--m d

トランザクションを削除します。トランザクションとは、PMDB 上で実行する前に承認が必要な 1 つ以上のコマンドのことです。トランザクションを作成したユーザのみがそのトランザクションを削除できます。

-m l

コマンドを起動したユーザの未処理トランザクション（Checker（チェッカ）を待機）を一覧表示します。各トランザクションは、トランザクション ID 番号、Maker（トランザクションを作成したユーザであり、この場合はコマンドを起動したユーザと同じユーザ）の名前、およびその説明（ある場合）と共に一覧表示されます。

-m la

すべての Maker（作成者）のすべての未処理トランザクションを一覧表示します。各トランザクションは、トランザクション ID 番号、Maker（作成者）の名前、およびその説明（ある場合）と共に一覧表示されます。

-m lo

コマンドを起動したユーザのトランザクションを除き、すべての Maker（作成者）の未処理トランザクション（Checker（チェッカ）を待機）を一覧表示します。

-m p

トランザクションを処理します。Checker（トランザクションを作成した Maker（作成者）以外のすべての admin ユーザ）が ID 番号を入力すると、指定されたトランザクションのすべてのコマンドがリストに表示されます。

このオプションは、以下の状況では機能しません。

- トランザクション内の 1 つ以上のコマンドが、コマンドを起動したユーザに関係する場合。
- トランザクションが別の Checker（チェッカ）によってロックされている場合。
- トランザクションがコマンドを起動したユーザによって作成された場合。Maker（作成者）は自分のトランザクションの Checker（チェッカ）にはなれません。
- 指定されたトランザクション ID が存在しない場合。
- コマンドを起動したユーザが Checker（チェッカ）になる権限を持っていない場合。

--m r

トランザクションの取得またはロックを実行します。

- トランザクションを作成したユーザ（Maker）の場合は、このパラメータで特定の未処理トランザクションを取得します。取得したトランザクションは、適切なファイルに送信し、ASCII エディタ（vi、emacs など）を使用して更新できます。
- Maker（作成者）でも Checker（チェッカ）でもないユーザの場合は、このパラメータで処理前のトランザクションをロックします。ロックされたトランザクションは変更できません。

transacationID

トランザクションの作成時に割り当てられる一意の ID 番号を指定します。

code

Checker（チェッカ）がトランザクションの処理時に何を実行する必要があるかを、以下のように数値コードで指定します。

0

トランザクションを拒否します。この場合、トランザクション内のすべてのコマンドが削除され、PMDB では変更が実行されません。

1

トランザクションを許可します。この場合、コマンドはただちに PMDB で実行されます。

2

トランザクションのロックを解除します。ロックを解除したトランザクションは、後から処理するか、異なる Checker（チェッカ）で処理できます。

sepmd ユーティリティ - PMDB のバックアップ

sepmd ユーティリティを使用すると、Policy Model データベースをバックアップできます。

このコマンドの形式は以下のようになります。

```
sepmd {-bl|-ul} pmd

sepmd -bd pmd destination

sepmd -bh pmd destination backup_host
```

-bd

pmd をディレクトリ *destination* にバックアップします。

-bh

pmd を階層構造の Policy Model のディレクトリ *destination* にバックアップします。つまり、バックアップにより PMDB サブスクライバが変更されるため、バックアップが *backup_host* ホストに移動しても、サブスクリプションは引き続き機能します。

--bl

pmd をロックすることによって、コマンドをサブスクライバに伝達しないようにします。

このオプションは、Policy Model にサブスクライバがあり、バックアップ中は更新を受け取らないようにする場合に使用します。

-ul

ロックされた *pmd* のロックを解除します。

backup_host

バックアップ ホストの移動先となるホストの名前を定義します。

destination

PMDB ファイルのバックアップ先となるディレクトリの名前を定義します。

pmd

Policy Model データベースを定義します。Policy Model データベースは、_pmd_directory_ 構成設定で指定された場所にあります。

例: PMDB のバックアップ

以下のコマンドは、myPMDB という名前の PMDB を /tmp/my_pmdb ディレクトリにバックアップします。

```
sepmd -bd pmdb /tmp/my_pmdb
```

必要に応じて、PMDB を以下のように管理できます。

```
selang -d /tmp/my_pmdb
```

例: サブスクライバがある PMDB のバックアップ

以下のコマンドは、サブスクライバがある PMDB をバックアップした後、その PMDB を別のホストに移動する方法を示しています。

1. PMDB のロック

   ```
   sepmd -bl mainPMDB
   ```

   更新の送受信が行われないように、CA Access Control によって PMDB がロックされます。

2. PMDB のバックアップ

   ```
   sepmd -bh mainPMDB /tmp/my_pmdb host63
   ```

   CA Access Control によって、PMDB が /tmp/my_pmdb にバックアップされます。

   UNIX では、指定したバックアップ ホスト名で subscribers.dat が更新されます。

   Windows では、*pmd*.reg ファイルが作成されます。このファイルは、指定した新しいホストに一致するように変更された Parent_Pmd 構成設定値を持つ *pmd* レジストリ設定のダンプです。

3. PMDB のロック解除

   ```
   sepmd -ul mainPMDB
   ```

   CA Access Control によって PMDB のロックが解除されます。

4. PMDB バックアップを新しいホストに転送します。

   注: 新しいホストには、現在のコンピュータと同じ OS および CA Access Control バージョンがインストールされている必要があります。

5. (Windows のみ) 新しいホスト上のレジストリに mainPMDB.reg ファイルをインポートします。

   これにより、通常どおりに PMDB を使用し続けることができます。

sepmd Utility - Policy Model のログ ファイルの管理

sepmd ユーティリティは、Policy Model のログ ファイルを管理します。Policy Model のログ ファイルには、Policy Model データベースのアクティビティの詳細な監査証跡が記録されています。以下に例を示します。

```
Wed Nov  4 10:08:02 2003 pmdb1:Processing list request for missouri.yourco.com
Wed Nov  4 10:08:02 2003 pmdb1:Processing list request for oregon.yourco.com
Wed Nov  4 10:09:14 2003 pmdb1:Empty request
Wed Nov  4 10:09:15 2003 pmdb1:Processing shutdown request
Wed Nov  4 10:09:15 2003 pmdb1:Delete filters
Wed Nov  4 10:10:04 2003 pmdb1:Opened error logs
Wed Nov  4 10:10:04 2003 pmdb1:Try to load filters
Wed Nov  4 10:10:04 2003 pmdb1:Filters file : nis_filter.dat
```

Policy Model のログ ファイルは、sepmdd を初めて実行したときに自動的に作成されます。

UNIX では、pmd_log_level PMDB 構成設定を使用して、PMDB のログに何を記録するかを以下のように制御できます。

- **0** - エントリを記録しません
- **1** - エラー メッセージのみを記録します。
- **2** - エラー メッセージおよび情報メッセージを記録します（デフォルト値）。

注: ファイル サイズの制限値を超えると、ログ ファイルに警告メッセージが記録されます。ログ ファイルのサイズが小さすぎる場合は、構成設定を使用して増やすことができます。

このコマンドの形式は以下のようになります。

```
sepmd {-sl|-kl|-dl|-cl} pmd
```

-cl

Policy Model のログ ファイルの内容を消去します。

-dl

Policy Model のログ ファイルを表示します。

-kl

Policy Model のログ ファイルを使用不可にします。

-sl

Policy Model のログ ファイルを使用可能にします。

pmd

Policy Model の名前を指定します。

sepmd ユーティリティ - PMDB の管理

sepmd ユーティリティは、Policy Model を停止および開始します。UNIX では、Policy Model に影響を与える構成設定を再ロードすることもできます。

注: UNIX とは異なり、Windows では、sepmd による Policy Model サービスの停止および再開は行われません。代わりに、Policy Model をアクティブ化および非アクティブ化することができます。

sepmd を使用して Policy Model を開始または問い合わせるには、Policy Model で ADMIN 権限が設定されている必要があります。

このコマンドの形式は以下のようになります。

`sepmd {-c|-e|-k|-S} pmd`

`sepmd -tm seconds`

-c

Policy Model のエラー ログを消去します。

--e

Policy Model のエラー ログを表示します。

-k

UNIX では、Policy Model デーモンを安全に停止します。Windows では、Policy Model サービスを非アクティブ化します。

注: UNIX で kill コマンドを使用して Policy Model デーモンを停止しないでください。

-ri

UNIX では、sepmdd の実行中に、Policy Model および CA Access Control 設定ファイル（pmd.ini ファイルと seos.ini ファイル）が再ロードされます。このオプションは、1 分以上の間隔で使用できます。このオプションでは、parent_pmd、_retry_timeout_、_min_retries_、および_shutoff_time_の各トークンで行われた環境設定の変更がチェックされます。

Windows では、Policy Model 情報をレジストリからホストに再ロードします。変更したデータをホスト PMDB に確実に送信する場合に、このオプションを使用します。

-S

UNIX では、Policy Model デーモンを開始します。Windows では、Policy Model サービスをアクティブ化します。

このオプションは、これ以外に実行するコマンドがない場合にデーモンを起動するために使用します。

-tm *seconds*

（Windows のみ）実行された要求に対する最初のタイムアウト間隔（秒単位）を設定します。

pmd

Policy Model の名前を指定します。

sepmd ユーティリティ - PMDB の管理

restorepmd コマンドは、ローカル ホスト上の PMDB をリストアします。PMDB のリストアに使用するバックアップ ファイルは、リストア ホストと同じプラットフォーム、オペレーティング システム、および CA Access Control バージョンが動作するホストに存在する必要があります。また、リストア ホスト上で CA Access Control が実行中である必要があります。

注: PMDB を別の端末にバックアップおよびリストアする場合、PMDB はリストアされた PMDB データベースにあるターミナル リソースの更新を、自動的には行いません。新しいターミナル リソースはリストアされた PMDB に追加する必要があります。新しい端末リソースを追加するには、リストアされた PMDB を停止して「*selang -p pmdb*」をコマンド実行します。その後、リストアされた PMDB を起動します。

このコマンドの形式は以下のようになります。

```
sepmd -restore pmd [-source path] [-admins user[,user...]]¥
[-xadmins user[,user...]] [-parent_pmd name[,name...]]
```

-restore

ローカル ホスト上の PMDB をリストアします。

-admins *user*[,*user*...]

(UNIX)リストアされた PMDB の管理者として内部ユーザを定義します。

-parent_pmd *name*[,*name*...]

(オプション)リストアされた PMDB の親の名前を定義します。親 PMDB は「*pmdb@host*」という形式で指定します。

pmd

リストアする PMDB の名前を定義します。

-source(*path*)

(オプション)バックアップ ファイルが配置されているディレクトリを定義します。ソース ディレクトリを指定しない場合、PMDB はデフォルトの場所にあるファイルからリストアされます。デフォルトの場所は「*_pmd_backup_directory_*」トークンで定義されます。

デフォルト: (UNIX) *ACInstallDir*/data/policies_backup/pmdName

デフォルト: (Windows) *ACInstallDir*/data/policies_backup/pmdName

-xadmins *user*[,*user*...]

(UNIX)リストアされた PMDB の管理者としてエンタープライズ ユーザを定義します。

sepmdadm ユーティリティ - PMDB 定義の作成

UNIX で該当

sepmdadm ユーティリティは、PMDB の実行に必要な定義を作成します。sepmdadm ユーティリティは、PMDB の定義、PMDB とその上位および下位にある PMDB との関係の定義、およびサブスクライバ端末の定義に必要な CA Access Control と UNIX のコマンドで構成されるスクリプトです。デフォルトでは、root ユーザは、PMDB の管理者および監査担当者として定義されます。sepmdadm ユーティリティは、リモート シェルから実行することもできますが、ローカルで実行する必要があります。sepmdadm を使用して新しい PMDB を作成する場合は、サブスクライバからの PMDB の参照、および UID と GID の同期の指定が可能です。

このユーティリティは、対話モードまたは非対話モードのどちらでも実行できます。

- 非対話モードでは、コマンド ラインに引数を入力します。指定された値に従って、PMDB とその階層が作成されます。
- 対話モードでは、コマンド ラインに引数を入力しません。対話モードで実行するかどうかの確認を求めるメッセージが表示されます。「y」と応答すると、オプション値の入力を促すメッセージが表示されます。

sepmdadm で新しい PMDB を作成する場合は、Policy Model のサブスクライバとなる端末を指定します。ただし、各サブスクライバの seos.ini ファイルにある parent_pmd トークンを、その端末をサブスクライブした PMDB の名前で更新する必要があります。これを行わないと、サブスクライバは PMDB からの更新情報を受け取りません。

複数の端末を同じ PMDB にサブスクライブし、ある PMDB 端末を別の PMDB 端末にサブスクライブすることによって、PMDB の階層を作成できます。

このコマンドの形式は以下のようになります。

`sepmdadm options`

--admin *name*

PMDB の CA Access Control 管理者を定義します。

--auditor *name*

PMDB の CA Access Control 監査者を定義します。

-c | --clean *pmdbName*

指定した Policy Model を削除します。Policy Model デーモンを停止し、データベースからファイル保護を削除して、Policy Model のディレクトリとその内容をすべて削除します。

このオプションは、--noconfirm オプションと同時に指定できません。

--desktop *hostname*

管理者がローカル ホスト上にある PMDB を管理できる端末を指定します。端末を指定しない場合、管理者はローカル ホストからのみ PMDB を管理できます。

--group_fname *fileName*

NIS のグループ ファイルの場所を定義します。

-h | --help

ヘルプ画面を表示します。

-i | --interactive

対話モードで sepmdadm を実行します。

-l

sepmdadm をローカル モードで実行するように指定します。つまり、CA Access Control が実行されていないときに PMDB を作成できます。

注: このオプションを指定しない場合は、sepmdadm を使用するときに CA Access Control が実行中である必要があります。

--nis | --NIS

Policy Model で NIS の設定を実行します。PMDB が NIS サーバにインストールされている場合は、このオプションを使用する必要があります。

--noconfirm

ユーザに応答の確認を求めないように指定します。このオプションは、非対話モードでシェル スクリプト内から sepmdadm を起動するときに便利です。

--parentpmd *pmdbName*

この PMDB をサブスクライブする親 PMDB の名前を指定します。このパラメータを -subsconfig パラメータと同時に指定すると、seos.ini ファイルの parent_pmd トークンが更新されます。このパラメータを --subsconfig パラメータなしで指定すると、pmd.ini ファイルの parent_pmd トークンが更新されます。

注: 複数の親 Policy Model を定義する場合は、引用符を使用する必要があります。たとえば、Policy Model を作成し、その親を定義する場合、以下のコマンドを使用します。

```
sepmdadm --pmdname subs2 --admin abc123 --admin root --auditors abc123 --desktop
pcp36949 ¥
--parentpmd "aa@pcp36949,bb@pcp36949"
```

--passwd_fname *fileName*

NIS のパスワード ファイルの場所を定義します。

--passwdpmd *pmdbName*

sepass によるパスワードの更新情報の送信先となる PMDB を指定します。このオプションによって、seos.ini ファイルの [seos] セクションにある passwd_pmd トークンが更新されます。

注: このパラメータは、-subsconfig スイッチを指定した場合にのみ使用できます。

複数の階層から成る Policy Model を作成する場合は、このパラメータを最上位の階層にある PMDB に設定して、パスワード変更が PMDB システムのすべての階層に伝達されるようにします。

--pmdname *pmdbName*

作成する PMDB の名前を指定します。

--pwmanager *name*

PMDB の CA Access Control パスワード マネージャを指定します。

--seosdir *directory*

CA Access Control のインストール ディレクトリを指定します。このオプションは、CA Access Control がデフォルトのディレクトリにインストールされていない場合にのみ使用します。

--subsconfig

ローカル端末がサブスクライバになるように指定します。このパラメータの使用時に、seos.ini ファイルの関連トークンを更新するには、-parentpmd *pmdbName* パラメータおよび -passwdpmd *pmdbName* パラメータを指定する必要があります。

注: サブスクライバの設定時に、これらのパラメータを -subsconfig オプションの後に指定する必要があります。

--subscriber *name*

この PMDB のサブスクライバを指定します。サブスクライバには、PMDB または端末を指定できます。

--xadmin *name*

PMDB のエンタープライズ ユーザ管理者を定義します。

--xauditor *name*

PMDB のエンタープライズ ユーザ監査者を定義します。

--xpwmanager *name*

PMDB のエンタープライズ ユーザ パスワード マネージャを指定します。

例: コマンド ラインを使用した PMDB の作成

bigcentral という端末で、他の端末がサブスクライブする PMDB を管理するとします。bigcentral で PMDB を作成するには、この端末で sepmdadm を実行します。このユーティリティは、*ACInstallDir*/bin ディレクトリにあります。

bigcentral で pmdb1 という名前の PMDB を作成し、サブスクライバとして workstat1 および workstat2 を指定して、管理者としてエンタープライズ ユーザ adm1 および adm2 を指定するとします。以下のコマンドを bigcentral で実行します。

```
sepmdadm --pmdname pmdb1 --subscriber workstat1 --subscriber workstat2 ¥
    --xadmin adm1 --xadmin adm2
```

例: サブスクライバ端末からの PMDB の参照

端末を PMDB のサブスクライバとして設定するには、サブスクライバ名を PMDB の端末に指定するだけでは不十分です。サブスクライバ端末でも特定の手順を実行する必要があります。

コマンド ラインを使用してローカル端末を PMDB にサブスクライブするには、--subsconfig パラメータだけでなく、--parentpmd パラメータおよび --passwdpmd パラメータも指定する必要があります。

たとえば、ローカル端末を HOST2 にある pmdb2 という PMDB および HOST1 にある master1 というパスワード PMDB にサブスクライブするには、以下のコマンドを入力します。

```
sepmdadm --subsconfig --parentpmd pmdb2@HOST2 --passwdpmd master1@HOST1
```

sepropadm Utility - データベース プロパティの管理

sepropadm ユーティリティは、データベースでプロパティの追加、更新、および削除を行います。このユーティリティは、データベースが格納されているディレクトリから、CA Access Control が実行されていない間に起動する必要があります。sepropadm ユーティリティは、一度に 1 つのプロパティしか追加できません。

重要: sepropadm ユーティリティは、CA Access Control テクニカル サポート担当者のみが使用します。sepropadm では、必ず CA Access Control テクニカル サポート担当者に承認された説明ファイルを使用してください。

このコマンドの形式は以下のようになります。

```
sepropadm file
```

file

CA Access Control サポート担当者が提供する説明ファイルを指定します。説明ファイルには以下の形式を使用します。

- シャープ記号 (#) で始まる行が 1 行必要です。この行は、記述行より前に置く必要があります。
- セミコロン (;) で始まる行はコメントであり、処理されません。
- 新しい二重リンク OID を追加する記述行は、以下の形式に従う必要があります。

  ```
  CLASS=%s    PROPERTY=%s    TYPE=%d    SIZE=%d    FLAGES=%x
  ```

- 新しいプロパティを追加する記述行は、以下の形式に従う必要があります。

  ```
  CLASS=%s  PROPERTY=%s  TYPE=%d  SIZE=%d  FLAGS=%x  LINK2CLASS=%s
  ```

- プロパティを削除する記述行は、以下の形式に従う必要があります。

  ```
  CLASS=%s  PROPERTY=%s
  ```

- プロパティを変更する記述行は、以下の形式に従う必要があります。

  ```
  CLASS=%s  PROPERTY=%s  TYPE=%d  SIZE=%d  FLAGES=%x REPLACE=YES
  ```

例: sepropadm の説明ファイル

説明ファイルのサンプルを以下に示します。

```
; Sample Patch File for the CA Access Control database
; Copyright 2004 Computer Associates International, Inc.
; ------------------------------------------
; DO NOT USE THIS FILE UNLESS YOU KNOW HOW TO!
# seclassadm database add property patch utility
; Format is :
CLASS=PROGRAM PROPERTY=MD5 TYPE=31 SIZE=16 FLAGS=0
```

sepurgdb ユーティリティ - 未定義のレコードへのデータベース参照のパージ

UNIX で該当

sepurgdb ユーティリティは、データベース全体から未定義のレコードへの参照を検索し、その参照をデータベースから削除します。これにより、データベースのサイズが小さくなります。

重要: 安全確保のため、最初にデータベースをバックアップしてから、CA Access Control デーモンが実行されていない間に sepurgdb ユーティリティを起動します。

レコードの削除時に、ACL またはグループ メンバシップのリストなどにある削除対象レコードへの参照は、処理時間を短縮するために、通常はそのまま残されます。これによって問題が発生することはありません。CA Access Control では一度も使用されていない一意の ID が新しいレコードに割り当てられるためです。sepurgdb ユーティリティは、空きディスク領域を確保するためにのみ使用します。

sepurgdb を実行するには、root ユーザである必要があり、またデータベース ファイルが格納されたディレクトリから起動する必要があります。データベース管理システムでは、事前に割り当てられたディスク領域を使用します。通常、データベース ファイルのサイズは、パージ後もほとんど変わりません。事前割り当てがあるため、データベースのサイズが後で大きくなっても、ファイル サイズはほとんど変わりません。

このコマンドの形式は以下のようになります。

```
sepurgdb FilePath [Username]
```

FilePath

sepurgdb ユーティリティのログ ファイルのベース名を指定します。sepurgdb では、以下の 2 つのログ ファイルが作成されます。

FilePath.err

発生したエラーのログが保存されます。

FilePath.log

実行されたアクションのログが保存されます。

注: マイナス記号(-)を *FilePath* に指定すると、この 2 つのログを統合して標準出力に送信できます。

ユーザ名

(オプション) USER レコードのグループ関連付けの削除済み所有者(存在しなくなったユーザ)を置き換えるためのユーザ名を指定します。

注: 指定したユーザがデータベースに存在している必要があります。存在しない場合、このオプションは無視されます。

sereport ユーティリティ - レポートの環境設定

sereport ユーティリティは、データベースおよび Policy Model 情報の HTML レポートを提供します。このレポートは Web ブラウザからアクセスできます。sereport は、認証エンジンで使用される現在のデータベースに対して実行されます。

sereport ユーティリティのオプションを以下のように設定できます。

- UNIX では、-f オプションを使用して指定した設定ファイルが使用されます。

  デフォルトのファイルは *ACInstallDir*/etc/sereport.cfg です。

- Windows では、レジストリが使用されます。レジストリは設定が可能です。sereport のレジストリ設定は、以下のレジストリ キーで定義されています。

  HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Report

以下の表に、生成可能なレポート、その説明、および対応する設定ファイルまたはレジストリ キーを示します。

レポート番号	タイトルと説明	セクション／サブキー	トークン／エントリ
1	管理者権限 指定されたユーザの管理者権限を表示します。	admin_report	■ ホスト名 ■ Objects_Pattern ■ User_Mode
2	ログイン制限 ユーザのログイン制限事項を表示します。	disablelogins_report	■ ホスト名 ■ Objects_Pattern ■ Properties ■ User_Mode
3	休止状態のアカウント アクティブになっていないアカウントを日付（日数）単位で表示します。 アカウントにログイン情報がない場合、休止状態の日数の計算に作成日が使用されます。	dormant_report	■ ホスト名 ■ Objects_Pattern ■ Dormant_account ■ User_Mode

レポート番号	タイトルと説明	セクション／サブキー	トークン／エントリ
4	最新のログイン ユーザの最新ログイン日を表示します。	login_report	■ ホスト名 ■ Objects_Pattern ■ User_Mode
5	パスワードの変更 指定された日数内にパスワードの変更が必要なユーザのリストを表示します。	passwd_report	■ Days_to_change ■ ホスト名 ■ Objects_Pattern ■ User_Mode
6	警告モード 警告モードのオブジェクトを含むリソースを表示します。	warning_report	■ Class_Name ■ ホスト名 ■ Objects_Pattern
7	untrusted プログラム untrusted モードのプログラムを表示します。	untrust_report	■ ホスト名 ■ Objects_Pattern
8	ユーザのアクセス権限 指定されたリソースへのユーザのアクセス権限を表示します。	accessor_report	■ アクセサ ■ Class_Name ■ ホスト名 ■ Objects_Pattern
9	データベースのユーザ/グループの比較 一部（すべてではない）のデータベースに定義されているユーザおよびグループを表示します。	grp_usr_compare	■ ホスト名 ■ Objects_Pattern
10	保護されたリソースの比較 リソースが指定されたデータベースに定義されているかどうかを表示します。	res_compare	■ Class_Name ■ ホスト名 ■ Objects_Pattern
11	アクセス権限の比較 Policy Model とサブスクライバ データベース間のリソース制限事項の違いを表示します。	acc_compare	■ Class_Name ■ ホスト名 ■ Objects_Pattern

レポート番号	タイトルと説明	セクション／サブキー	トークン／エントリ
12	ユーザ情報の比較 Policy Model とサブスクライバ データベース間のユーザ定義の違いを表示します。	usr_compare	■ ホスト名 ■ Objects_Pattern ■ Properties
13	PMDB とサブスクライバの比較 PMDB にあり、サブスクライバ データベースにはない（Class_Name トークンおよび Object_pattern トークンで定義された）ルールを表示します。 **注**: PMDB のすべてのルールがサブスクライバ データベースに存在する場合、データベースは IDENTICAL とレポートされます。	pmdb_compare	■ Class_Name ■ ホスト名 ■ Objects_Pattern

アクセサ

アクセサの選択パターン（マスク）を指定します。すべてのアクセサを選択するには、アスタリスク（*）を使用します。

Class_Name

クラスのリストを指定します。

Days_to_change

パスワード変更を要求されるまでの残り日数を指定します。

Dormant_account

アカウントが休止状態とみなされる期間を指定します。

ホスト名

データを取得するホストのリストを指定します。

Objects_pattern

オブジェクトの選択パターン（マスク）を指定します。すべてのオブジェクトを選択するには、アスタリスク（*）を使用します。

Properties

オブジェクトに関連付けられた属性を指定します。

Report_place

(UNIX のみ)レポートの出力先の完全パスを指定します。

注: Windows では、コマンドの -f オプションを使用して出力先を定義します。

User_Mode

カンマで区切られたユーザ モードのリストを指定します。

色付きのセクション キーには、以下の追加の環境設定があります。

title

レポートのタイトルの色を指定します。

class_title

レポートの class_title の色を指定します。

background

(UNIX のみ)レポートのタイトルの背景色を指定します。background および logo は、完全パスで入力する必要があります。

logo

ロゴを作成します。background および logo は、完全パスで入力する必要があります。

sereport ユーティリティ - UNIX での HTML レポートの作成

UNIX で該当

sereport ユーティリティは、データベースおよび Policy Model 情報に関する、Web ブラウザからアクセス可能な HTML レポートを作成します。sereport は、認証エンジンで使用される現在のデータベースに対して実行されます。

sereport を使用するには、照会するすべてのデータベースに対して READ 権限が必要です。

注: デフォルトの環境設定ファイルは *ACInstallDir*/etc/sereport.cfg です。

このコマンドの形式は以下のようになります。

```
sereport [-f|-file pathname] -r|-report number [-host hostnames]
```

-f | -file *pathname*

(オプション) 環境設定ファイルの完全パスを指定します。ファイルを指定しない場合は、デフォルトのファイル *ACInstallDir*/etc/sereport.cfg が使用されます。

-host *hostnames*

(オプション) レポートを行う 1 つ以上のホストの名前を指定します。ホストを指定しない場合は、環境設定ファイルからホスト名が取得されます。

-r | report *number*

作成するレポート番号を指定します。

sereport ユーティリティ - Windows での HTML レポートの作成

Windows で該当

sereport ユーティリティは、データベースおよび Policy Model 情報に関する、Web ブラウザからアクセス可能な HTML レポートを作成します。sereport は、認証エンジンで使用される現在のデータベースに対して実行されます。

sereport を使用するには、照会するすべてのデータベースに対して READ 権限が必要です。

このコマンドの形式は以下のようになります。

```
sereport -f|-file pathname -r|-report number [-host hostnames]
```

-f | -file *pathname*

出力ファイル(レポート)の完全パス名を指定します。

注: 指定したファイルの内容は HTML 形式で構造化されます。このため、*.html* 拡張子を指定してファイルを自動的に関連付ける必要があります。

-host *hostnames*

(オプション)レポートを行う 1 つ以上のホストの名前を指定します。

ホストを指定しない場合は、*localhost* が使用されます。

-r | report *number*

作成するレポート番号を指定します。

seretrust ユーティリティ -- プログラムを再度 trust 状態にし、ファイルをセキュリティ保護するコマンドを生成します。

seretrust ユーティリティは selang コマンドを生成します。このコマンドは、データベース内で定義されているプログラムおよび保護対象ファイルを再度 trusted 状態にする場合に必要となります。seretrust ユーティリティは、trusted として定義されている SECFILE リソースおよび PROGRAM リソースが変更された場合にそのステータスをレポートします。seretrust では、プログラムが変更された場合に Watchdog で対処済みかどうかの確認も行います (つまり、CA Access Control データベースでは、これらのプログラムが trusted とマークされたままであることを意味します)。これらのプログラムは、seretrust の出力に追加されます。この際、プログラムの内容またはタイムスタンプが変更されたこと、およびプログラムを再度 trusted 状態にする必要があることも明記されます。

注: UNIX では、setuid プログラムおよび setgid プログラムは、それぞれの i-node 値などの詳細な説明と共にデータベースに格納されています。バックアップからシステムを復元すると、このプログラムは異なる i-node に格納されます。CA Access Control では、i-node 間の不一致が検出されると、すべての trusted プログラムに untrusted のマークが付けられます。seretrust ユーティリティは、データベースに定義されている trusted プログラムを検索し、それぞれの i-node 値を更新します。このため、CA Access Control の起動時に、trusted プログラムが trusted の状態のまま維持されます。

スイッチを指定しない場合は、untrusted プログラムおよび保護された untrusted ファイルのみが処理されます。

このコマンドの形式は以下のようになります。

```
seretrust [-a] [-l|-m|-p|-s] path
```

-a

すべての trusted オブジェクトおよび untrusted オブジェクトを処理します

-h

このユーティリティのヘルプ画面を表示します。

--l

現在のディレクトリのデータベースからプログラムおよびファイルに関する情報を抽出します。

このオプションを省略すると、CA Access Control が使用するデータベースが処理されます。

-m

すべてのカーネル モジュールのシグネチャを計算します。カーネル モジュール レコードのシグネチャ プロパティが無効な場合は、正しいシグネチャに更新されるため、カーネル モジュールは trusted 状態になります。シグネチャは、Linux カーネル モジュールにのみ使用されます。

-p

PROGRAM クラスのレコードのみを処理します。

-s

SECFILE クラスのレコードのみを処理します。

path

再度 trusted 状態にする必要があるプログラムおよび保護対象ファイルを検索するための基本パスを指定します。

このユーティリティは、指定したディレクトリおよびすべてのサブディレクトリを処理します。

例: untrusted プログラムおよび保護対象ファイルを再度 trusted に戻す

この例は、seretrust ユーティリティを使用して、プログラムおよび保護対象ファイルを再度 trusted 状態にする方法を示しています。

注: この例は、UNIX でのサンプルのコマンド出力を示していますが、このユーティリティは Windows でも同様に機能します。

プログラムおよび保護対象ファイルを再度 trusted 状態にするには、以下の手順に従います。

1. CA Access Control データベース管理者として、以下の seretrust コマンドを入力します。

   ```
   seretrust > retrust_script
   ```

   オプションが指定されていないため、trusted プログラムと保護対象ファイルの両方が処理されます。また、基本パスも未指定であるため、ルート パスが使用されます。

   以下の情報が画面に表示されます。

   ```
   Retrusting PROGRAMs & SPECFILEs, Base path = /
   Total of 0 entries retrusted. (Class=SECFILE)
   Total of 16 entities retrusted. (class=PROGRAM)
   ```

   以下の例は、スクリプト ファイル seretrust が作成する内容を示しています。

   ```
   chres PROGRAM ("/usr/bin/chgrpmem") trust
   chres PROGRAM ("/usr/bin/chie") trust
   chres PROGRAM ("/usr/bin/crontab") trust
   chres PROGRAM ("/usr/bin/cu") trust
   chres PROGRAM ("/usr/bin/ecs") trust
   chres PROGRAM ("/usr/bin/newgrp") trust
   chres PROGRAM ("/usr/bin/rmquedev") trust
   chres PROGRAM ("/usr/bin/rsh") trust
   chres PROGRAM ("/usr/bin/sysck") trust
   chres PROGRAM ("/usr/bin/uuname") trust
   chres PROGRAM ("/usr/lib/methods/showled") trust
   chres PROGRAM ("/usr/lib/mh/post") trust
   chres PROGRAM ("/usr/lib/mh/slocal") trust
   chres PROGRAM ("/usr/lpp/X11/bin/xlock") trust
   chres PROGRAM ("/usr/lpp/X11/bin/xterm") trust
   chres PROGRAM ("/usr/sbin/chvirprt") trust
   ```

2. プログラムおよびファイルを trusted 状態にするために作成された selang スクリプト ファイル seretrust を実行します。

   ```
   selang -f retrust_script
   ```

serevu ユーティリティ - 失敗したログイン試行の処理

UNIX で有効

serevu ユーティリティは、指定した期間内に指定した失敗ログイン試行回数に達したユーザを処理します。 指定内容に基づいて、ユーザを無効化、レポート、または無視できます。デフォルトでは、ローカル端末の UNIX 環境ではユーザは無効化されます。該当するユーザがローカルに存在しない場合、serevu は NIS 情報をチェックして、該当するユーザを検索します。

passwd_pmd 構成設定に値を設定すると、適切な PMDB が更新され、その更新情報が各サブスクライバに伝達されます。passwd_pmd トークンに値を設定しない場合は、parent_pmd 構成設定の値が使用され、その更新情報が各サブスクライバに伝達されます。

注: serevu で PMD（serevu.cfg で設定可能）にコマンドを送信する必要がある場合に、PMD でルートに対して ADMIN 属性または端末へのアクセスが設定されていなければ、以下の内容を PMD とそのサブスクライバすべてに定義してください。

```
eu _serevu logical
authorize admin USER uid(_serevu) access(a)
# 以下の行が実行できるのは、マスタ PMD 上でのみです。
authorize terminal localTerminalName uid(_serevu) access(a)
```

注: serevu ユーティリティを正常に機能させるためには、root ユーザが /etc/passwd ファイルに対して write アクセス権限を持っている必要があります。serevu 環境設定ファイル（serevu.cfg）でリモート コンピュータを定義する場合は、ログイン権限をリモートコンピュータに付与する必要があります。以下に例を示します。

```
eu _serevu admin logical
authorize terminal localTerminalName uid(_serevu) access(a)
er specialpgm $ACDIR/bin/serevu seosuid(_serevu ) unixuid(root)
```

このコマンドの形式は以下のようになります。

```
serevu {daemon|nodeamon} [-f nn] ¥
    [-d {nn[s|m|h|d|w]|FOREVER}] ¥
    [{-s|-t} nn[s|m|h|d|w]]
```

daemon

ユーティリティをデーモンとして実行します。デフォルト値です。

nodaemon

ユーティリティを標準プロセスとして実行します。

-d

ユーザのログインを無効にする期間を指定します。デフォルトでは、この値は秒単位です。

注: ユーザ アカウントを無効にする期間は、各 serevu スキャンを実行する間隔の時間より短く設定することはできません。ユーザ アカウントを無効にする期間は、各 serevu スキャンを実行する間隔の時間の倍数に設定する必要があります。

-f

失敗ログイン回数を指定します。この失敗ログイン回数に達したユーザのアカウントは、指定された期間内は無効になります。

注: 失敗ログイン回数(*def_fail_count* 構成設定の値でも定義可能)は、システムに設定されている許容失敗ログイン回数の値と常に等しくすることをお勧めします (たとえば Solaris では、システムのこの値は RETRIES トークンによって /etc/default/login に設定されています)。詳細については、オペレーティング システムのマニュアルを参照してください。

-h

このユーティリティのヘルプ画面を表示します。

-s

現時点からさかのぼる期間を指定します。この期間内に serevu は失敗したログインをスキャンします。

デフォルト: 300 秒(環境設定)。

--t

serevu の次のチェックまでの経過時間を指定します。

デフォルト: 120 秒(環境設定)。

FOREVER

-d オプションを共に使用して、時間を無期限に指定します。このパラメータを使用する場合、ユーザ ログインは無期限に無効になります。

nn[s|m|h|d|w]

-d、-s、-t の各オプションと共に使用して、オプションの時間を指定します。

s

nn は秒単位（デフォルト）。

m

nn は分単位。

h

nn は時間単位。

d

nn は日単位。

w

nn は週単位。

sessfgate ユーティリティ - CA Access Control への Unicenter Security Requests の転送

sessfgate ユーティリティは、Unicenter Security API をメッセージ キューから CA Access Control に転送して再フォーマットします。UNIX の Unicenter Security API は、すべてメッセージ キューに格納されます。sessfgate ユーティリティは、メッセージ キューから送信された API 要求を処理し、再フォーマットおよび再転送されたこれらの要求を CA Access Control に転送します。その後、ユーティリティは CA Access Control のリターン コードを Unicenter TNG の対応するリターン コードに変換します。

ゲートウェイをアクティブにするには、Unicenter 統合のセットアップ手順を実行する必要があります。Unicenter 統合のセットアップでは、sessfgate プログラムが *ACInstallDir*/tng/bin ディレクトリにインストールされます（*ACInstallDir* は CA Access Control のインストール ディレクトリであり、デフォルトでは /opt/CA/AccessControl/ です）。Unicenter Security が停止され、CA Access Control が起動された後に、sessfgate は SSF の代わりに API 要求を受け取ることができます。

このコマンドの形式は以下のようになります。

```
sessfgate [-i|-s|-l] -t
```

-I

ゲートウェイの起動を指定します。

-S

ゲートウェイの停止を指定します。

--I

ステータスを指定します。

--t

トレース ファイルの有効または無効を切り替えます（ログ ファイルは /opt/CA/AccessControl//log/sessftrace.log です）。

注: Unicenter TNG を実行する前に seload を実行する場合は、以下のコマンドを使用して、sessfagte を手動で起動する必要があります。

```
ACInstallDir/tng/bin/sessfagte -I
```

この場合、*ACInstallDir* は CA Access Control がインストールされているディレクトリです。

sesu ユーティリティ - ユーザの代替

sesu ユーティリティを使用すると、一時的に他のユーザとして操作を行うことができます。このユーティリティは、UNIX の su コマンドの CA Access Control バージョンです。ただし、sesu ユーティリティではユーザ代替コマンドが用意されていて、このコマンドでは、代替ユーザのパスワードを入力する必要はありません。認証プロセスは、SURROGATE クラスに定義されている CA Access Control のアクセス ルールに基づいて実行されます。また、コマンドを実行するユーザのパスワードに基づいて実行される場合もあります。

sesu ユーティリティでは、seos.ini ファイルの sesu セクションにあるトークンを使用します。また、以下の特殊ファイルも使用します。

- /etc/passwd
- /etc/group
- /etc/shells

このプログラムは、誤って使用されることを防ぐために、ファイル システム内でマークされており、誰もこれを実行できません。 このため、セキュリティ管理者は、このプログラムを実行する前に、それが実行可能ファイルであることをマークし、ユーザ ID を root に設定する必要があります。

重要: sesu ユーティリティを使用する前に、すべてのユーザを CA Access Control データベースに定義し、前提条件を設定してください。これは、CA Access Control に定義されていないユーザに対してシステム全体が開放されることを防止するためです。

使用上の注意

- CA Access Control の承認サーバが見つからない場合、ユーティリティはシステムの標準 su コマンドを実行します。
- sesu.old_sesu 構成トークンが no に設定されている場合、ユーティリティはシステムの標準 su コマンドを実行します。
- /etc/shells が存在していて、それが現在のシェルを指定していない場合、sesu はアカウントの代理使用を root に許可しません。

このユーティリティの構文は、以下のようになります。

```
sesu [-] [username] [-l] [-n] [-s shell] [-c command]
```

-

環境をターゲット ユーザの環境に設定します。

注: Linux では、*-l* オプションの使用と同じです。

-c *command*

指定されたコマンドを実行して、終了します。

空白を含むコマンドは、引用符で囲みます。

-h

このユーティリティのヘルプ画面を表示します。

-l

(Linux のみ)。開いているシェルがログイン シェルであることを示します。

-n

ユーザに対してパスワードを要求しないように指定します。

重要: このオプションを使用した場合、ユーティリティは root アカウントとして実行され、LOGIN イベントを実行します。

注: セキュリティ許可サーバが見つからない場合、ユーティリティは /bin/su を使用します。

-s *shell*

(Linux のみ)。ユーザのパスワード入力によるシェルではなく、開くシェルを指定します。

このシェルは、/etc/shells ファイルのリストにある必要があります。

username

セッションに関連付けられている ID を、指定されたターゲット ユーザの *username* の ID に変更します。

username を指定しない場合、sesu によってデフォルトで root が設定されます。

例

- UID を root に変更するには、以下のコマンドを入力します。環境は、このコマンドを実行したユーザの環境のままです。

  ```
  sesu
  ```

- *UID* を root に変更するには、以下のコマンドを入力します。環境は、root ユーザの環境に変更されます。

  ```
  sesu-
  ```

- ユーザ John の代理ユーザになるには、以下のコマンドを入力します。

  ```
  sesu John
  ```

- ユーザ Carol の代理になり、指定されたコマンド ls -la を /home/carol ディレクトリから実行するには、以下のコマンドを入力します。

  ```
  sesu - Carol -c "ls -la /home/carol"
  ```

- 以下のコマンドを使用して、ユーザ Angelo の代理ユーザになり、bash シェルを使用し、それをログイン シェルとして開きます。

  ```
  sesu Angelo -l -s /bin/bash
  ```

  注: これは、Linux でのみ有効です。

sesudo ユーティリティ

sesudo ユーティリティを使用すると、別のユーザの権限でコマンドを実行できます。これにより、一般ユーザは、管理者権限が必要なアクションを実行できます。

このような方法でコマンドを実行するユーザ権限を管理するルールは、SUDO クラスにアクセス ルールとして定義されます。SUDO クラスのレコードにはコマンド スクリプトが保存されているので、sesudo によってそのスクリプトの実行を許可されているユーザおよび禁止されているユーザの両方を指定できます。

sesudo ユーティリティ - UNIX で別のユーザとしてコマンドを実行

UNIX で該当

sesudo ユーティリティを使用すると、別のユーザの権限でコマンドを実行できます。sesudo は、他のユーザ（ターゲット ユーザ）の権限を借りて 1 つ以上のコマンドを実行するユーティリティです。このユーティリティを使用すると、一般ユーザもスーパーユーザ権限が必要なアクション（mount コマンドなど）を実行できます。

このような方法でコマンドを実行するユーザ権限を管理するルールは、SUDO クラスにアクセス ルールとして定義されます。SUDO クラスのレコードにはコマンド スクリプトが保存されているので、sesudo によってそのスクリプトの実行を許可されているユーザおよび禁止されているユーザの両方を指定できます。

sesudo を実行するたびに、以下の値のいずれか 1 つが返されます。

-2

ターゲット ユーザが見つからないか、またはコマンドが中断されました。

-1

パスワード エラー

0

実行が成功しました。

10

パラメータの使用法に問題があります。

11

syscall がロードされていません。

20

ターゲット ユーザ エラー

22

syscall はロードされていますが、デーモンが実行されていません。

30

権限エラー

このコマンドの形式は以下のようになります。

```
sesudo {-h|-list|record [params]}
```

-h

ヘルプ画面を表示します。

-list

実行可能な sesudo コマンドをリストします。これらのコマンドは、実行権限を与えられている CA Access Control データベースに定義されている SUDO レコードです。

レコード

sesudo ユーティリティを使用して実行するコマンドにセキュリティ管理者が付与した SUDO クラス レコードの名前を指定します。

params

（オプション）実行するコマンドに渡すパラメータを指定します。

sesudo ユーティリティ - Windows で別のユーザとしてコマンドを実行

Windows で有効

sesudo ユーティリティを使用すると、別のユーザの権限でコマンドを実行できます。sesudo は、他のユーザ（ターゲット ユーザ）の権限を借りて 1 つ以上のコマンドを実行するユーティリティです。このユーティリティを使用すると、一般ユーザもスーパーユーザ権限が必要なアクション（mount コマンドなど）を実行できます。

このような方法でコマンドを実行するユーザ権限を管理するルールは、SUDO クラスにアクセス ルールとして定義されます。SUDO クラスのレコードにはコマンド スクリプトが保存されているので、sesudo によってそのスクリプトの実行を許可されているユーザおよび禁止されているユーザの両方を指定できます。

注: sesudo によって起動されたプログラムを実行するユーザは、Windows 用の CA Access Control から変更できません。

このコマンドの形式は以下のようになります。

```
sesudo {-h|-list|-do record [params]}
```

-h

オンライン ヘルプ画面を表示します。

-list

実行可能な sesudo コマンドをリストします。これらのコマンドは、実行権限を与えられている CA Access Control データベースに定義されている SUDO レコードです。

-do *record* [*params*]

sesudo で別のユーザとしてコマンドを実行するように指定します。

record

sesudo ユーティリティを使用して実行するコマンドにセキュリティ管理者が付与した SUDO クラス レコードの名前を指定します。

params

（オプション）実行するコマンドに渡すパラメータを指定します。

seuidpgm ユーティリティ - trusted プログラムの抽出

UNIX で該当

seuidpgm ユーティリティは、Set-User-ID ビットまたは Set-Group-ID ビットがオンであるすべてのプログラムを抽出します。seuidpgm は、ファイル システム全体をスキャンし、検出されたプログラムを PROGRAM クラスに追加する selang コマンドを作成します。

seuidpgm は、selang のコマンドでコマンドを作成し、そのコマンドを標準出力に書き込みます。selang ユーティリティへのパイプラインを使用することも、出力をファイルに送ることもできます。出力を編集して不要なプログラムを削除したり、プログラムをさらに追加することができるため、出力はファイルに送ることをお勧めします。この方法を使用して、システム内の不要な setuid プログラムを検索します。

注: UxImport ユーティリティを使用して、seuidpgm ユーティリティの実行前にユーザおよびグループを定義することをお勧めします。ただし、UxImport を事前に実行していない場合でも、-g オプションと -u オプションを指定して seuidpgm を実行するとユーザおよびグループを定義できます。

seuidpgm は、コマンド ラインで指定したすべてのパスを、開始パスのすべてのサブディレクトリまで検索します。複数の開始パスを使用できます。

任意の数のオプションを指定できます。複数のオプションを指定する場合は、各オプションをスペースで区切ります。

プログラムが setuid プログラムであり、write アクセス権限が割り当てられている場合、seuidpgm は、他のすべての setuid プログラムと同様にそのプログラムを処理します。ただし、標準エラーの警告も送信します。

注: PROGRAM クラスのレコードの制御方法の詳細については、「*UNIX エンドポイント管理ガイド*」を参照してください。

このコマンドの形式は以下のようになります。

```
seuidpgm option startDir ... [-x excludeDir]
```

-d

UNIX のファイル アクセス許可を解析して許可されているファイル アクセスを決定する代わりに、defaccess を「execute」に設定し、PROGRAM クラスに setuid プログラムおよび setgid プログラムのエントリを自動的に作成します。setuid プログラムまたは setgid プログラムが相互にそれぞれのプログラムを実行する場合もあります。このオプションを指定しないと、setuid プログラムまたは setgid プログラムの実行を試みるプログラムは、これらのプログラムを実行できません。

このオプションを使用することをお勧めします。

-f

FILE クラスおよび PROGRAM クラスの両方のルールを作成します。

--g

setgid プログラムの GROUP レコードを作成します。

注: このオプションは、UxImport を実行していない場合にのみ使用してください。

--l

ハード リンクまたはシンボリック リンクを持つプログラムに 1 つの許可を作成します。

ファイル システムを root ディレクトリからではなく特定のディレクトリのみからスキャンし、-l オプションを指定する場合は、コマンド ラインで複数の開始パスを使用します。複数の開始パスを使用しないと、-l オプションが無効になることがあります。

-n

NFS をスキャンしません。

このオプションを使用することをお勧めします。

-o

ファイル名を標準出力に書き込みますが、selang のコマンドは作成しません。

-p

setuid プログラムを NFS ディレクトリから有効にします。ただし、マウント テーブルが、マウントされたファイル システムから setuid を実行することを許可している場合にのみ実行できます。

-q

Quiet-Mode でユーティリティを実行します。つまり、標準エラーに対するエラー メッセージは送信されません。

-s

PROGRAM クラスに setuid/setgid プログラムのエントリを作成するのではなく、SECFILE クラスにエントリを作成します。

-u

setuid プログラムの USER レコードを作成します。

注: このオプションは、UxImport を実行していない場合にのみ使用してください。

-x *excludeDir*

ツリーからディレクトリを除外します。指定されたディレクトリでは、setuid プログラムおよび setgid プログラムは検索されません。このオプションはコマンドラインの最後に指定する必要があります。*path* は、除外するディレクトリの完全パスです。複数のディレクトリを除外するには、各ディレクトリに対して -x オプションを繰り返し指定します。

startDir

trusted プログラムを検索する上位ディレクトリのスペース区切りリストを指定します。

例

- 重複する名前または同一の i-node を Quiet モードでチェックし、NFS をスキャンしないという設定で、set-user-id または set-group-id が「on」、defaccess が「execute」に指定されたすべてのプログラムを追加する selang のコマンドを出力するには、以下のコマンドを入力します。プログラムは、/usr ディレクトリとそのサブディレクトリ、/var ディレクトリとそのサブディレクトリ、および /etc ディレクトリとそのサブディレクトリをスキャンします。出力は、ホーム ディレクトリにある seprogs.seos ファイルに送られます。

  ```
  seuidpgm -dlqn /usr /var /etc > ~/seprogs.seos
  ```

  出力内容は以下のようになります。

  ```
  ## ************************************************
  ## seuidpgm List Sun Feb 9 14:24:16 1997
  # Start Path= /usr
  # ************************************************
  nr PROGRAM /usr/lpp/bos/inst_root/lpp/inu_LOCK defaccess(EXEC)
  nr PROGRAM /usr/lpp/X11/bin/xlock defaccess(EXEC)
  nr PROGRAM /usr/bin/setsenv defaccess(EXEC)
  nr PROGRAM /usr/bin/shell defaccess(EXEC)
  nr PROGRAM /usr/bin/su defaccess(EXEC)
  nr PROGRAM /usr/bin/sysck defaccess(EXEC)
  nr PROGRAM /usr/bin/tcbck defaccess(EXEC)
  nr PROGRAM /usr/bin/usrck defaccess(EXEC)
  nr PROGRAM /usr/bin/vmstat defaccess(EXEC)
  ```

- /home ディレクトリを除き、root ディレクトリとそのすべてのサブディレクトリをスキャンするには、以下のコマンドを入力します。

  ```
  seuidpgm -qln / -x /home
  ```

詳細情報:

UxImport ユーティリティ - UNIX オペレーティング システムからの情報の抽出 (P. 290)
selang ユーティリティ - CA Access Control コマンドラインの実行 (P. 200)
seoswd デーモン (P. 322)
seosd デーモン (P. 316)

seversion ユーティリティ - CA Access Control プログラム モジュールのバージョン情報の表示

UNIX で該当

seversion は、CA Access Control モジュールのバージョン情報を表示するユーティリティです。以下のデータを表示できます。

- グローバル バージョン番号およびマイナー バージョン番号
- モジュールがコンパイルされた日時
- モジュールがコンパイルされた端末

このコマンドの形式は以下のようになります。

```
seversion [-a|-l|-g|-h|-m|-s|-5] module
```

--a

要求された情報を表形式で表示します。

--g

タイトルを省略し、グローバル バージョン番号のみを表示します。

-h

このユーティリティのヘルプ画面を表示します。

--l

組み込まれているライブラリ情報を表示します。

-m

タイトルを省略し、マイナー バージョン番号のみを表示します。

-s

タイトルを省略し、SHA1 シグネチャを表示します。

-5

タイトルを省略し、MD5 シグネチャを表示します。

このオプションは、FIPS-only モードでない場合にのみ機能します。

module

表示するバージョン番号のモジュールのファイル名を指定します。

例

sesudo ユーティリティのバージョン情報を表示するには、以下のコマンドを入力します。

```
seversion /opt/CA/AccessControl//bin/seosd
```

FIPS モードでない場合に、以下のようなメッセージが画面に表示されます。

```
CA Access Control seversion vX.X.X.xxx - Display module's version
Copyright (c) YYYY CA. All rights reserved.
Running under:  Linux
File name: /opt/CA/AccessControl//bin/seosd
Version  : major.minor.sp.build
Created  : MMM DD YYYY hh:mm:ss
OS info  : i86PC
SHA1     : 10068CC6A70195B84AF896682CCBA1A4B7B43CD1
MD5:     : 1F9BD56CA523A33FFBC47551ECE093E5
```

sewhoami ユーティリティ - UNIX での CA Access Control ユーザ名およびセキュリティ クレデンシャルの表示

UNIX で該当

sewhoami ユーティリティは、CA Access Control 認証デーモンが認識できるユーザ名を表示するユーティリティです。sewhoami は UNIX の whoami ユーティリティに類似していますが、表示される情報は異なり、通常 sewhoami の情報の方が有用です。

- su コマンドを実行し、次に UNIX の whoami ユーティリティを実行すると、su コマンド実行後に取得されたユーザ ID に基づいてユーザ名が表示されます。
- su コマンドを実行し、次に CA Access Control の sewhoami ユーティリティを実行すると、そのユーザの元のログイン ID とその権限情報が表示されます。

このコマンドの形式は以下のようになります。

```
sewhoami [-a|-d]
```

--a

ユーザのクレデンシャル、つまりユーザの ACEE の内容を表示します。

注: ACEE の詳細については、「*UNIX エンドポイント管理ガイド*」を参照してください。

-d

ユーザに関連付けられた ACEE ハンドルおよびデータベースにあるそのハンドル名を表示します。

例: UNIX での CA Access Control ユーザ名およびセキュリティ クレデンシャルの表示

以下の例は、CA Access Control 認証デーモンで認識されているユーザ名およびセキュリティ クレデンシャルを表示します。

```
sewhoami -a
```

root ユーザの場合、sewhoami 出力は以下のようになります。

```
root
ACEE Contents
 User's Name             : root
 ACEE's Handle           : 52
  Group Connections Table:
   Group Name              Connection Mode
          ==================    ==============================
   adm                   Regular
   bin                     Regular
   daemon                  Regular
   disk                    Regular
   root                    Regular
   seosaudt                Regular
   sys                     Regular
    wheel                   Regular
Categories              : <None>
Profile Group           : <None>
Security Label          : <None>
User's Audit Mode       : Failure LoginSuccess LoginFailure
User's Security Level   : 0
Source Terminal         : <Unknown>
Process Count for ACEE  : 19
User's Mode             : Admin Auditor
ACEE's Creation Time    : Tue Mar 17 14:53:07 2009
```

test という名前のユーザで root ユーザではない場合、sewhoami 出力は以下の例のようになります。

```
test
ACEE Contents
 User's Name             : test
 ACEE's Handle           : 65
  Group Connections Table:
   Group Name              Connection Mode
           ==================    ==============================
   seosaudt                Regular
   users                   Regular
Categories              : <None>
Profile Group         : secadmin
Security Label          : <None>
User's Audit Mode       : Failure LoginSuccess LoginFailure
User's Security Level   : 0
Source Terminal         : localhost.localdomain
Process Count for ACEE  : 2
User's Mode             : Admin Auditor
ACEE's Creation Time    : Wed Mar 18 15:34:53 2009
```

詳細情報:

secons -whoami 機能 - ユーザ名およびセキュリティクレデンシャルの表示 (P. 185)

uninstall_AC ユーティリティ - 現在のコンピュータからの CA Access Control の削除

UNIX で該当

uninstall_AC ユーティリティは、コマンドを実行するステーションから CA Access Control の一部またはすべてを削除します。デフォルトは「-all」で、端末から製品全体を削除します。

注: CA Access Control のカーネル拡張は、アンインストール前にアンロードする必要があります。

このコマンドの構文は、以下のようになります。

```
uninstall_AC [-all | -admin] [-f] [-force] [-h] [-ignore_dep] [-d path] [-fn file]
```

-admin

端末から Security Administrator および seauditx などの管理ツールのみを削除します。

注: 現在では *admin* パッケージは CA Access Control に含まれていません。古いバージョンの CA Access Control を削除する場合には、このオプションを使用します。

-all

端末から製品全体を削除します。

-d *path*

CA Access Control のインストール先ディレクトリを定義します。

注: CA Access Control をデフォルトのディレクトリ（/opt/CA/AccessControl/）にインストールする場合、このオプションを指定する必要はありません。

-f

サイレント モードで CA Access Control を削除します。

-fn *file*

アンインストールが完了した後に指定したファイルを実行します。

-force

カーネル拡張のアンロード プロセスが失敗した場合でも、アンインストールを強制的に続行します。

-h

このユーティリティのヘルプ画面を表示します。

-ignore_dep

アンインストール手順で、他の製品との依存関係をチェックしないように指定します。

例: コンピュータから CA Access Control を完全に削除する

CA Access Control がデフォルトのディレクトリにインストールされている場合に、使用中のコンピュータから完全に削除するには、以下のコマンドを入力します。

```
uninstall_AC
```

uxauthd.sh スクリプト -- UNIX 認証ブローカエージェントを管理します。

uxauthd.sh スクリプトを使用して、UNIX 認証ブローカ エージェントを管理します。環境が正しく設定されることが保証されるため、uxauthd.sh スクリプトを使用して UNIX 認証ブローカ エージェントを管理することを推奨します。

デフォルトでは、uxauthd.sh スクリプトは /opt/CA/uxauthd/lbin ディレクトリ内にあります。

このコマンドの形式は以下のようになります。

```
uxauthd.sh {start | stop | restart | status | debug level}
```

start

UNIX 認証ブローカ エージェントを起動します。

stop

UNIX 認証ブローカ エージェントを停止します。

再起動

UNIX 認証ブローカ エージェントを再起動します。

status

UNIX 認証ブローカ エージェントのステータスを表示します。ステータスの状態は以下のとおりです。

- uxauthd は動作している
- uxauthd は動作していない

デバッグ レベル

UNIX 認証ブローカ エージェントをデバッグ レベルで起動するように指定します。

範囲: 1 ～ 3

注: uxauthd.sh を使用して UNIX 認証ブローカ エージェントを起動または停止すると、レポート エージェントのステータスに影響します。

uxconsole ユーティリティ -- UNIX 認証ブローカ エンドポイントの管理

uxconsole ユーティリティを使用して、UNIX 認証ブローカ エンドポイントを管理することができます。uxconsole ユーティリティを使用すると、UNIX 認証ブローカのインストールに関する情報を表示し、UNIX 認証ブローカ エンドポイントを Active Directory に登録し、ユーザとグループを管理および移行することができます。

このユーティリティはいくつかのタスクを処理します。以下の関数を使用します。

タスク	関数
UNIX コンピュータを Active Directory に登録する	uxconsole -register (P. 277)

タスク	関数
UNIX コンピュータの Active Directory での登録を解除する	uxconsole -deregister (P. 277)
詳細レベルを設定する	uxconsole -debug (P. 287)
Active Directory ユーザのログインを有効にする	uxconsole -activate
Active Directory ユーザのログインを無効にする	uxconsole -deactivate
ユーザおよびグループを Active Directory へ移行する	uxconsole -migrate (P. 274)
ユーザとグループを管理する	uxconsole -manage (P. 272)
エンドポイント ステータスを表示する	uxconsole -status (P. 280)
Kerberos 操作を実行する	uxconsole -krb (P. 283)
Active Directory で LDAP クエリを実行する	uxconsole -ldap (P. 284)
UNAB NSS キャッシュ データを表示する	uxconsole -dbdump (P. 286)
Active Directory ユーザ アカウントを確認する	uxconsole -verify (P. 288)

uxconsole -manage - ユーザおよびグループを管理する

UNIX で有効

このコマンドは、ローカルまたはエンタープライズ ユーザおよびグループに関する情報を一覧表示、表示、または編集するために使用します。

このコマンドの形式は以下のようになります。

```
uxconsole –manage {-find | -show [-detail]} {-user <filter> | -group <filter>}
```

-find

ローカルおよびエンタープライズ ユーザまたはグループのリストの表示を指定します。

-show

特定のユーザやグループの詳細、またはユーザとグループのサブセットを表示するよう指定します。

-detail

ユーザ設定の詳細を表示するよう指定します。

-user *filter*

ユーザのサブセットを返すワイルドカードを定義します。

-group *filter*

グループのサブセットを返すワイルドカードを定義します。

例: ユーザ ステータスの表示

以下の例は、ローカル UNIX ユーザ(local1)で、Active Directory ユーザに別の名前(ent1)でマップされているユーザに関する出力を表しています。Active Directory ユーザは、有効な UNIX 属性を持っているため、UNIX 認証ブローカ エンドポイントにログインできます。

```
uxconsole> ./uxconsole -manage -show -detail -user ent1
CA Access Control UNAB uxconsole v12.52.0.160 - console utility
Copyright (c) 2009 CA. All rights reserved.

USER 'ent1' information
-----------------------------------------------------
Type                : Local User
Login Name          : local1
Mapped to           : ent1@example.com
Enterprise Account  : Enabled
Local Account       : Enabled
Login               : Allowed
Login Reason        : User exists locally
Uid                 : 300
Gid                 : 101
Shell               : /bin/bash
Home Directory      : /home/local1

Type                : Enterprise User
Login Name          : ent1
Principal Name      : ent1@example.com
Enterprise Account  : Enabled
Login               : Allowed
Login Reason        : According to internal default
Uid                 : 10133
Gid                 : 13870
Shell               : /bin/sh
Home Directory      : /home/ent1
```

uxconsole -migrate - UNIX のユーザとグループの Active Directory への移行

UNIX で有効

migrate を使用して、ユーザおよびグループを UNIX ホストから Active Directory に移行します。移行処理では、ローカル ユーザおよびグループを Active Directory に移行し、ローカル アカウントを無効にする処理を試みます。

このコマンドの形式は以下のようになります。

```
uxconsole -migrate [-scope {l|n|a}] {-mode {p|f}|-input file} [-emulate] [-d domain]
[-a name [-w pass]] [-users] [-groups] [-cgc container] [-new] [-v level] [-h]

uxconsole -migrate [-show {-user filter|-group filter}]
```

-migrate

UNIX ユーザの移行オプションを定義します。

-scope {l | n | a}

移行の範囲を指定します。

- l - ローカル ユーザおよびグループのみを移行します。
- n - NIS¥NIS+ サーバから NIS ユーザおよびグループを移行します。
- a - ローカルおよび NIS/NIS+ のユーザおよびグループを移行します。

デフォルト: l

-mode {p | f}

移行モードを指定します。

オプション: partial、full

デフォルト: f

-input *file*

アカウント マップ ファイルの完全パスを定義します。

注: マッピング ファイルを使用して、移行処理中に検出されたユーザ アカウントの競合を解決します。以下のフィールドおよびパラメータを持つ CSV 形式内のマップ ファイルを作成します。

```
type <USER|GROUP>, UNIX name <username>, requested action <KEEPLOCAL|MIGRATE|MAP>,
AD name <AD mapped name>
```

例: USER、uxuser、MAP、aduser。

-emulate

マイグレーション処理がエミュレーション モードで実行されることを指定します。

注: エミュレーション モードで uxconsole -migrate コマンドを実行しても、ユーザは Active Directory に移行されません。エミュレーション モードでは、uxconsole は、ユーザおよびグループの ID で競合する可能性があるものをレポートするジャーナル ファイルを作成します。エミュレーション モードは、UNIX/Active Directory のユーザおよびグループの ID 競合を解決するためにを使用してください。

-d *domain*

ユーザおよびグループの移行先のドメインの名前を定義します。

注: 管理者クレデンシャルを指定しないで -migrate -d コマンドを実行すると、UNIX 認証ブローカ でユーザおよびグループを Active Directory に移行することはできません。

-a *name*

Active Directory でユーザ プロパティを登録、作成、更新するために使用される Active Directory 管理者を指定します。

注: 管理者のクレデンシャルを指定せずに -migrate コマンドを実行すると、UNIX 認証ブローカ が有効にならないため、UNIX 属性を追加したり、アカウントやグループ Active Directory に追加することができません。Active Directory の管理者クレデンシャル指定しない場合、移行中に検出された競合を解決することができません。

-w *passwd*

Active Directory 管理者のアカウント パスワードを指定します。

-users

(オプション)ユーザのみを Active Directory に移行します。

注: 指定しない場合、一部のユーザは Active Directory に移行されません。

-groups

(オプション)グループのみを Active Directory に移行します。

注: 指定しない場合、一部のグループは Active Directory に移行されません。

-cgc *container*

新規グループを作成する Active Directory コンテナの名前を指定します。

-new

前回移行されていない新規ユーザおよびグループのみを移行するように指定します。

-v *level*

詳細レベルを指定します。

範囲: 1 ～ 5

-h

ヘルプを表示します。

-show

ユーザおよびグループ移行情報を表示します。

注: 指定した場合、ユーザおよびグループは移行されません。

-user *filter*

フィルタ条件に一致するユーザのみを表示します。

-group *filter*

フィルタ条件に一致するグループのみを表示します。

uxconsole -register - Active Directory への UNIX マシンの登録

UNIX で有効

このコマンドを使用して Active Directory に UNIX ホストを登録します。UNIX ホストの登録は、UNIX 認証ブローカ 設定プロセスの一部として実行され、Active Directory ユーザが UNIX ホストにログインできるようにします。

注: UNIX ホストを登録した後、Active Directory ユーザがホストにログインできるようにするには、UNIX 認証ブローカ をアクティブにする必要があります。

以下の状況では、UNIX ホストを登録することはできません。

- UNIX コンピュータのホスト名が、ドメイン サフィックスを除いて 15 文字より多い場合、登録は失敗します。これは、Active Directory では、コンピュータ オブジェクト名に NetBIOS ベースの文字数制限が適用されるためです。

  たとえば、engineering-dept-sol2 という名前の UNIX コンピュータを Active Directory に登録することはできません。ホスト名が 15 文字を超えるためです。eng-dept-sol2.example.com という名前の UNIX コンピュータは登録できます。ドメイン名を除くホスト名（eng-dept-sol2）が 15 文字より少ないためです。UNIX コンピュータのホスト名を表示するには、hostname コマンドを実行します。

- Active Directory との通信に UNIX ホストが使用する Active Directory サイト内のすべての DC が、uxauth.ini ファイル内の ad セクションの ignore_dc_list 設定に指定されている場合、登録は失敗します。

  UNIX ホストを Active Directory に登録する際、デフォルトで、uxconsole ユーティリティはエンドポイントの物理的な場所に最も近い Active Directory サイトを自動的に検出し、このサイト内の DC とのみ通信します。-t オプションを使用して、この Active Directory サイトを指定することもできます。

このコマンドは、同じコンピュータ上で複数実行できます。たとえば、keytab ファイルが削除された場合、このコマンドを実行して Active Directory への UNIX 認証ブローカ ホストの登録を修復できます。

注: デフォルトの設定を使用するには、引数を指定せずに uxconsole - register コマンドを実行します。ユーザは必要な追加情報を入力するよう求められます。

このコマンドの形式は以下のようになります。

```
uxconsole -register [-a name] [-w pass] [-d domain] [-v level] [-n] [-o container] [-s server] [port #] [-h] [-t site] [-sso]

uxconsole -deregister [-a name] [-w pass] [-v level] [-o container] [-s server] [port #]
```

-register

Active Directory が UNIX 認証ブローカ を登録することを指定します。

-deregister

Active Directory が UNIX 認証ブローカ の登録を解除することを指定します。

-a *name*

Active Directory にコンピュータを登録する権限のあるユーザ名を定義します。

デフォルト: administrator

-w *pass*

Active Directory にコンピュータを登録する権限のあるユーザのパスワードを定義します。

-d *domain*

Active Directory を含むドメイン名を定義します。

-h

プログラム ヘルプを表示します。

-n

登録完了後に uxauthd エージェントが実行されるよう指定します。

このオプションを指定しない場合、登録処理が完了した後に uxauthd は実行されません。

-o *container*

UNIX コンピュータが登録されている Active Directory コンテナ名を定義します。

注: UNIX コンピュータを登録する前に、Active Directory コンテナが存在している必要があります。

-port #

Active Directory リスニング ポート番号を定義します。

-s *server*

Active Directory サーバ名を定義します。

-sso

uxconsole がシングル サインオン（SSO）用の Kerberos ファイルを管理するように指定します。

-t *site*

Active Directory との通信に UNIX 認証ブローカ が使用する DC を含む Active Directory サイトを定義し、uxauth.ini ファイル内の ad セクションの ad_site 設定にサイトの名前を書き込みます。

このオプションは指定することをお勧めします。このオプションを指定しない場合、ユーティリティが自動的に最適な Active Directory サイトを選択します。

注: ignore_dc_list と lookup_dc_list の設定値は、UNIX 認証ブローカ で Active Directory サイト サポートがどのように実装されるかに影響します。

-v *level*

インストール処理中に使用する詳細レベルを定義します。

例: Active Directory での UNIX ホストの登録方法

この例では、UNIX コンピュータを Active Directory に登録する方法を示します。ユーザ名（-a administrator）およびパスワード（-w admin）を入力し、詳細レベル（-v 3）を設定し、インストール完了時に UNIX 認証ブローカ エージェントが実行されないよう指定（-n）します。さらに、Active Directory のコンテナの名前を定義します（-o OU=COMPUTERS）。コンテナは、UNIX コンピュータを Active Directory に登録する前に存在している必要があります。

```
./uxconsole -register -a administrator -w admin –v 3 -n -o OU=COMPUTERS
```

uxconsole -status-Display UNIX 認証ブローカ Status

UNIX で有効

このコマンドを使用して、エンドポイント上の UNIX 認証ブローカ のステータスを表示します。-detail 引数を使用すると、UNIX 認証ブローカ のステータスについて、可能な限りのすべての情報が表示されます。

このコマンドの形式は以下のようになります。

```
uxconsole -status [-detail]
```

-status

UNIX 認証ブローカ ステータスを表示するように指定します。

-detail

UNIX 認証ブローカ ステータスの詳細を表示するように指定します。

例: 詳細な UNIX 認証ブローカ ステータスの表示

uxconsole - status -detail を実行した場合に表示される出力例を以下に示します。

```
#./uxconsole -status -detail
CA Access Control uxconsole v12.52.0.160 - console utility
Copyright (c) 2009 CA. All rights reserved.

Registration domain    - example.com
DCs                    - computer1, computer2
User search base       - DC=unixauth,DC=example,DC=com
User search filters
              Include   - CN=Users; OU=Test
             Exclude   - OU=WrongOU
Group search base      - CN=Users,DC=example,DC=com
Group search filters
             Exclude   - OU=Computers
Trusted domain         - DC=unab,DC=example,DC=com
DCs                    - winserver
User search base       - DC=unabdom,dc=example,dc=com
User search filters
            Include    - CN=users
Group search base      - DC=unab,DC=example,DC=com
UNAB mode              - full integration
full integration           - activated
Agent status           - running, pid = 6178
Time sync               - enabled (NTP server: 192.168.1.100)
Enterprise policy      - login@computer.com (updated: Mon Oct 19 14:36:47 2009)
Enterprise policy      - loginHG@GHNODE#01 (updated: Mon Oct 19 14:36:47 2009)
Local policy           - enabled
Default login access   - deny
AD Unix users          - 16 (updated: Sun Oct 19 15:53:04 2009)
AD Unix groups         - 8 (updated: Sun Oct 19 15:53:04 2009)
AD Windows groups      - 19 (updated: Sun Oct 19 15:53:04 2009)
Migration              - not migrated
CA Access Control      - installed
                         Include AD users and groups in AC ladb : yes
                         Display AD names in AC Audit : no
                         Support AD non-Unix groups in AC: yes
                         PAM authentication in AC utilities : yes
```

この例では、以下の情報が出力されています。

- Active Directoryドメイン名 -- example.com
- エンドポイントが通信する DC -- computer1、computer2
- ユーザおよびグループの検索ベースフィルタ

- 信頼済みドメイン -- unab.example.com
- UNAB モード -- full integration（完全統合）
- UNAB ステータス -- activated（アクティブ）
- UNAB エージェント（uxauthd）ステータス -- running, pid = 6178（実行中）
- 時間同期がアクティブにされたかどうか -- enabled（有効）
- NTP サーバ IP アドレス -- 192.168.1.100
- デプロイされた企業ログイン ポリシーの名前 -- login@computer.com、loginHG@GHNODE#01
- 企業ログイン ポリシーの最終更新日 -- updated: Mon Oct 19 14:36:47 2009
- ローカル ログイン ポリシーがアクティブにされたかどうか -- enabled（有効）
- デフォルト ログイン ポリシーが有効化どうか -- deny（拒否）
- Active Directory 内の UNIX ユーザの数 -- 16（最終更新時間）
- Active Directory 内の UNIX グループの数 -- 8（最終更新時間）
- Active Directory 内の Windows グループの数 -- 19
- UNIX ユーザとグループおよび Windows グループの最終更新時間 -- updated: Sun Oct 19 15:53:04 2009
- ユーザの移行ステータス -- not migrated（移行されていない）
- CA Access Control はこのエンドポイントにインストールされるかどうか -- installed（インストール済み）
- CA Access Control ladb 内に Active Directory ユーザおよびグループに関する情報を含めるかどうか -- yes
- CA Access Control 監査レコード内の Active Directory ユーザおよびグループ名を表示させるかどうか -- yes
- CA Access Control は非 UNIX Active Directory グループをサポートするかどうか -- yes
- CA Access Control ユーティリティ内の PAM 認証をサポートさせるかどうか -- はい

uxconsole -krb — Kerberos 操作の実行

UNIX で有効

このコマンドを使用して、UNIX 認証ブローカ エンドポイントから、チケットの作成などの Kerberos 操作を実行します。Kerberos 操作を実行するために、エンドポイントに Kerberos をインストールする必要はありません。

このコマンドの形式は以下のようになります。

```
uxconsole -krb [-init | -list | -vno | -destroy
```

-init

チケットを取得しキャッシュするように指定します

-list

クレデンシャル キャッシュまたは keytab のコンテンツを表示します

-vno

Kerberos プリンシパルの鍵のバージョン番号を表示します

-destroy

クレデンシャル キャッシュを破壊するように指定します

例: UNIX 認証ブローカ keytab を使用して、Ticket Granting Ticket (TGT)を取得します

以下の例では、UNIX 認証ブローカ keytab を使用して TGT を取得する方法を示しています。

```
./uxconsole -krb -init -k
```

例: クレデンシャル キャッシュのコンテンツをリスト表示します。

以下の例では、クレデンシャル キャッシュのコンテンツをリスト表示する方法を示しています。

```
./uxconsole -krb -list
```

例: 暗号化データを持つ keytab のコンテンツをリスト表示します。

以下の例では、利用可能な暗号化情報を含めて keytab のコンテンツを表示する方法を示します。

```
./uxconsole -krb -list -ke
```

uxconsole -ldap — Active Directory での LDAP クエリの実行

UNIX で有効

このコマンドを使用して、LDAP がインストールされていない UNIX 認証ブローカ エンドポイントから、Active Directory 上で LDAP クエリを実行します。ldapsearch ユーティリティの代わりに、このコマンドを使用します。このコマンドは、UNIX 認証ブローカ インストールのトラブルシューティングに使用できます。たとえば、Active Directory に使用するコンテナを問い合わせることができます。

重要: このコマンドを使用する前に、Ticket Granting Ticket (TGT) があることを確認してください。コマンド uxconsole -krb を使用して、TGT を取得できます。

注: LDAP フィルタは RFC 2254 に準拠する必要があります。

このコマンドの形式は以下のようになります。

```
uxconsole -ldap -search [-d DC] [-p port] [-b base] [-s scope] [filter [attributes]]
```

-search

検索オプションを指定します

-d *DC*

問い合わせるドメイン コントローラを指定します

-p *port*

使用する LDAP ポートを指定します

-b *base*

検索ベースを指定します

-s scope

検索範囲を指定します

デフォルト: sub

filter *[attributes]*

使用するフィルタおよび属性を指定します

注: フィルタを指定しない場合、'(objectClass=*) が使用されます。属性を指定しない場合、select all オプション('*') が使用されます。

例: DSE の表示

以下の例は、DSE の表示方法を示しています。

```
./uxconsole -ldap -search '(&(objectClass=user) (objectCategory=user) )'
```

uxconsole -dbdump—Display UNAB NSS cache data

UNIX で有効

このコマンドを使用して、UNIX 認証ブローカ NSS データベースからユーザおよびグループの情報を表示します。このコマンドを使用して、Active Directory に定義されているユーザおよびグループに関する情報を表示できます。

このコマンドの形式は以下のようになります。

```
uxconsole -dbdump [table [item]]
```

table [*item*]

テーブルおよび項目のコンテンツを表示するように指定します。

注: テーブル名を指定しない場合、このコマンドは利用可能なテーブルをすべて表示します。

例: キャッシュに格納されている Active Directory ユーザをすべて表示します。

以下の例は、エンドポイント キャッシュに格納された Active Directory ユーザをすべて表示する方法を示しています。

```
./uxconsole -dbdump pw
```

例: キャッシュに格納されている Active Directory グループをすべて表示します。

以下の例は、エンドポイント キャッシュに格納された Active Directory グループをすべて表示する方法を示しています。

```
./uxconsole -dbdump -gr
```

uxconsole -debug -- モジュールの詳細レベルを設定する

UNIX で有効

モジュールごとに詳細レベルを設定するには、このコマンドを使用します。UNIX 認証ブローカ は、また、PAM および NSS のデバッグ情報をデバッグ情報ファイルへ送信します。

このコマンドの形式は以下のようになります。

```
uxconsole -debug -m mod [-v level]
```

-m *mod*

詳細レベルを設定するモジュールを指定します。

オプション: nss、pam、all

-v *level*

詳細レベルを指定します。

制限:0 ～ 5

UNIX 認証ブローカ は、以下のファイルにデバッグ情報を書き込みます。

```
UNABInstallDir/log/debug/pam_debug
UNABInstallDir/log/debug/pam_debug.back
UNABInstallDir/log/debug/nss_debug
UNABInstallDir/log/debug/nss_debug.back
```

注: エージェントが実行されていない場合に、詳細レベルを 1 以上に設定すると、UNIX 認証ブローカ PAM モジュールが有効にされたことを示すメッセージが表示されます。UNIX 認証ブローカ は、syslog にのみデバッグ情報を送信します。

uxconsole -verify -- Active Directory ユーザ アカウント UNIX 属性の確認

UNIX で該当

このコマンドを使用して、Active Directory ユーザ アカウントが UNIX 認証ブローカ で使用可能であることを確認します。このコマンドは、ユーザ アカウントを特定し、UNIX 属性(ログイン シェル、ホーム ディレクトリ、UID および GID)が、UNIX 認証ブローカ ユーザ キャッシュ データベース内に存在する値と一致していることを確認します。

注: このコマンドはユーザ パスワードを確認することはしません。

このコマンドの形式は以下のようになります。

```
uxconsole -verify -user <user_name>[<user_name1>][<user_name2>...]
```

-user

Active Directory 内のユーザ アカウントの UNIX 属性を確認するように指定します。

<*user_name*>

Active Directory ユーザ アカウントを指定します。

例: Active Directory ユーザ アカウント UNIX 属性の確認

以下の例は、Active Directory ユーザ アカウント UNIX 属性を確認する方法を示します。

```
./uxconsole -verify -user Joe
```

この例では -verify コマンドを使用してユーザ アカウント Joe の UNIX 属性を確認します。UNIX 認証ブローカ は以下を実行します。

- /etc/shells ファイルを参照し、指定されたログイン シェルがサポートされていることを確認します
- ユーザ名の長さが、オペレーティング システムによる制限内であることを確認します
- ホーム ディレクトリが指定されていることを確認します
- UID が指定されていることを確認します
- GID が指定されていることを確認します

uxconsole が Active Directory サイトを検出する方法

Active Directory に UNIX 認証ブローカ エンドポイントを登録するとき、デフォルトでは、uxconsole ユーティリティは最も近い Active Directory サイトを検出し、このサイトのドメイン コントローラ(DC)とのみ通信します。

以下のプロセスでは、uxconsole がどのように最も近い Active Directory サイトを検出するかについて説明します。

1. UNIX 認証ブローカ エンドポイントは、以下の形式で、SRV(サービス)レコードについて DNS にクエリします。

   _ldap._tcp.dc._msdcs.*domainName*

   DNS は、ドメインにある DC のレコードを返します。

2. エンドポイントは、以前のクエリで返された DC にバインドおよび認証することにより、Active Directory にアクセスします。

   注: エンドポイントは返される DC のいずれにもバインドできます。

3. エンドポイントは LDAP クエリを使用して、エンドポイントが存在するサイトを Active Directory で検索します。クエリは以下のフィルタを使用します。

   - ベース Dn -- 値はありません。
   - スコープ -- ベース
   - 属性 -- Netlogon
   - DnsDomain -- 完全修飾ドメイン名
   - ntver -- 6.00

   たとえば、「(&(DnsDomain=example.company.com)(ntver=6.00))」のようなフィルタを使用します。

   DC は、エンドポイントが存在するサイトの名前を返します。

   注: DC はエンドポイント IP アドレスを使用して、エンドポイントが存在するサイトを決定します。

4. エンドポイントは、以下の形式で、SRV レコードについて DNS にクエリします。

   _ldap._tcp.*LocalSiteName*._sites.dc._msdcs.*domainName*.

   DNS は、エンドポイントが存在するサイトにある DC のレコードを返します。エンドポイントはこのサイトの DC とのみ通信します。

UxImport ユーティリティ - UNIX オペレーティング システムからの情報の抽出

UNIX で該当

uximport ユーティリティは、UNIX オペレーティング システムから、定義されているユーザ、グループ、端末、ホスト、および TCP サービスに関する情報を抽出します。NIS がインストールされている場合は、NIS からの情報に基づいてシステムの環境設定が行われます。また、DNS もサポートします。uximport をインストール手順の一部として使用する必要があります。

uximport は、抽出された情報を自動的に処理して、ユーザおよびグループを CA Access Control データベースに追加する際に使用できる selang のコマンドを生成します。生成されたコマンドは標準出力に表示されます。出力をファイルに送るか、または selang ユーティリティへのパイプラインを使用します。

このコマンドの形式は以下のようになります。

```
UxImport switches [options]
```

--a

ユーザ、グループ、およびホストをインポートし、ユーザをそれぞれのデフォルト グループに追加するのに必要な selang のコマンドを生成します。

-c

ユーザをそれぞれのデフォルト グループに明示的に追加するのに必要な selang のコマンドを生成します。

注: -g スイッチを指定してグループをインポートする場合も、CA Access Control ではユーザが明示的にリンクされているグループにユーザを追加するコマンドを生成します。

--g

UNIX および NIS から CA Access Control データベースにグループをインポートするのに必要な selang のコマンドを生成します。

-h

UNIX、NIS および DNS から CA Access Control データベースにホストをインポートするのに必要な selang のコマンドを生成します。uximport は、/etc/hosts ファイルおよび NIS からホスト情報を抽出し、HOST リソースを作成します。/etc/hosts ファイルまたは NIS から抽出された各ホスト エントリに対して、適切な newres コマンドが作成され、任意の TCP サービスを受け取る権限がそのホストに割り当てられます。

また、-d オプションを指定すると DNS がサポートされます。一部のコンピュータでは、指定された DNS デーモンが実行中の場合は、/etc/hosts ファイルおよび NIS から抽出された情報が無視されます。Solaris では、収集される情報は、/etc/nsswitch.conf ファイルのシステム環境設定によって異なります。

--t

UNIX および NIS から CA Access Control データベースに端末ルールをインポートするのに必要な selang のコマンドを生成します。

uximport は、/etc/hosts ファイルおよび NIS からホスト情報を抽出し、TERMINAL リソースを作成します。*/etc/hosts* ファイルまたは NIS から抽出された各エントリに対して、適切な newres TERMINAL コマンドが作成され、その端末からのログイン許可が与えられます。

また、-d オプションを指定すると DNS がサポートされます。一部のコンピュータでは、指定された DNS デーモンが実行中の場合は、/etc/hosts ファイルおよび NIS から抽出された情報が無視されます。Solaris では、収集される情報は、/etc/nsswitch.conf ファイルのシステム環境設定によって異なります。

-T

UNIX および NIS から CA Access Control データベースに TCP サービスをインポートするのに必要な selang のコマンドを生成します。名前は UNIX の GECOS に基づいて設定されます。名前が 40 文字より長い場合は、40 文字に切り詰められます。

-u

UNIX および NIS から CA Access Control データベースにユーザをインポートするのに必要な selang のコマンドを生成します。実際のユーザ名は UNIX の GECOS に基づいて設定されます。名前が 40 文字より長い場合は、40 文字に切り詰められます。

options

-d

インポートするホストおよび端末のリストの生成に DNS を使用するように指定します。-h スイッチまたは -t スイッチを設定する必要があります。

-f

同じ名前が複数ある場合は検索を省略します。このオプションは標準の uximport プロセスを使用しないため、多数のユーザおよびグループを迅速にインポートし、メモリを節約できます。-f オプションはホストには適用されないため、スイッチ -u、-g、または -a の 1 つ以上と組み合わせて指定する必要があります。また、-c スイッチと -f オプションを同時に指定する場合も、これらのスイッチのいずれかを使用します。

Join ルールおよび Surrogate ルールは、Create レコードと共に出力されます。

--G

グループの SURROGATE クラス ルールを作成します。uximport はレコードを、定義した各グループの SURROGATE クラスに追加します。その結果、SURROGATE 要求は保護されたリソースになります。また、root ユーザが各グループの代理になれるようにルールを追加します。

-gr *n*

すべてのユーザに対して猶予ログイン回数を指定します。ログイン回数が *n* 回を超えると、ユーザはパスワードを変更する必要があります。これによって、USER クラスのレコードの PASSWD_L_C プロパティが更新されます。

-o *owner*

各レコードに所有者権限ルールを設定します。root ユーザが自動的にすべてのレコードの所有者になることを防止するために、このオプションを使用することをお勧めします。*owner* には、uximport で定義したすべてのレコードの所有者権限が割り当てるユーザまたはグループの名前を指定します。

注: *owner* の後に別個の引数としてこのオプションを指定する必要があります。

-pr *groupname*

プロファイル グループをユーザに割り当てます。このオプションを指定した場合、CA Access Control はユーザのプロファイルの作成時に指定したグループを使用します。指定しない場合は、UNIX のプライマリ グループを使用します。

-r

失敗してもスキャンを継続するように指定します。

-s

ユーザおよびグループの SURROGATE クラス ルールを作成します。uximport は、定義したすべてのグループに対して SURROGATE レコードを追加します。したがって、グループへの SURROGATE 要求は保護されたリソースになります。

-U

ユーザの SURROGATE クラス ルールを作成します。uximport はレコードを、定義した各ユーザの SURROGATE クラスに追加します。その結果、SURROGATE 要求は保護されたリソースになります。また、root ユーザが各ユーザの代理になれるようにルールを追加します。

-v

プログラムのステータス(詳細モード)を表示します。 サイトに多数のユーザ、グループ、またはホストが存在する場合は、プログラムの進行状況を検証できるように、このオプションを指定することをお勧めします。

例

以下のコマンドによって、UNIX および NIS のデータベースから、ユーザ、グループ、およびホストの情報がすべて抽出されます。その後、抽出したレコードをデータベースに追加する selang のコマンドが作成されます。uximport は SURROGATE クラス レコードを作成し、進行状況を表示します。出力は、ホーム ディレクトリにある uxinfo.seos ファイルに送られます。

```
UxImport -a -s -v > ~/uxinfo.seos
```

詳細情報:

seerrlog ユーティリティ - エラー ログ レコードの表示 (P. 189)
selang ユーティリティ - CA Access Control コマンドラインの実行 (P. 200)
seuidpgm ユーティリティ - trusted プログラムの抽出 (P. 260)

uxpreinstall Utility - システム コンプライアンスのチェック

UNIX で有効

uxpreinstall ユーティリティは、UNIX エンドポイントが UNIX 認証ブローカ システム要件に準拠していることを確認します。uxpreinstall は、以下の検査を実行します。

- オペレーティング システムに、インストールされているバージョン、パッチ、ライブラリおよびモジュールを問い合わせます。
- DNS サーバに対してクエリを行って、ドメイン名を解決します。
- LDAP と Kerberos のサービスを検索します。
- 詳細については、LDAP サービスを使用して Active Directory に対してクエリを行ってください。
- 利用可能なポートのスキャン
- ローカル ホストと Active Directory ドメインの間のクロック スキューを確認します。
- ネットワーク アプリケーション、ネットワーク サーバおよび ssh と sshd の特性が Kerberized Single Sign On（SSO）ログインをサポートすることを確認します。

uxpreinstall ユーティリティがチェックを続行できない重大なエラーを検出した場合、ユーティリティはただちに停止します。

uxpreinstall の実行後、チェックの結果が表示されます。uxpreinstall 出力におけるエラーまたは競合は、UNIX 認証ブローカ の操作で、ユーザ認証エラーなどの問題を起こす可能性があります。uxpreinstall によって識別されるエラーまたは競合を解決してから、<uban> をアクティブ化し、使用することを強くお勧めします。

重要： uxpreinstall ユーティリティは、実在または潜在的な問題を報告しますが、その修正は行いません。このユーティリティを使用して、オペレーティング システムまたは UNIX 認証ブローカ を設定することはできません。

uxpreinstall の実行は、UNIX 認証ブローカ インストールの前後に行うことができます。uxpreinstall を実行してから UNIX 認証ブローカ をインストールすると、ユーティリティによって一時 Kerberos ファイルが作成され、uxauth.ini 設定ではなく、Kerberos ファイルの設定がチェックされます。UNIX 認証ブローカ をインストールしてから uxpreinstall を実行すると、ユーティリティによって一時 Kerberos ファイルは作成されません。代わりに、uxauth.ini ファイルの[ad]セクションにある lookup_dc_list トークンの値が確認されます。

注: UNIX 認証ブローカ をインストールする前に uxpreinstall を実行するには、UNIX 認証ブローカ がインストールされている別のエンドポイントからユーティリティをコピーします。

uxpreinstall 出力の以下のセクションによって、エンドポイント設定によってユーザが Kerberized SSO ログインを使用できるかどうかが確認されます。UNIX 認証ブローカ ユーザの SSO ログインを有効にしない場合、これらのセクションの情報を無視できます。

- CHECKING KERBEROS RPMS
- CHECKING NATIVE KERBEROS
- == SSO 操作に影響を及ぼす sshd 特性のレポート ==
- == SSO 操作に影響を及ぼす ssh 特性のレポート ==
- ネットワーク アプリケーションの確認
- ネットワーク サーバの確認

注: uxpreinstall を使用したシステムの適合性の確認の詳細については、「*実装ガイド*」を参照してください。

このコマンドの形式は以下のようになります。

```
uxpreinstall [-a user] [-w passwd] [-n ntp_server] [{-d domain | -s server}] [-p port]
[-f logfile] [-v level] [-l] [-h]
```

-a *user*

Active Directory へのログインに使用するユーザ アカウントを定義します。

デフォルト: Administrator

-w *passwd*

ユーザ アカウントのパスワードを定義します。

-n *ntp_server*

Network Time Server（NTP）の名前を定義します。

-d *domain*

Active Directory がインストールされているドメイン名を定義します。

-s *server*

Active Directory サーバの名前を定義します。

-p *port*

Active Directory がリスンするポート番号を定義します。

-f *logfile*

ログ ファイルに使用する名前を定義します。

-v *level*

uxpreinstall 出力の詳細レベルを定義します。

オプション:

0 -- uxpreinstall が実行する確認、および識別するエラーまたは競合の概要を表示します。

1 -- 0 と同じ情報および各確認に関する追加情報を表示します。

2 -- 1 と同じ情報、および uxpreinstall が各確認に使用するコマンドを表示します。

3 -- 2 と同じ情報および各コマンドの出力を表示します。

4 -- 3 と同じ情報およびパッケージの詳細など、一部の確認の追加情報を表示します。

デフォルト: 0

-l

syslog ファイル上でチェックを実行するように指定します。root ユーザのみに適用可能です。

-h

ユーティリティ ヘルプを表示して終了するように指定します。

例: uxpreinstall ユーティリティの実行

この例では、Active Directory ドメイン domain.com に対して、管理者ユーザのクレデンシャルで uxpreinstall ユーティリティを詳細レベル 1 で実行します。

```
/opt/CA/uxauth/bin/uxpreinstall -a administrator -w admin -d mydomain.com -v 1
```

例: uxpreinstall ユーティリティ レポート

以下は、システムが要件に準拠しているかどうかを判断する方法を示す uxpreinstall ユーティリティレポートのスニペットです。

```
OS detected: Linux 2.6.5-7.244-default
*********************************************
 CHECKING CLOCK SYNCHRONIZATION
*********************************************
Comparing the value of the currentTime attribute in DSE with the local time ...
Current clock skew is 34 sec.
The default value for the maximum clock skew is 300 seconds.
Warning! Significant clock skew can cause user authentication failure
---------------------------------------------
 W A R N I N G
---------------------------------------------

*********************************************
 CHECKING KERBEROS AUTHENTICATION VIA AD
*********************************************
principal_name = <Administrator@mydomain.com>

Kerberos authentication for <Administrator@mydomain.com> succeeded

---------------------------------------------
 S U C C E S S
---------------------------------------------

*********************************************
 CHECKING AD SCHEMA VERSION
*********************************************
Trying LDAP service at server.mydomain.com:389
Binding to Active Directory via 'server1.mydomaiin.com' ...

AD Schema version 31 (Windows Server 2003 R2 or Windows Server 7 (AD LDS))

supports full and partial UNAB integration modes.
---------------------------------------------
 S U C C E S S
---------------------------------------------
. . .
```

この例では、以下の情報が出力されています。

- ローカル ホスト上で実行中のオペレーティング システム -- Linux 2.6.5-7.244-default
- クロック スキュー -- 34 秒
- Kerberos サービス -- <Administrator@mydomain.com> の Kerberos 認証に成功
- Active Directory スキーマ バージョン -- AD Schema version 31
- Active Directory がインストールされているオペレーティング システムのバージョン -- Windows Server 2003 R2 または Windows Server 7
- Active Directory スキーマは UNIX 認証ブローカ の完全統合モードと部分統合モードの両方をサポートしています。

サービスおよびデーモンの詳細

このセクションでは、CA Access Control のすべてのデーモンおよびサービスについて説明します。

CA Access Control エージェント マネージャ

Windows で有効

CA Access Control エージェント マネージャ サービスは、CA Access Control プラグイン用の管理サービスを提供します。CA Access Control エージェント マネージャ サービスは、以下のサービスをプラグインに提供します。

- スケジューリング サービス -- プラグイン スケジュールを管理します。
- Watchdog サービス -- プラグインが実行されていることを確認し、失敗の場合はプラグインを開始します。
- メッセージ サービス -- メッセージ キュー サービスをプラグインに提供し、エンタープライズ管理サーバが使用不可になった場合にメッセージを格納します。

エージェント マネージャ レジストリ キーは、エージェント マネージャの調整ができるレジストリ エントリを含んでいます。キーは以下の場所にあります。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥common¥AgentManager
```

CA Access Control メッセージ キュー サービス

Windows で有効

CA Access Control メッセージ キュー サービスは、エンタープライズ管理サーバとその他の CA Access Control コンポーネントの間の着信および送信メッセージをすべて処理するメッセージ キュー（TIBCO サーバ）を管理します。メッセージ キューには、エンタープライズ管理サーバと通信する各クライアント コンポーネント専用の以下のキューがあります。

- レポート キュー - エンドポイント データベースのスケジュールされたスナップショットを受信します。

  レポート サービスは、スナップショットを使用して CA Access Control レポートを生成します。

- 監査キュー - エンドポイント上で発生した監査イベントを受信します。

  監査イベントを収集し、レポートするように CA Enterprise Log Manager を設定できます。

- サーバ - エンドポイント キュー - エンドポイントが収集した DMS からのデータを受信します。

  たとえば、UNAB 設定ポリシーをデプロイする場合、DMS は設定ポリシーをこのキューに送信します。次に UNAB エージェントは、このキューからポリシーを収集し、UNAB エンドポイントにポリシーをデプロイします。

- エンドポイント - サーバ キュー - DMS が収集したエンドポイントの情報を受信します。

  たとえば、UNAB エンドポイントはハートビート通知をこのキューに送信します。DMS は、このキューからハートビート通知を収集し、データベース内のエンドポイントのステータスを更新します。

CA Access Control Web サービス

Windows で有効

Web サービスは、CA Access Control の企業インストールを管理するために使用する Web ベースアプリケーションを管理します。Web ベースのアプリケーションはアプリケーション サーバにインストールします。アプリケーション サーバは、デフォルトではエンタープライズ管理サーバ上にインストールされます。

アプリケーション サーバには次の Web ベース アプリケーションが含まれています。

- CA Access Control エンタープライズ管理 -- 企業全体のポリシーを管理し、UNIX 認証ブローカ エンドポイントを設定できます。CA Access Control エンタープライズ管理 には、企業全体の特権アカウントを管理でき、特権アカウントのパスワード ボールトとして機能する、特権ユーザ パスワード管理 (PUPM)も含まれています。
- CA Access Control エンドポイント管理 - 各 CA Access Control エンドポイントを中央の管理サーバから管理および設定します。
- CA Access Control パスワード マネージャ -- CA Access Control ユーザ パスワードを管理できます。 CA Access Control ユーザのパスワードを変更したり、次回ログイン時にユーザに強制的にパスワードを変更させたりすることができます。

Web サービス レジストリ キーは、Web サービスの調整ができるレジストリ エントリを含んでいます。キーは以下の場所にあります。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥WebService
```

注: ユーザが UNIX コンピュータにエンタープライズ管理サーバをインストールする場合、eacws デーモンは Web ベースアプリケーションを管理します。

CA Identity Manager -- コネクタ サーバ (Java) サービス

Windows で有効

CA Identity Manager -- コネクタ サーバ (Java) サービスは、Windows オペレーティング システムや SQL Server などの、Java によってサポートされている管理対象デバイスとの通信を管理します。このサービスは、さらに 特権ユーザ パスワード管理 エンドポイント上の特権アカウントを管理します。

eacws デーモン

UNIX で有効

eacws デーモンは、CA Access Control の企業インストールを管理するために使用する Web ベースアプリケーションを管理します。Web ベースのアプリケーションはアプリケーション サーバにインストールします。アプリケーション サーバは、デフォルトではエンタープライズ管理サーバ上にインストールされます。

アプリケーション サーバには次の Web ベース アプリケーションが含まれています。

- CA Access Control エンタープライズ管理 -- 企業全体のポリシーを管理し、UNIX 認証ブローカ エンドポイントを設定できます。CA Access Control エンタープライズ管理 には、企業全体の特権アカウントを管理でき、特権アカウントのパスワード ボールトとして機能する、特権ユーザ パスワード管理（PUPM）も含まれています。
- CA Access Control エンドポイント管理 - 各 CA Access Control エンドポイントを中央の管理サーバから管理および設定します。
- CA Access Control パスワード マネージャ - CA Access Control のユーザ パスワードを管理します。CA Access Control ユーザのパスワードを変更したり、次回ログイン時にユーザに強制的にパスワードを変更させたりすることができます。

注: Windows コンピュータにエンタープライズ管理サーバをインストールする場合、CA Access Control Web サービスは Web ベースアプリケーションを管理します。

KBLAudMgr デーモン -- セッション ロギング

UNIX で有効

KBLAudMgr デーモンは、キー ロガーのセッション記録エージェントを管理します。UNIX と Linux のエンドポイント内の特権ユーザ セッションを追跡するためにキー ロガーを使用します。キー ロガーは対話式セッションを記録し、終了時に再生して分析およびレポートのため CA Enterprise Log Manager に送信できます。

seos.ini ファイルの[kblaudit]セクションは、キー ロガー エージェントを調整できるトークンを含みます。

PolicyFetcher デーモン

UNIX で有効

PolicyFetcher デーモンは定期的にデプロイされたポリシー内の偏差を確認して、DH 上のデプロイメント タスクを検索し、ローカル CA Access Control データベース(seosdb)にポリシー更新を適用、一定の間隔で DH にハートビートを送信します。

start DEVCALC selang コマンドを使用して、偏差計算機能を開始します。エンドポイントに詳細ポリシー管理をインストールした場合、PolicyFetcher は偏差計算機能を実行します。

ReportAgent デーモン

UNIX で有効

レポート エージェント(ReportAgent)デーモンは、レポート スナップショットおよび監査イベントを配布サーバに送信して CA Access Control、UNIX 認証ブローカ、および CA Enterprise Log Manager のレポートに含まれるようにする ReportAgent を管理します。UNIX コンピュータで、ReportAgent ユーティリティを *ACSharedDir*/bin ディレクトリから実行します。*ACSharedDir* は、デフォルトでは /opt/CA/AccessControlShared ディレクトリです。report_agent.sh スクリプトを使用して、ReportAgent を設定、開始、停止することもできます。

accommon.ini ファイルの[ReportAgent]セクションは、レポート エージェント デーモンの動作をコントロールするトークンを含んでいます。

ReportAgent サービス（Windows）

Windows で有効

レポート エージェント（ReportAgent）サービスは、レポート スナップショットおよび監査イベントを配布サーバに送信して CA Access Control、UNIX 認証ブローカ、および CA Enterprise Log Manager のレポートに含まれるようにする ReportAgent を管理します。エンドポイントに CA Access Control をインストールし、ReportAgent のインストールを選択した場合、ReportAgent サービスは起動時に自動的に実行されます。

ReportAgent レジストリ キーは、ReportAgent の調整ができるレジストリ エントリを含んでいます。キーは以下の場所にあります。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥ReportAgent
```

sepmdd デーモン（UNIX）

Policy Model デーモンです。

sepmdd デーモンは、PMDB のデーモンです。sepmdd デーモンは以下の機能を実行します。

- Policy Model の CA Access Control データベースおよび UNIX データベースの管理
- サブスクライバのデータベースの管理
- PMDB からサブスクライバ データベースへの変更の伝達

sepmdd デーモンは *ACInstallDir*/lbin ディレクトリにあります。PMDB がすでに作成されている場合、これが開始されます。

構文

```
sepmdd policyModel
```

パラメータ

policyModel

Policy Model の名前です。

その他のファイル

その他の特別なファイルは使用しません。

注:

selang を使用して(hosts pmd@hostname で)ターゲットとして Policy Model を選択した場合、sepmdd に対するクエリは PMDB に適用されますが、さまざまなサブスクライバ データベースには適用されません。

- PMDB がそれ自体のサブスクライバではないことを確認します。PMDB がそれ自体にサブスクライブされた場合、Policy Model が遮断されるか、ネットワークの負荷が大きくなり、ディスク領域が消費されます。
- selang の UNIX 環境で Policy Model を更新する場合は、newusr コマンドに複数のユーザを指定できません。また newgrp コマンドに複数のグループを指定できません。
- selang から UNIX ファイル属性を更新すると、Policy Model はコマンドがサブスクライバに送信されたことを示すメッセージを生成します。
- Policy Model を操作する場合、UNIX ファイル属性のステータスは参照できません。
- _shutoff_timeout_ の値を 0 に設定した場合、手動で停止するまで sepmdd デーモンは無限に実行を続けます。Policy Model デーモンを停止するには、sepmd -k コマンドを実行します。

詳細情報:

sepmd ユーティリティ (P. 222)
sepmdadm ユーティリティ - PMDB 定義の作成 (P. 236)
seagent デーモン (P. 314)

sepmdd の機能

CA Access Control(seagent)は sepmdd を起動します。つまり、sepmdd を明示的に実行する必要はありません。sepmdd デーモンは、CA Access Control の論理ユーザ ID「_seagent」および UNIX のユーザ ID *root* で実行されます。sepmdd を実行する別の論理ユーザを指定することはできません。

PMDB は共通ディレクトリに格納されます。共通ディレクトリの名前は、Policy Model が格納されている端末上の seos.ini ファイルの [pmd] セクションにある _pmd_directory_ トークンを使用して指定します。各 Policy Model は、共通ディレクトリ内の別々のサブディレクトリに格納されます。Policy Model の名前は、Policy Model が格納されているサブディレクトリの名前と同じです。

sepmdd の起動時に、更新の必要があるサブスクライバ データベースの有無が確認され、必要に応じてサブスクライバ データベースが更新されます。この起動プロセスの後、sepmdd はユーザからの要求を待機します。ユーザからの要求は、Policy Model 管理プログラム（sepmd）および selang のユーティリティによって、seagent を使用して送信されます。

sepmdd は、受け取った要求を PMDB に適用し、ユーザに結果を返します。要求を伝達する必要がある場合は、サブスクライバ データベースに更新情報を伝達します。

sepmdd デーモンは、_QD_timeout_ トークンに指定された期間にサブスクライバ データベースの更新を試みます。制限時間が経過した時点でサブスクライバを更新できなかった場合、デーモンはそのサブスクライバの更新処理を省略して、サブスクライバ リストにある残りのサブスクライバの更新を試みます。sepmdd は、サブスクライバ リストの 1 回目のスキャンが終了した後、2 回目のスキャンを実行します。2 回目のスキャンでは、1 回目のスキャンで更新できなかったサブスクライバの更新を試みます。2 回目のスキャンでは、接続システム コールがタイムアウトになるまで（約 90 秒間）サブスクライバの更新を試みます。

注: _QD_timeout_ トークンが seos.ini ファイルおよび pmd.ini ファイルの両方に記述されている場合があります。その場合、sepmdd は pmd.ini ファイルの値を使用します。

2 回目のスキャン時にもサブスクライバを更新できない場合、sepmdd は 30 分間隔で更新情報の送信を試みます。この送信間隔の変更は、_retry_timeout_ トークンの設定で行います。更新情報は受信したときと同じ順序で送信する必要があるため、sepmdd はサブスクライバ データベースが使用可能になるまで、その後の更新情報を送信しません。

サブスクライバ データベースの seos.ini ファイルの [pmd] セクションにある pull_option トークンを「yes」設定すると、サブスクライバ データベースがただちに更新されます。マシン上の全 Policy Model について、ホストおよび各サブスクライバの PMDB が起動していることを seagent が親 Policy Model に通知すると、sepmdd は更新情報をただちに送信します。

sepmdd がサブスクライバ データベースの更新に失敗するたびに、Policy Model のエラー ログに警告メッセージが書き込まれます。Policy Model のエラー ログの詳細については、「*UNIX エンドポイント管理ガイド*」を参照してください。

CA Access Control は、Policy Model に追加または Policy Model から削除されるサブスクライバを完全修飾しようとします。

使用不可能なサブスクライバのリストからサブスクライバを削除するには、以下のコマンドを入力します。

```
sepmd -r policyModel subscriber
```

サブスクライバ データベースと PMDB が異なる場合など、サブスクライバ データベースで更新が拒否された場合、sepmdd はその Policy Model のエラー ログにエラー メッセージを書き込み、処理を続行します。

エラー ログを表示するには、PMDB が格納されているホストで以下のコマンドを入力します。

```
sepmd -e policyModel
```

一定期間アクティブでない sepmdd は、自動的に停止することができます。ただし、デフォルトでは、sepmdd は自動的に停止しません。sepmdd を自動的に停止するには、_shutoff_time_ トークンに 0 より大きい値を設定します。この値は、sepmdd がアクティブでない状態で待機する時間の長さ(分単位)を示します。この時間が経過すると、sepmdd は自動的に停止します。sepmdd を手動で停止するには、以下のように入力します。

```
sepmd -k policyModel
```

重要: sepmdd を手動で停止する場合に、UNIX の *kill -9* コマンドを使用しないでください。このコマンドを使用すると、PMDB が壊れる場合があります。

UID と GID の同期

表示されるメッセージでは、ユーザはユーザ名ではなく UID で参照されるため、各ユーザの UID を把握する必要があります。ただし、PMDB を使用している場合は、新規ユーザの UID の割り当て方法に注意しないと、各サブスクライバのコンピュータで同じユーザに異なる UID が割り当てられることがあります。したがって、すべての場所で同じ UID を指定するように各ユーザに指示することをお勧めします。GID も同様に割り当てます。「*UNIX エンドポイント管理ガイド*」の「UID と GID の同期」を参照してください。

フィルタ メカニズム

PMDB では、次のように特定のサブスクライバ端末を選択して更新できます。サブスクライバ端末にどのレコードを送信するかを定義するには、pmd.ini ファイルで filter トークンにフィルタ ファイルを指定します。このように設定すると、フィルタ ファイルを通過したレコードのみが更新情報としてサブスクライバ端末に送信されます。

フィルタ ファイルは、各行に 6 つのフィールドを持つ複数の行で構成されます。フィールドには以下の情報が含まれます。

- 許可または禁止されるアクセスの種類。指定可能な値は、AUTHORIZE_DELETE、AUTHORIZE_MODIFY、CREATE、DELETE、DEPLOY、EDIT、FILESCAN、GET、SEOS_ACCS_READ、JOIN_DELETE、JOIN_MODIFY、MODIFY、READ、START、または UNDEPLOY です。
- 影響を受ける環境。指定可能な値は、AC、CONFIG、UNIX、NT、または NATIVE です。
- レコードのクラス。指定可能な値は、ユーザ定義クラスを含む CA Access Control のすべてのクラスです。

- ルールが適用されるクラスのオブジェクト。たとえば、User1、AuditGroup、または TTY1 になります。
- レコードによって許可または取り消されるプロパティ。たとえば、ユーザ レコードのフィルタ行の OWNER および FULL_NAME は、これらのユーザ プロパティを持つコマンドはすべてフィルタ処理されることを意味します。各プロパティを正確に入力する必要があります。
- 該当するレコードをサブスクライバ端末に転送するかどうか。
  指定可能な値は、PASS または NOPASS です。

どのフィールドでも、アスタリスクを使用して「可能なすべての値」を指定することができます。同じレコードが複数の行に該当する場合は、最初の該当する行が使用されます。

フィルタ ファイルの各行では、フィールドをスペースで区切ります。フィールドに複数の値がある場合は、値をセミコロンで区切ります。「#」で始まる行はコメント行とみなされます。空白行は使用できません。フィルタ ファイルの行の例を次に示します。

CREATE	AC	USER	*	FULL-NAME;OBJ_TYPE	NOPASS
アクセス形式	*環境*	*クラス*	*レコード名 (* = すべての名前)*	*properties*	*処理方法*

たとえば、この行を指定したファイルの名前が TTY1_FILTER で、Policy Model TTY1 の pmd.ini ファイルにフィルタとして filter=/opt/CA/AccessControl//TTY1_FILTER を指定したとします。Policy Model TTY1 は、FULL_NAME および OBJ_TYPE(管理者、監査担当者など)プロパティを持つの新規 CA Access Control ユーザを作成するレコードを送信しません。アスタリスクは「すべての名前」を意味します。

各アクセス値に関連する selang のコマンドを以下に示します。

アクセス	selang のコマンド
AUTHORIZE_DELETE	authorize-
AUTHORIZE_MODIFY	authorize
CREATE	newres、newusr、newgrp、newfile
DELETE	rmres, rmusr, rmgrp, rmfile, join- (UNIX)

アクセス	selang のコマンド
DEPLOY	deploy
EDIT	editres、editusr、editgrp、editfile
FILESCAN	search
GET	get devcalc
JOIN_DELETE	join-
JOIN_MODIFY	join
MODIFY	chres、chusr、chgrp、chfile、join（UNIX）
READ	list
START	start devcalc
UNDEPLOY	deploy- (undeploy)

CA Access Control はルールを検証しません。したがって、ルールに無効な値を入力すると、そのルールは更新トランザクションと一致しません。

CA Access Control Policy Model サービス（sepmdd）

Windows で有効

CA Access Control Policy Model サービス（sepmdd）は PMDB サービスです。sepmdd は以下の機能を実行します。

- Policy Model の CA Access Control データベースおよび Windows データベースの管理
- サブスクライバのデータベースの管理
- PMDB からサブスクライバ データベースへの変更の伝達

sepmdd サービスは、SeOSAgent によって開始されます。sepmdd を明示的に実行する必要はありません。各 Policy Model は、起動済みまたは停止済みのいずれかの状態です。

PMDB は共通ディレクトリに格納されます。HKLM¥Software¥ComputerAssociates¥AccessControl¥Pmd サブキーのレジストリ値 _pmd_directory_ で、共通ディレクトリの名前を指定します。各 Policy Model は、共通ディレクトリ内の別々のサブディレクトリに格納されます。Policy Model の名前は、Policy Model が格納されているサブディレクトリの名前と同じです。

sepmdd の起動時、更新の必要があるサブスクライバ データベースの有無が確認され、必要に応じてサブスクライバ データベースが更新されます。このスタートアップ プロセスの後、sepmdd サービスはユーザからの要求を待機します。ユーザからの要求は、Policy Model 管理ユーティリティの sepmd によって送信されるか、または CA Access Control Agent を使用して selang によって送信されます。

sepmdd は、受け取った要求を PMDB に適用し、ユーザに結果を返します。要求を伝達する必要がある場合は、サブスクライバ データベースに更新情報を伝達します。

sepmdd サービスは、サブスクライバ データベースの更新を 30 秒間試みます。30 秒が経過してもサブスクライバを更新できない場合、sepmdd サービスはその特定のサブスクライバの更新処理を省略し、リストに含まれている他のサブスクライバの更新を試みます。sepmdd は、サブスクライバ リストの 1 回目のスキャンが終了した後、2 回目のスキャンを実行します。2 回目のスキャンでは、1 回目のスキャンで更新できなかったサブスクライバの更新を試みます。2 回目のスキャンでは、接続システム コールがタイムアウトになるまで（約 90 秒間）サブスクライバの更新を試みます。

2 回目のスキャン時にもサブスクライバを更新できない場合、sepmdd は 30 分間隔で更新情報の送信を試みます。

更新情報は受信したときと同じ順序で送信する必要があるため、sepmdd はサブスクライバ データベースが使用可能になるまで、その後の更新情報を送信しません。

sepmdd がサブスクライバ データベースの更新に失敗するたびに、Policy Model のエラー ログに警告メッセージが書き込まれます。

フィルタ メカニズム

PMDB では、次のように特定のサブスクライバ端末を選択して更新することができます。サブスクライバ端末に送信するレコードを定義するには、次のレジストリ キーの文字列値をフィルタ ファイルに指定します。このように設定すると、フィルタ ファイルを通過したレコードのみが更新情報としてサブスクライバ端末に送信されます。

以下に例を示します。

```
HKEY_LOCAL_MACHINE¥Software¥ComputerAssociates¥AccessControl¥Pmd¥PolicyModelName¥
Filter
```

フィルタ ファイルは、各行に 6 つのフィールドを持つ複数の行で構成されます。フィールドには以下の情報が格納されます。

許可または禁止されるアクセスの種類

有効な値は、AUTHORIZE_DELETE、AUTHORIZE_MODIFY、CREATE、DELETE、DEPLOY、EDIT、FILESCAN、GET、SEOS_ACCS_READ、JOIN_DELETE、JOIN_MODIFY、MODIFY、READ、START、または UNDEPLOY です。

影響を受ける環境

有効な値は、AC、CONFIG、UNIX、NT、または NATIVE です。

レコードのクラス

有効な値は、ユーザ定義クラスを含む CA Access Control のすべてのクラスです。

ルールが適用されるクラスのオブジェクト

たとえば、User1、AuditGroup、または COM2 になります。

レコードによって許可または取り消されるプロパティ

たとえば、ユーザ レコードのフィルタ行の GROUPS および FULLNAME は、これらのユーザ プロパティを持つコマンドはすべてフィルタ処理されることを意味します。各プロパティを正確に入力する必要があります。

該当するレコードをサブスクライバ端末に転送するかどうか

有効な値は、PASS、NOPASS です。

注: どのフィールドでも、アスタリスクを使用して「可能なすべての値」を指定することができます。同じレコードが複数の行に該当する場合は、最初の該当する行が使用されます。

フィルタ ファイルの各行では、フィールドをスペースで区切ります。フィールドに複数の値がある場合は、値をセミコロンで区切ります。「#」で始まる行はコメント行とみなされます。空白行は使用できません。フィルタ ファイルの行の例を次に示します。

CREATE	AC	USER	*	FULLNAME;OBJ_TYPE	NOPASS
アクセスの形式	環境	クラス	レコード名（* = すべての名前）	properties	処理方法

たとえば、上のような行を持つ Printer1_Filter.flt というファイルがあり、レジストリ キー HKEY_LOCAL_MACHINE¥Software¥ComputerAssociates¥AccessControl¥Pmd¥PM-¥Filter に C:¥Program Files¥CA¥AccessControl¥¥data¥Printer1_Filter.flt という行が含まれる場合、Policy Model PM-1 は FULLNAME および OBJ_TYPE（管理者、監査担当者など）を持つ新しいユーザを作成するレコードを送信しません。アスタリスクは「すべての名前」を意味します。

各アクセス値に関連する selang のコマンドを次に示します。

アクセス	selang のコマンド
AUTHORIZE_DELETE	authorize-
AUTHORIZE_MODIFY	authorize
CREATE	newres、newusr、newgrp、newfile
DELETE	rmres, rmusr, rmgrp, rmfile, join- (UNIX)
DEPLOY	deploy
EDIT	editres、editusr、editgrp、editfile
FILESCAN	search
GET	get devcalc
JOIN_DELETE	join-
JOIN_MODIFY	join
MODIFY	chres、chusr、chgrp、chfile、join（UNIX）
READ	list
START	start devcalc

アクセス	selang のコマンド
UNDEPLOY	deploy- (undeploy)

注: CA Access Control はルールを検証しません。したがって、ルールに無効な値を入力すると、そのルールは更新トランザクションと一致しなくなります。

レジストリ サブキー

各 PMDB では、以下の独自のレジストリ サブキーが使用されます。

```
HKEY_LOCAL_MACHINE¥Software¥ComputerAssociates¥AccessControl¥Pmd
```

このサブキーには、PMDB のアクティビティを定義および決定する値が含まれています。サブキーが存在しない場合は、sepmdd ユーティリティによって必要最低限のエントリを持つサブキーが作成されます。

Notes

- selang を使用して(hosts pmd@hostname で)ターゲットとして Policy Model を選択した場合、sepmdd に対するクエリは PMDB に適用されますが、さまざまなサブスクライバ データベースには適用されません。
- PMDB がそれ自体のサブスクライバではないことを確認します。PMDB がそれ自体にサブスクライブされた場合、Policy Model が遮断されるか、ネットワークの負荷が大きくなり、ディスク領域が消費されます。
- UNIX 環境で selang を使用して Policy Model を更新する場合、newusr コマンドに複数のユーザを指定できません。
- UNIX 環境で selang を使用して Policy Model を更新する場合、newgrp コマンドに複数のグループを指定できません。
- selang から UNIX ファイル属性を更新すると、Policy Model はコマンドがサブスクライバに送信されたことを示すメッセージを生成します。
- Policy Model を操作する場合、Windows ファイル属性のステータスのクエリは実行できません。
- sepmdd サービスは、-k オプションを使用して非アクティブ化されるまで、無限にアクティブな状態を維持します。

詳細情報:

seagent デーモン (P. 314)
sepmd ユーティリティ (P. 222)
sepmdadm ユーティリティ - PMDB 定義の作成 (P. 236)

seagent デーモン

UNIX で該当

seagent デーモンは、リモート端末から要求を受け取り、その要求をローカルの CA Access Control データベースおよび UNIX データベース、または PMDB に適用します。また、Watchdog デーモン(seoswd)が実行中であることを確認し、実行されていない場合は再開します。

注: CA Access Control をロードすると(seload)、seagent も開始されます。このデーモンは独立して機能せず、seagent コマンドを使用して開始できません。

seagent デーモンは、seoslang および seoslang2 という TCP サービス(デフォルト値はそれぞれ 8890 と 8891)に対する接続を待機します。接続要求を受け取ると、seagent は子プロセスを作成し、接続から発生する通信を処理します。その後、引き続き新規の接続を待機します。

seagent の子プロセスは、クライアントから要求を受け取り、その要求をローカルデータベースに適用します。

Agent には、以下の役割もあります。

- UNIX ユーザ ファイル /etc/passwd、システムの shadow パスワード ファイル、および UNIX グループ ファイル /etc/group を更新します。
- 更新内容の送信時に、Policy Model デーモンに警告します。
- (それまで停止していた)サブスクライバ端末が更新可能になると、ローカルホストとコンピュータ上の Policy Model の両方の親 Policy Model に警告します。

CA Access Control では、8890 と 8891 のポートのみが使用されます。これらのポートは変更しないようお勧めします。

seagent Agent は RPC メカニズムを使用します。そのため、ローカル コンピュータ上で portmapper が実行されている必要があります。portmapper の詳細については、ご使用のシステムのマニュアルを参照してください。

このコマンドの形式は以下のようになります。

```
seagent
```

詳細情報:

seoswd デーモン (P. 322)
sepmdd デーモン（UNIX） (P. 303)

seauxd デーモン

UNIX で該当

seauxd デーモンは CA Access Control 補助デーモンで、Unicenter カレンダの設定を管理します。

seauxd をアクティブにするために、TNG_calendars 環境設定を Yes に設定します。

seauxd デーモンは、初期設定に従って、seosd デーモンによって起動されます。seauxd デーモンは以下の機能を実行します。

- seosd からの分析要求
- Unicenter TNG カレンダーの取得。この機能を有効にするには、seos.ini ファイルの [seauxd] セクションにある TNG_calendars トークンを「yes」に設定します。この機能が有効な場合、seosd は Unicenter TNG カレンダーのリストを seauxd に送信します。seauxd デーモンは、Unicenter TNG を呼び出し、各カレンダーのステータスを更新して、更新されたカレンダーのリストを seosd に返します。

seos.ini の [seauxd] セクションには、seauxd デーモンを調整できる多くのトークンがあります。

seosd デーモン

UNIX で該当

CA Access Control 認証デーモンです。seosd は、実行可能ファイルであり、CA Access Control の主要なデーモンです。デーモンは、制御 TTY および親プロセスの両方から切り離されたプロセスです。CA Access Control デーモンは、リソースへのアクセスを許可または拒否するために必要な実行時の決定を行います。

seosd を起動できるのは root ユーザのみであり、seosd を停止できるのは ADMIN 属性または OPERATOR 属性を持つユーザのみです。

CA Access Control デーモンは、データベースを開き、読み込みおよび更新を行います。CA Access Control デーモンの実行中は、その他のプロセスがこのデータベースにアクセスすることはできません。 また、CA Access Control デーモンは、CA Access Control の監査ファイルやトレース ファイルなどの重要なファイル、および必要に応じて CA Access Control バイナリ ファイルに対する書き込み、削除、または名前変更のアクセスをブロックします。

以下の条件の一方または両方を満たす場合にのみ、seosd 実行可能ファイルはデーモンになります。

- トレース メッセージが画面に送信されない場合。つまり、seos.ini ファイルの trace_to トークンが「*file*」、「*file,stop*」、または「*none*」に設定されている場合。
- ユーティリティを起動する際に、コマンド ラインで-d 以外の引数を指定しない場合

これらの条件のいずれにも当てはまらない場合、seosd は通常のプロセスのまま起動した端末に接続されます。

起動時には、seosd は以下のプロセスも起動します。

- seagent（CA Access Control のエージェント デーモン）
- seoswd（CA Access Control の Watchdog デーモン）

これらの CA Access Control デーモンが実行されると、デーモンの初期化が完了します。初期化後、これら 3 つのデーモンが維持する一種のハンドシェイク プロトコルによって、3 つのデーモンすべてがアクティブかつ応答していることが保証されます。これらのデーモンのいずれかが停止していることが検出されると、他の 2 つのデーモンのいずれか一方が、停止しているデーモンを自動的に再起動します。

このコマンドの形式は以下のようになります。

```
seosd [-d|argument]
```

注: 引数を指定せずに seosd を入力すると、seosd はデーモンとして実行されます。

argument

無視されます。ただし、引数を指定した場合、seosd は通常のプロセスとして続行されます。

-d

seosd はデーモンとして実行され、強制的に trace_file にトレースされます。

selogrcd デーモン - 監査レコードの収集

UNIX で該当

CA Access Control ログ ルーティング システムの収集デーモンです。

注: selogrcd は、IPv6 のみの環境では機能しません。

CA Access Control ログ ルーティング デーモン(selogrd および selogrcd)を使用すると、システム管理者は、目的の監査ログ レコードを簡単に選択できます。

selogrcd ユーティリティは、収集デーモンです。このデーモンは、さまざまサテライト システムから送信された選択済みの監査ログ レコードを収集し、監査データ収集ファイルに格納します。デフォルトのファイルは、*ACInstallDir*/log/seos.collect.audit です。

2 つのトークンによって、監査データ収集ファイルの管理機能が拡張されています。これらのトークンは、両方とも seos.ini ファイルの [selogrd] セクションにあります。

- Caudit_size トークンを使用して、監査データ収集ファイルの最大サイズを指定します。ファイルがこのサイズに達すると、バックアップ ファイルが作成され、新しいファイルが開きます。
- CbackUp_Date トークンを使用して、監査データ収集ファイルの自動バックアップ間隔およびタイムスタンプを指定します。

selogrcd に USR1 シグナルを送信して、新しい監査ファイルを作成するように指定できます。selogrcd プロセス ID の取得後、以下のように kill コマンドを使用して、USR1 シグナルを selogrcd に送信します。

```
kill -USR1 processID
```

selogrcd は USR1 シグナルを受信した後、既存の監査ファイル名を *ACInstallDir*/log/seos.collect.bak に変更し、新しい監査ファイルを作成します。また、cron ジョブを使用して、このタスクを定期的に実行することもできます。このタスクを実行するサンプル スクリプトは、*ACInstallDir*/samples/selogrcd ディレクトリにあります。

注: selogrcd デーモンの機能を拡張するには、CA Access Control に用意されている API を使用するプログラムを作成します。詳細については、「SDK 開発者ガイド」を参照してください。

このコマンドの形式は以下のようになります。

```
selogrcd [-d] [-l lock-file-name]
```

-d

デバッグ モードを指定します。このモードの場合、selogrcd はデーモンとして実行されません。selogrcd はデバッグ情報を端末に送信します。

-h

このユーティリティのヘルプ画面を表示します。

-l *lock-file-name*

使用するロック ファイルの名前(*lock-file-name*) デフォルトでは、*ACInstallDir*/lock/selogrcd ファイルが使用されます。

注: selogrd が別のログ ファイル(PMDB ログ ファイルなど)で機能するように設定した場合、ロック ファイルには、selogrd コマンド (P. 319)のパラメータとして使用されていた PMDB 名またはデータ ファイル名に基づいて拡張子が付けられます。

selogrd デーモン - 監査レコードの送出

UNIX で該当

CA Access Control ログ ルーティング システムの送出デーモンです。

注: selogrd は、IPv6 のみの環境では機能しません。

CA Access Control ログ ルーティング デーモン(selogrd および selogrcd)を使用すると、システム管理者は、目的の監査ログ レコードを簡単に選択できます。

selogrd ユーティリティは、送出デーモンです。このデーモンは、選択されたローカル監査ログ レコードをさまざまな送信先ホストに配布します。さらに、監査ログ レコードを電子メール メッセージ、ASCII ファイル、またはユーザ ウィンドウの形式に再フォーマットし、監査済みイベントに基づいて通知メッセージを送信します。

注: ログ ルーティング デーモンで CA Access Control イベントに関する重要な情報を収集するには、CA Access Control デーモンが稼動中である必要があります。CA Access Control デーモンが稼動していない場合は、古い監査レコードのみが転送されます。

ログ ルーティング デーモンは、環境設定ファイルを使用して、各監査ログ レコードの送信先、ログ レコードの書式、および転送するレコードを決定します。デフォルトでは、監査ログ ルーティング設定ファイル *ACInstallDir*/log/selogrd.cfg が使用されます。selogrd と selogrcd で使用する環境設定ファイルおよびその他のグローバル環境変数の名前は、CA Access Control 初期設定ファイル(seos.ini)に指定します。

selogrd デーモンは定期的に再起動し、環境設定ファイルを読み込みます。指定された時間に selogrd デーモンを再起動するように指定することもできます。これを行うには、以下のように指定して HUP シグナルを送信する必要があります。

```
kill -HUP processID
```

ProcessID

selogrd のプロセス ID を定義します (UNIX の ps コマンドを使用して、プロセス ID を確認します。詳細については、ご使用の UNIX システムのマニュアルを参照してください)。

selogrd ユーティリティは、CA Access Control で作業するプログラマに API アクセスを提供します。Logroute API を使用すると、プログラマは独自のオプションを CA Access Control 監査ログ システムに組み込み、現在のログ ルーティング機能では提供されていない社内用の警告を設定できます。また、ログ ルーティング デーモンを使用して、独自のプログラムに機能を追加することもできます。CA Access Control のすべての API の詳細については、「SDK 開発者ガイド」を参照してください。

このコマンドの形式は以下のようになります。

```
selogrd [-audit fileName] [-config fileName] [-d] ¥
    [-data fileName] [-pmdb policy-model-name]
```

-audit *fileName*

入力監査用ファイルとして、seos.ini に指定されているファイルの代わりに、使用する監査ファイルを定義します。

-config *fileName*

環境設定用ファイルとして、seos.ini に指定されているファイルの代わりに、使用する環境設定ファイルを定義します。

-d

デバッグ メッセージを印刷するように指定します。

-data *fileName*

ルーティング進行状況の情報を保存するために、seos.ini に指定されているファイルの代わりに、使用するデータ ファイルを定義します。

-h

このユーティリティのヘルプ画面を表示します。

-pmdb *policy-model-name*

PMDB からの監査データの転送先を selogrd に指示します。コマンドで指定した PMDB から、PMDB の pmd.ini ファイルの audit_log トークンに指定した監査ファイルに監査データを送るように、selogrd に指示します。

デフォルトでは、Policy Model 名で構成されるデータ ファイルおよびロック ファイルが使用されます。コマンド ラインでデータ ファイルまたはロック ファイル、あるいはその両方を指定すると、それらのファイルがデフォルト値よりも優先されます。ロック ファイル名およびデータ ファイル名には、端末の監査データを転送する selogrd のファイル名とは異なる名前を指定する必要があります。selogrd は、12 文字の Policy Model 名のみをサポートできます。

PMDB から送信される監査データは、名前が policy-model-name@station-name の端末から取得したデータであるかのように、収集された監査ファイルに表示されます。

詳細情報:

監査ログ ルーティング環境設定ファイル selogrd.cfg (P. 478)

seostngd デーモン

UNIX で該当

Unicenter TNG 用の CA Access Control 同期デーモンです。

Unicenter Security と CA Access Control は共に、全体的な移行が行われる前に、各企業の IT 環境を管理します。さまざまな製品ツールを使用して管理作業を行う複雑さを軽減するために、同期デーモンを提供しています。

このデーモンは seostngd と呼ばれます。CA Access Control は、CA Common Communication Interface（CAICCI）を使用して、Policy Model データベース（PMDB）の更新情報を seostngd に送信します。seostngd デーモンは CAICCI で更新情報を待機し、その後、このグローバル データで Unicenter Security データベースを更新するために、メッセージを等価な cautil コマンドに変換します。

現在の Unicenter TNG 処理は、引き続きその他の Unicenter TNG クライアント インストールを更新できます。Unicenter Security データベースのあるコンピュータと同じコンピュータ（通常は Unicenter マスタ コンピュータと呼ばれます）で seostngd を実行する必要があります。また、CA Access Control も同じコンピュータで実行する必要があります。

このコマンドの形式は以下のようになります。

```
seostngd

seostngd {-stop|-shut}
```

seoswd デーモン

UNIX で該当

CA Access Control の Watchdog デーモンです。

Watchdog（seoswd）は、データベースに Trusted プログラムとして定義されているプログラムのファイル情報およびデジタル署名を監視します。監視はバックグラウンドで実行されるので、システムの負荷は最小限に保たれます。CA Access Control のエージェント デーモン（seagent）は、seoswd を自動的に起動します。

seoswd デーモンは以下の機能を実行します。

- データベースの PROGRAM クラスに定義されたプログラムを監視します。Watchdog は、プログラムが変更されたことを検出すると、CA Access Control のデーモン（seosd）に通知します。seosd は、変更されたプログラムを Untrusted としてマークします。seosd デーモンは、Untrusted プログラムの実行を許可しません。また、データベースでプログラムのステータスを Untrusted に変更し、監査レコードを作成します。
- 保護対象ファイルとして定義されているファイルを監視します。これらのファイルは、データベースの SECFILE クラスに定義されます。
- seosd が実行中であることを監視します。Watchdog は、seosd で問題を検出すると、自動的に seosd を再起動します。
- seoswd デーモンは、seosd が応答を停止したことを検出すると、システム ログ syslogd を使用して、セキュリティ管理者に通知します。すべてのシステム ログ メッセージは AUTH 機能として送信されます。システム ログ機能の詳細については、man ページの syslogd および syslog.conf のセクションを参照してください。

- CA Access Control に各種イベントをレポートし、変更が確認されたプログラムおよび保護対象ファイルの監査レコードを作成します。
- Trusted プログラムと保護対象ファイルの期間および固定スキャン スケジュールを指定できます。
- Watchdog は、SIGHUP 以外のすべてのシグナルを無視します。seosd を停止する前に、seoswd デーモンを強制終了(kill)することはできません。ただし、kill -SIGHUP *pid* コマンドを実行した場合は、Watchdog がデータベース内のすべての trusted プログラムおよび保護対象ファイルをスキャンします。

Watchdog スキャン メカニズムの設定には以下の 2 つの方法があります。

1. 開始時刻を決定してから、所定の間隔でスキャンを繰り返します。

   たとえば、Trusted プログラムをチェックするときには、Watchdog は *PgmTestStartTime* に最初のスキャンを開始し、Trusted プログラムをすべてチェックします。前回のスキャンが開始されてから *PgmTestInterval* 秒後に、再スキャンが実行されます。
2. 指定した時刻にスキャンします。

注: どちらの場合でも、Watchdog は、各スキャン中に、事前設定されたリセット期間にわたって(*PgmRest* 秒間)、定期的にスリープ状態になります。Watchdog は、システムの過負荷を防止するために休止します。

1 つのメカニズムを使用することも、同時に両方のメカニズムを使用することもできます。たとえば、12:00 に開始して 4 時間ごとにスキャンし、さらに 13:00 と 17:30 にスキャンすることもできます。

Trusted プログラムと保護対象ファイルのルーチン スキャンの上記のメカニズム以外に、HUP シグナルを送信して 1 回のみのオンデマンドのスキャンを実行する方法があります(トークン SignalMinInterval を参照)。

引数を指定せずに seoswd を起動すると、seoswd はデーモンとして実行されます。-d 引数を指定して seoswd を呼び出すと、デーモンとして実行されます。ただし、このユーティリティを起動した端末のデバッグ情報はすべて表示されます。

詳細情報:

seuidpgm ユーティリティ - trusted プログラムの抽出 (P. 260)

第 3 章: 設定ファイル

このセクションには、以下のトピックが含まれています。

accommon.ini ファイル

accommon.ini 環境設定ファイルには、レポート エージェントの初期化処理を制御するトークンおよび、一般的な通信設定を制御するトークン（例えば、CA Access Control エンタープライズ管理 を使用した UNIX 認証ブローカ 登録設定）が含まれます。accommon.ini ファイルは以下のセクションに分かれています。

セクション	説明
communication	一般的な通信設定を制御するトークンを含んでいます。
global	CA Access Control グローバル設定を含んでいます。
ReportAgent	レポート エージェント設定を制御するトークンを含んでいます。
AccountManager	アカウント マネージャ設定を制御するトークンを含んでいます。

通信

[communication]セクションでは、トークンは通信と暗号化オプションを制御します。

Distribution_Server

配布サーバの URL を定義します。カンマ区切りリストに複数の配布サーバを定義できます。

例: tcp://ds.comp.com:7222, tcp://ds_dr.comp.com:7222

デフォルト: none

endpoint_to_server_queue

エンドポイントが CA Access Control エンタープライズ管理 への情報の送信に使用するメッセージ キューの名前を定義します。

デフォルト: ac_endpoint_to_server

server_to_endpoint_broadcast_queue

CA Access Control エンタープライズ管理 がすべてのエンドポイントへメッセージをブロードキャストするために使用するメッセージ キューの名前を定義します。

デフォルト: ac_server_to_endpoint_broadcast

server_to_endpoint_queue

CA Access Control エンタープライズ管理 がエンドポイントへのメッセージの送信に使用するメッセージ キューの名前を定義します。

デフォルト: ac_server_to_endpoint

ServerVersion

前方互換性用の配布サーバ バージョンを定義します。

例: 12.01.0648

デフォルト: none

ssl_custom

ホスト名の検証機能を使用するかどうかを指定します。

制限: 0 - ホスト名の検証機能を使用しない、1 - ホスト名の検証機能を使用する。

デフォルト: 0

ssl_hostname

SSL のホスト名を定義します。

デフォルト: none

ssl_identity

レポート エージェントの ID を定義します。

制限: 証明書データが含まれているファイルへの完全パス名。

デフォルト: none

ssl_issuer

SSL 接続に対する発行元の証明書を定義します。

制限: 証明書データが含まれているファイルへの完全パス名。

デフォルト: none

ssl_key

レポート エージェントの秘密鍵を定義します。

制限: 証明書データが含まれているファイルへの完全パス名。

デフォルト: none

ssl_noverifyhost

ホスト証明書の検証を有効にするかどうかを指定します。

制限: 0 - ホスト証明書の検証を無効にする、1 - ホスト証明書の検証を有効にする。

デフォルト: 0

ssl_noverifyhostname

ホスト名の検証を有効にするかどうかを指定します。

制限: 0 - ホスト名の検証を無効にする、1 - ホスト名の検証を有効にする。

デフォルト: 0

ssl_trace

SSL トレースを有効にするかどうかを指定します。

制限: 0 - SSL トレースを無効にする、1 - SSL トレースを有効にする。

デフォルト: 0

ssl_trusted

SSL 接続に対して信頼されている証明書を定義します。

制限: 証明書データが含まれているファイルへの完全パス名。

デフォルト: none

global

[global] セクションのトークンは、CA Access Control エンドポイントの動作を制御します。

accommon_path

accommon ディレクトリのフル パス名を指定します。

デフォルト: /opt/CA/AccessControlShared/

AC_Version

エンドポイントにインストールされた CA Access Control のバージョンを定義します。

デフォルト: none

java_home

（Linux s390）Java ライブラリへのパスを定義します。

例: Linux390 コンピュータにインストールされた IBM J2SE バージョン 5.0 JRE の場合: /opt/ibm/java2-s390-50/jre

デフォルト: none

ReportAgent

[ReportAgent] セクションのトークンは、レポート エージェント デーモン（ReportAgent）の動作を制御します。

audit_enabled

エンドポイント監査データを配布サーバに送信するかどうかを指定します。

値: 0 - いいえ、**1** - はい

デフォルト: 0

audit_filter

レポート エージェントが外部ソース(CA Enterprise Log Manager など)に経路指定する監査レコードのフィルタリング ルールが含まれているファイルへのフル パス名を定義します。このファイルは、レポート エージェントが経路指定するレコードを特定します。

デフォルト: *ACSharedDir*/etc/auditrouteflt.cfg

audit_queue

レポート エージェントがエンドポイント監査データを送信するキューの名前を定義します。

デフォルト: キュー/監査

audit_read_chunk

レポート エージェントが監査ファイルの単一の読み取りで収集を試みる最大監査レコードを定義します。

制限: 正の整数を入力します。

デフォルト: 300

audit_send_chunk

レポート エージェントが各接続で配布サーバに送信する監査レコードの最大数を定義します。レポート エージェントは、収集する監査レコードがこの数に達すると、それらを配布サーバに送信します。

制限: 正の整数を入力します。

デフォルト: 1800

audit_sleep

レポート エージェントが監査レポートを生成する間のスリープする時間の長さを定義します。

制限: 秒数を表す正の整数。

デフォルト: 10

audit_timeout

レポート エージェントがエンドポイント監査データを配布サーバに送信する周期を定義します。最後の送信からこの時間が経過すると、収集したレコード数が audit_send_chunk 値よりも少ない場合であっても、レポート エージェントは監査データを配布サーバに送信します。

制限: 秒数を表す正の整数。

デフォルト: 300

Debug

Report Agent でデバッグ情報をログとして記録するかどうかを指定します。

はい(1)に指定すると、Report Agent では以下をログとして記録します。

- *ACSharedDir*/log/ac2xml.log への CA Access Control レポート
- UNIX 認証ブローカ による *ACSharedDir*/log/unab2xml.log へのレポート(uxauthd)
- CA Enterprise Log Manager へ、そこから *ACSharedDir*/log/ac2elm.log に送信される CA Access Control 監査レポート
- CA Enterprise Log Manager へ、そこから *ACSharedDir*/log/unab2elm.log に送信される UNIX 認証ブローカ 監査レポート
- CA Enterprise Log Manager へ、そこから *ACSharedDir*/log/kbl2elm.log に送信される Keyboard Logger レポート

制限: 0 を指定すると、Report Agent はデバッグ情報をログとして記録しません。1 を指定すると、Report Agent はデバッグ情報をログとして記録します。

デフォルト: 0

elm_event_interval

レポート エージェントがユーザ セッション監査イベントを CA Enterprise Log Manager に送信する間隔を秒単位で定義します。

制限:「0」は間隔なしです。メッセージ サイズが elm_max_msg_size トークンに指定された値を超えると監査イベントを送信します。正の整数を入力します。

デフォルト: 60

elm_max_msg_size

レポート エージェントが CA Enterprise Log Manager に送信する Keyboard Logger メッセージの最大サイズをバイト数単位で指定します。

値: 正の整数を入力します

デフォルト: 300000

間隔

CA Access Control がレポートを作成して配布サーバに送信する間隔(秒)を定義します。

[*スケジュール*]設定では、間隔の開始時間および実行する曜日を定義します。レポート エージェントが予定されているオカレンスよりも遅く開始した場合は、スケジュールから計算した次の間隔でレポートを送信し、その後は予定された曜日の定義された間隔で送信します。

例: 「schedule=8:30@Mon,Tue,Wed」および「interval=5 」に設定されている場合は、レポート エージェントは火曜日の 8:47 am にロードして、レポートを 8:50 am に作成して送信します。これは、5 分間隔を使用して予定されている開始時刻から計算された最早の周期です。

値: **0** - 間隔なし(予定されているオカレンスのみを使用); *正の整数* - 間隔として使用する分数

デフォルト: 0

reportagent_enabled

ローカル コンピュータでレポートが有効(1)になっているかどうかを指定します。

デフォルト: 0

schedule

レポートを生成し、配布サーバに送信する日時を定義します。

この設定は、次の形式で指定します。time@day[,day2][...]

たとえば、「19:22@Sun,Mon」と指定すると、レポートは毎週土曜日と日曜日の 7:22 pm に生成されます。

デフォルト: 00:00@Sun,Mon,Tue,Wed,Thu,Fri,Sat

send_queue

レポート エージェントがローカル データベースおよび任意の PMDB のスナップショットを送信する配布サーバのレポート キューの名前を定義します。

デフォルト: queue/snapshots

詳細情報:

auditrouteflt.cfg ファイル - 監査レコード ルーティングのフィルタリング (P. 469)

AccountManager

[AccountManager] セクションのトークンは、AccountManager プラグインの動作を制御します。

OperationMode

AccountManager プラグインが有効か無効かを定義します。

オプション: 1 の場合は有効、0 の場合は無効

デフォルト: 1

PluginPath

AccuntManager プラグインの完全パス名を定義します。

デフォルト: /opt/CA/AccessControlShared/lib/AccountManager.so

ScheduleType

AccountManager プラグインのスケジュール タイプを定義します。

オプション:

- 0 -- 1 度だけ実行
- 1 -- オンデマンドで実行
- 2 -- N 秒ごとに実行
- 3 -- スケジュール文字列に基づいて実行:
  00:00@Sun.Mon,tue,Wed,Thu,Fri,Sat

デフォルト: 2

Interval

AccountManager プラグインの間隔を秒数で指定します

デフォルト: 300

注: ScheduleType 制御値を 2 に設定した場合に適用可能です。

スケジュール

AccountManager プラグインのスケジュール文字列を指定します。

デフォルト: 00:00@Sun,Mon,Tue,Wed,Thu,Fri,Sat

注: ScheduleType 制御値を 3 に設定した場合に適用可能です。

QueryFilter

メッセージ キューの受信キュー フィルタに追加するカスタム値を指定します。

オプション:

- "ENDPOINT_CUSTOM1="
- "ENDPOINT_CUSTOM2="
- "ENDPOINT_CUSTOM3="
- "ENDPOINT_CUSTOM4="
- "ENDPOINT_CUSTOM5="
- "ENDPOINT_OWNER="
- ENDPOINT_DEPARTMENT="

デフォルト: 値なし

注: AND オペランドを使用して複数のカスタム プロパティを使用することができます。

例: "ENDPOINT_DEPARTMENT='Finance' AND 'ENDPOINT_CUSTOM1=Accounting'"

重要: カスタム プロパティを指定する場合は以下を必ず確認してください。

- プロパティ値を指定するためにアポストロフィを使用している
- 複数のプロパティを指定するときは AND、OR オペランドを使用している
- OR オペランドを使用するときは丸かっこを使用している

kblaudit.cfg -- キー ロガー監査レコードのフィルタ

UNIX で該当

kblaudit.cfg ファイルは、監査ファイルに送信されるレコードを定義することによって、ホストの監査レコードをフィルタリングします。各行は、監査情報を除外するためのルールを表します。設定するフィルタ ルールは kbl.audit ファイルに適用されます。

デフォルトでは、kblaudit.cfg ファイルは以下のディレクトリにあります。

```
/opt/CA/AccessControl/etc
```

kblaudit.cfg ファイルには、キー ロガー監査レコードをフィルタするのに役立つ 2 つのセクション［EXCLUDE］および［INCLUDE］が含まれています。各セクションには、フィルタ ルールを表すエントリが含まれます。

例: kblaudit.cfg フィルタ セクション

kblaudit.cfg ファイルの以下のコードの一部は、kblaudit.cfg の［EXCLUDE］および［INCLUDE］セクションを編集する方法の例を示しています。

```
[EXCLUDE]
TRACE;*;*;test_user; test_user; test_user;*;*seos.ini*
[INCLUDE]
TRACE;*;*; test_user; test_user; test_user;*;*AccessControl*
```

この例では、kbl.audit ファイルで、ユーザ test_user が実行した seos.ini からの監査レコードを除外し、ユーザ test_user が Access Control で実行したレコードを含めるようにします。

kblaudit.cfg ファイルを使用して以下の監査イベント タイプのレコードをフィルタで除外します。各タイプに異なる構文が使用されます。

- ログイン イベント (P. 335)
- ユーザのトレース メッセージ (P. 335)

注: 各タイプの構文の列に * がある場合には、「何らかの値」を意味します。

Kblaudit.cfg -- ログイン イベント フィルタ構文

UNIX で該当

ログイン イベントに属する監査レコードのフィルタ形式は、以下のとおりです。

LOGIN;*UserName*;*UserId*;*TerminalName*;*LoginProgram*

Login

ユーザ トレース レコードをルールがフィルタリングするように指定します。

UserName

アクセサの名前を定義します。

UserId

アクセサのネイティブ ユーザ ID を定義します。

TerminalName

イベントが発生したリモート ホスト名を定義します。

LoginProgram

ログインまたはログアウトを試みたプログラムの名前を定義します。

制限: cmdlog

kblaudit.cfg —— ユーザ イベント フィルタ構文のトレース メッセージ

UNIX で該当

ユーザのトレース メッセージ イベントに属する監査レコードのフィルタ形式は、以下のとおりです。

TRACE;*TracedClassName*;*TracedObjectName*;*RealUserName*;*ACUserName*;*AuthorizationResult*;*TraceMessageMask*;*KBLSessionID*

TRACE

ユーザ トレース レコードをルールがフィルタリングするように指定します。

TracedClassName

ユーザがアクセスしようとしたオブジェクト クラスの名前を定義します。

オプション: KBL raw, KBL output, KBL input, KBL execargs

TracedObjectName

ユーザがアクセスしようとしたオブジェクトの名前を定義します。

RealUserName

トレース レコードを生成したログイン ユーザの名前を定義します。

ACUserName

トレース レコードを生成した有効なユーザの名前を定義します。

AuthorizationResult

認証結果を定義します。

値: P (許可されました)、D (拒否されました)、*

TraceMessageMask

生成されたトレース メッセージを定義します。

KBLSessionID

キー ロガー セッション ID を表示します

seos.ini 初期設定ファイル

UNIX で有効

seos.ini ファイルには、CA Access Control で使用されるさまざまな設定と初期設定のためのトークンが記録されます。1 行に 1 つのトークンを以下の形式で指定します。

token = *value*

CA Access Control の特定のユーティリティ、デーモン、またはその他の機能に関するトークンを含む行が、セクション単位でまとめられています。各セクションはヘッダ行で始まります。ヘッダ行にはセクションの名前が角かっこ [ ] 内に示されます。各トークンは 1 つのセクションに属しています。たとえば、以下の行は serevu ユーティリティを管理するセクションの先頭行です。

```
[serevu]
```

seos.ini ファイルは、インストール時の初期状態では CA Access Control によって保護されていて、CA Access Control の実行中は更新できません。seos.ini ファイルには、CA Access Control のデフォルト設定で書き込みアクセス権が設定されます。これは、実行中の多数のユーティリティが seos.ini ファイルにアクセスするためです。seos.ini ファイルを読み込めない場合、ユーティリティの実行は失敗します。

CA Access Control が実行中であっても権限のあるユーザが seos.ini ファイルを更新できるようにするために、以下の selang コマンドを入力します。

```
newres FILE /opt/CA/AccessControl//seos.ini owner(authUser)
```

authUser は、権限を持つユーザの名前です。このコマンドは、*authUser* をこのファイルの所有者として設定します。つまり、*authUser* はいつでもこのファイルを更新できるようになります。

CA Access Control エンドポイント管理 または seini ユーティリティを使用すると、初期設定ファイルでトークンの読み込み、追加、変更、および削除を行うことができます。

注: : seosd が実行中でない場合、またはデータベースのルールによって明示的に許可されている場合にのみ、seini ユーティリティで seos.ini ファイルを更新できます。

secons -rl コマンドを使用すると、seosd デーモンを再起動せずに、トークンの更新を反映した seos.ini ファイルを再ロードできます。

以下の表に、seos.ini ファイルのすべてのセクションを示します。

セクション	説明
AccountManager	複数の JCS エンドポイント モジュール
AgentManager	CA Access Control プラグイン管理
crypto	暗号化モジュール ライブラリの設定。
daemons	seload ユーティリティが自動実行される CA Access Control デーモンのリスト。
Dependency	ユーザが定義したとおりに、CA Access Control を埋め込みコンポーネントとして使用する製品のリスト。
devcalc	ポリシー偏差計算機能（devcalc）の設定。
kblaudit	キーロガーのセッション トラッキングの設定。
lang	CA Access Control 管理インターフェース（selang）の設定。
ldap	LDAP サンプル EXIT 用 LDAP サーバの設定。
logmgr	ログ機能の設定。
message	メッセージ ファイルの設定。
mfsd	メインフレーム同期デーモン（mfsd）の設定。
OS_user	エンタープライズ ユーザ ストア使用法の設定。
package	CA Access Control のインストール済みパッケージのリスト。
pam_seos	Pluggable Authentication Module（PAM）プログラミング インターフェースの設定。
passwd	パスワードの変更およびユーザ関連サービスの設定。
pmd	Policy Model データベースの共通設定。
policyfetcher	ポリシー フェッチャ デーモン（policyfetcher）の設定。
PUPMAgent	特権ユーザ パスワード管理 デーモン（pupmagent）の設定。
seagent	seagent デーモンの設定。
seauxd	Unicenter カレンダ設定用の補助デーモン（seauxd）の設定。
segrace	ユーザのログイン情報ユーティリティ（segrace）の設定。
seini	環境設定ファイル管理ユーティリティ（seini）の属性。

セクション	説明
selock	デスクトップの非アクティブ性保護ユーティリティ(selock)の設定。
selogrd	ログ ルーティング デーモン(selogrd および selogrcd)の設定。
seos	グローバル環境設定。
SEOS_syscall	SEOS_syscall カーネル モジュールの設定。
seosd	認証デーモン(seosd)の設定。
seosdb	データベースのチェックおよび再構築の設定。
seoswd	Watchdog デーモン(seoswd)の設定。
serevu	失敗したログイン試行解決ユーティリティ(serevu)の設定。
sesu	CA Access Control のユーザ切り替えユーティリティ(sesu)の設定。
sesudo	CA Access Control のユーザ一時変更ユーティリティ(sesudo)の設定。
standalone	スタンドアロン コンピュータ管理の設定。
tcp_communication	共通の TCP 接続設定。
tng	CA Access Control と Unicenter との統合の設定。

AgentManager

[AgentManager]セクションのトークンは、CA Access Control プラグイン管理に関連する側面を制御します。

exclude_endpoint_types

アカウント マネージャが管理しないエンドポイント タイプのカンマ区切りリストを指定します。

Interval

プラグイン スケジュールを秒単位で定義します。

デフォルト: 1

注: ScheduleType が 2 に設定されている場合にのみ適用されます。

max_threads_count

プール内の最大作業スレッド数を指定します。

デフォルト: 10

OperationMode

プラグインの操作モードを定義します。

オプション: 0 - プラグイン無効、1 - プラグイン有効

デフォルト: 1

Plugins

CA Access Control エージェント マネージャが使用するプラグインを指定します。

デフォルト: AccountManager、Heartbeat、Policyfetcher

PluginPath

プラグインの完全パス名を定義します。

デフォルト: /opt/CA/AccessControlShared/lib/Heartbeat.so

RefreshTimeout

プラグインの更新タイムアウトを定義します。

デフォルト: 10

Schedule

プラグイン スケジューリング文字列を定義します。

デフォルト: 00:00@Sun.Mon,Tue,Wed,Thu,Fri,Sat

注: ScheduleType が 2 に設定されている場合にのみ適用されます。

ScheduleType

プラグイン スケジュール タイプを定義します。

オプション: 0 - 1 回実行、1 - オン デマンドで実行、2 - 指定間隔で実行、3 - スケジュールにしたがって実行

デフォルト: 1

TraceEnabled

CA Access Control エージェント マネージャトレース モードを定義します。

オプション: 0、1

デフォルト: 1

注: トレース メッセージのログは、次の場所に記録されます。
<WorkSpace>/AgentManager.log

WorkSpace

CA Access Control エージェント マネージャ ワークスペースの完全パス名を指定します。

デフォルト: /opt/CA/AccessControlShared/data/AgentManager

AccountManager

[AccountManager]セクションのトークンは、JCS 管理に関連する側面を制御します。

Interval

プラグイン スケジュールを秒単位で定義します。

デフォルト: 1

注: ScheduleType が 2 に設定されている場合にのみ適用されます。

OperationMode

プラグインの操作モードを定義します。

オプション: 0 - プラグイン無効、1 - プラグイン有効

デフォルト: 1

PluginPath

プラグインの完全パス名を定義します。

デフォルト: /opt/CA/AccessControlShared/lib/AccountManager.so

QueryFilter

メッセージ キューの受信キュー フィルタに追加される追加値を指定します。

オプション: ENDPOINT_CUSTOM 1...5=、ENDPOINT_OWNER=、ENDPOINT_DEPARTMENT=

以下の点に注意してください。

- プロパティ値はアポストロフィで囲みます。
- 複数のプロパティを指定する場合は、オペランド AND および OR を使用します。
- 必要に応じて丸かっこを使用します。

Schedule

プラグイン スケジューリング文字列を定義します。

デフォルト: 00:00@Sun.Mon,Tue,Wed,Thu,Fri,Sat

注: ScheduleType が 2 に設定されている場合にのみ適用されます。

ScheduleType

プラグイン スケジュール タイプを定義します。

オプション: 0 - 1 回実行、1 - オン デマンドで実行、2 - 指定間隔で実行、3 - スケジュールにしたがって実行

デフォルト: 1

crypto

[crypto] セクションのトークンは、暗号化モジュールに関連付けられている部分を制御します。

ca_certificate

認証局(CA)の証明書データベースへの完全パス名を定義します。

デフォルト: *ACInstallDir*/data/crypto/def_root.pem

communication_mode

Secure Socket Layer（SSL）のプロトコルを有効にするかどうかを指定します。

これを ssl_only に設定した場合は、SSL V2、SSL V3、TLS の各接続のみが有効になります。つまり、このコンピュータは、SSL をサポートしていないコンピュータと通信できないため、SSL をサポートしていない、r12.0 より前の各バージョンの Access Control を実行しているコンピュータと通信できません。

注：CA Access Control r12.0 以降が実行されているコンピュータでは、SSL がサポートされています。

fips_only トークンが 1 に設定されている場合は、FIPS モード（つまり TLS）では実際の通信モードは ssl_only に設定され、communication_mode トークンは無視されます。

有効な値は以下のとおりです。

- all_modes
- ssl_only
- non_ssl

デフォルト： non_ssl

CAPKIHOME

CAPKI のインストール ディレクトリを定義します。

デフォルト： /opt/CA/SharedComponents/CAPKI

encryption_methods

メッセージを復号化するために CA Access Control エージェントが使用する暗号化ライブラリを指定します。復号化が成功するまで、エージェントはリスト内の各ライブラリを順番に使用します。

制限： libaes256、libaes192、libaes128、libdes、libtripledes, libscramble

デフォルト： libaes256、libaes192、libaes128、libdes、libtripledes

fips_only

このトークンは、CA Access Control が FIPS 専用モードで機能するかどうかを制御します。このモードでは、FIPS 以外のすべての機能が無効になります。

有効な値は以下のとおりです。

1 CA Access Control は FIPS 専用モードで機能します。

0 CA Access Control は FIPS 以外のモードで機能します。

デフォルト： 0

LIBRARY_PATH

ETPKI 暗号化ライブラリのディレクトリを定義します。

private_key

所有者の秘密鍵への完全パス名を定義します。

デフォルト: *ACInstallDir*/data/crypto/sub.key

ssl_port

CA Access Control のクライアントとサービスの間の SSL 通信のポートを定義します。

デフォルト: 5249

subject_certificate

所有者の証明書への完全パス名を定義します。

デフォルト: *ACInstallDir*/data/crypto/sub.pem

daemons

[daemons] セクションの各トークンは、seload ユーティリティで、CA Access Control のインストール ディレクトリから特定のプログラムを実行するかどうかを（実行する場合は、実行方法も）指定します。各トークン名は、CA Access Control のデーモン名に対応しているか、またはプログラムのニックネームであり、複数の値を割り当てることができます。

program-name

以下のいずれかを指定します。

- 以下の値と一致するデーモンまたはその他のプログラムの名前。
  - *yes*。seload はデフォルトのパラメータを使用してプログラムを実行します。
  - *no*。seload はプログラムを実行しません。
  - 一連のパラメータ。seload はこのパラメータを使用してプログラムを実行します。

  たとえば、デフォルトのパラメータを使用して、CA Access Control のインストール ディレクトリから serevu を実行するには、以下のように入力します。

  ```
  serevu=yes
  ```

  serevu を実行しない場合は、以下のように入力します。この指定は、serevu トークンを使用しないことと同じです。

  ```
  serevu=no
  ```

  指定したパラメータを使用して、CA Access Control のインストール ディレクトリから serevu を実行するには、以下のように入力します。

  ```
  serevu=-f 3 -d 6m -t 1m -s 5m
  ```

- デーモンまたはその他のプログラムの絶対パス名と一致するダミー文字列。続けてオプションのパラメータを指定します。seload は指定に従ってプログラムを実行します。

  たとえば、指定したパラメータを使用して、/opt/CA/AccessControl//bin ディレクトリに存在する serevu ユーティリティを実行するには、以下のように入力します。

  ```
  run_it=/opt/CA/AccessControl//bin/serevu -f 3 -d 6m -t 1m
  ```

  複数のプログラムに対する指定を含めるには、プログラムごとにトークンを 1 回使用します。

デフォルト: no

注: seosd デーモンを指定する必要はありません。seload は、seosd デーモンが実行中であることを常に確認します。

Dependency

[Dependency] セクションの各ユーザ定義トークンは、CA Access Control を埋め込みコンポーネントとして使用する製品を指定します。

product-name

CA Access Control を埋め込みコンポーネントとして使用する製品を指定します。有効な値は以下のとおりです。

0 - 埋め込み製品ではありません。

1 - 埋め込み CA Access Control 製品です。

デフォルト: デフォルトの製品が指定されていません。

devcalc

[devcalc] セクションのトークンは、ポリシー偏差計算機能に関連付けられている部分を制御します。

dms_command_retry_interval

DMS 通知コマンドの試行間隔を秒数で定義します。

デフォルト: 60

init_ac_db

使用されなくなりました。

max_dms_command_retry

ポリシー偏差計算機能が DMS に更新通知の送信を再試行する最大回数を定義します。この回数を超えても送信されないと、再試行しなくなります。

デフォルト: 3

max_lines_request

get devcalc selang コマンドが任意の時点で(ポリシー偏差データ ファイルから)返す最大行数を定義します。以下のコマンドを使用して、追加行を取得する必要があります。

```
get devcalc params("offset=X")
```

X

前の *get devcalc* 出力で返された行オフセットを定義します。

デフォルト: 50

kblaudit

[kblaudit] セクション内のトークンは、キーロガーのセッション トラッキング プログラムの動作を制御します。

audit_back

キーロガーのバックアップ監査ログ ファイルの名前を指定します。

デフォルト: *ACInstallDir/log/kbl*.audit.bak

audit_group

監査ログに対する読み取り権限を持つグループを指定します。このトークンを **none** に設定すると、root のみに監査ログの読み取り権限が付与されます。CA Access Control はこのトークンの値の有効性を確認しないため、無効なグループ名を入力すると、監査ログ ファイルに対するアクセス許可はどのグループにも割り当てられません。

既存の監査ログ ファイルのグループ所有者権限を変更するには、以下の手順に従います。

selang の chgrp コマンドを使用して、ファイルのグループ所有者権限を設定します。

以下のコマンドを入力して UNIX のアクセス許可を変更します。

```
chmod 640 ACInstallDir/log/seos.audit
```

デフォルト: none

audit_log

キーロガーの監査ログ ファイルの名前を指定します。

デフォルト: *ACInstallDir*/log/kbl.audit

audit_max_files

バックアップ モードで保持する監査ログ ファイルの最大数を指定します。この数に達すると、最新のファイルが作成される時点で CA Access Control によって最も古いバックアップ ファイルが削除されます。

制限: 正の整数

デフォルト: 0

注: 0 に設定した場合、CA Access Control はバックアップ ファイルを累積し、古いファイルを削除しません。

audit_size

監査ログ ファイルの最大サイズ(KB 単位)を指定します。

最小値: 50KB。

デフォルト: 24000

注: 監査ファイルのサイズが 2GB を超えた場合、CA Access Control は、監査ファイルへの監査レコードの書き込みを停止します。

BackUp_Date

CA Access Control が監査ログ ファイルをバックアップする条件、および CA Access Control がタイムスタンプをバックアップ ファイル名に追加するかどうかを指定します。

audit_size 設定で指定されたサイズに達すると、CA Access Control は*常に*監査ログ ファイルをバックアップします。

値: none、yes、daily、weekly、monthly

- yes -- audit_size で指定されたサイズに達すると、CA Access Control は監査ログ ファイルをバックアップしし、タイム スタンプをバックアップ ファイル名に追加します。
- none -- audit_size で指定されたサイズに達すると、CA Access Control は監査ログ ファイルをバックアップしますが、タイム スタンプをバックアップ ファイル名に追加しません。

- daily、weekly、monthly -- 指定された時間間隔が経過し、かつ audit_size で指定されたサイズに達すると、CA Access Control は監査ログ ファイルをバックアップし、タイムスタンプをバックアップ ファイル名に追加します。ただし、指定された時間間隔内に監査イベントが監査ログ ファイルに書き込まれない場合、間隔が経過しても、CA Access Control はファイルをバックアップしません。

  注: CA Access Control は、最初の監査ログ ファイルを作成した時間から指定された間隔を数え、適切な日の午前零時にファイルをバックアップします。

例: 設定には週単位の値があり、CA Access Control は 4 月 1 日午前 9 時に監査ログ ファイルを作成します。多くの監査イベントが今週発生し、監査ログ ファイルは 4 月 4 日月曜日上に audit_size 設定で指定された値を超過します。CA Access Control は 4 月 4 日に監査ログ ファイルをバックアップし、タイム スタンプをバックアップ ファイル名に追加します。監査ログ ファイルが最初に作成された一週間後の 4 月 8 日金曜日の午前零時に、CA Access Control は再度監査ログ ファイルをバックアップし、タイムスタンプをバックアップ ファイル名に追加します。

デフォルト: none

cmd_log

キー ロガー cmdlog バイナリ ファイルへのリンクを指定します。

デフォルト: /etc/AC

error_back

キーロガーのエラー ログ バックアップ ファイルの名前を指定します。

デフォルト: *ACInstallDir*/log/kbl.error.bak

error_group

エラー ログ ファイルに対する読み取り権限を持つグループを指定します。このトークンを **none** に設定すると、root のみにエラー ログ ファイルの読み取り権限が付与されます。CA Access Control はこのトークンの値の有効性を確認しないため、無効なグループ名を入力すると、エラー ログ ファイルに対するアクセス許可はどのグループにも割り当てられません。

既存のエラー ログ ファイルのグループ所有者権限を変更するには、以下の手順に従います。

selang の chgrp コマンドを使用して、ファイルのグループ所有者権限を設定します。

以下のコマンドを入力して UNIX のアクセス許可を変更します。

```
chmod 640 ACInstallDir/log/seos.audit
```

デフォルト: none

error_log

キーロガーのエラー ログ ファイルの名前を指定します。

デフォルト: *ACInstallDir*/log/kbl.error

error_size

エラー ログ ファイルの最大サイズ(KB 単位)を指定します。

制限: 最小値は 50 KB です。

デフォルト: 500

kbl_enabled

キーロガーを有効にするかどうかを指定します。

値: yes、no

デフォルト: no

kbl_flush_timeout

印刷可能なログ データが kbl 監査ファイルに保存された後のユーザ セッション非アクティブ状態間隔を秒単位で指定します。このトークンを 0 に設定すると、無効になります。

デフォルト: 30

Kbl_seos_trace

seosd がセッション中のトレースをアクティブにし、ユーザ アクティビティ データをキー ロガーに送信するかどうかを指定します。

値: yes、no

デフォルト: yes

OS_etc_shells

オペレーティング システム シェル ファイルの名前を指定します。

デフォルト: /etc/shells

socket_name

キーロガーの監査マネージャのソケット名を指定します。

デフォルト: *ACInstallDir*/kblserver

lang

[lang] セクションのトークンは、selang のコマンド プログラムである selang、Security Administrator、および seadm によって使用される属性を指定します。

check_password

selang がユーザにユーザ自身のパスワードの入力を要求するかどうかを指定します。有効な値は以下のとおりです。

no - selang はパスワードを要求しません。

yes - ユーザは自分のパスワードを入力するように要求されます。

デフォルト: no

exit_timeout

CA Access Control で exit プログラムを実行できる最長時間（秒単位）を指定します。この時間が経過すると、exit プログラムは CA Access Control によって強制終了されます。

デフォルト: 30

exits_dir

ACInstallDir/lbin/install_exits.sh シェル スクリプトによってインストールされる exit プログラムのターゲット ディレクトリを指定します。

デフォルト: *ACInstallDir*/exits

exits_source_dir

ACInstallDir/install_exits.sh シェル スクリプトによってインストールされる exit プログラムのソース ディレクトリを指定します。

デフォルト: *ACInstallDir*/samples/exits-src

help_path

lang ヘルプ ファイルがインストールされているディレクトリを指定します。

デフォルト: *ACInstallDir*/data/langhelp

language

CA Access Control のインストール言語を定義します(内部用)。

デフォルト: english

max_groups_buffsize

セキュリティ管理者がデータベースとの通信に使用するバッファのサイズ(KB 単位)を指定します。このトークンは、UNIX の更新を適用する必要があるときに使用されます。

デフォルト: 128

no_check_password_users

パスワードの入力を要求されないユーザを指定します。

このトークンが関連するのは、check_password トークンが **yes** に設定されている場合のみです。

カンマで区切られたユーザのリストも有効な値です。

デフォルト: none

passwd_copy

ユーザ情報変更後に一時ファイルを元のファイルにコピー バックする際に、マシン パスワード ファイル(/etc/passwd)または PMDB パスワード ファイル (*/PMDB_Directory*/policies/pmdb/ passwd)の更新方法を指定します。有効な値は以下のとおりです。

fast_copy - 情報をファイルに上書きコピーします。

rename - 新しいファイルを指すようにディレクトリを変更します。

デフォルト: fast_copy

post_group_exit

UNIX 環境でグループ コマンドを実行した後に呼び出される exit プログラムのパスを指定します。

デフォルト: *ACInstallDir*/exits/lang_exit.sh

post_user_exit

UNIX 環境でユーザ コマンドを実行した後に呼び出される exit プログラムのパスを指定します。

デフォルト: *ACInstallDir*/exits/lang_exit.sh

pre_group_exit

UNIX 環境でグループ コマンドを実行する前に呼び出される exit プログラムのパスを指定します。

デフォルト: *ACInstallDir*/exits/lang_exit.sh

pre_user_exit

UNIX 環境でユーザ コマンドを実行する前に呼び出される exit プログラムのパスを指定します。

デフォルト: *ACInstallDir*/exits/lang_exit.sh

query_size

データベースへの問い合わせで一覧表示されるレコードの最大数を指定します。

デフォルト: 100

RecvTimeOut

selang が情報の受信を待機する場合のタイムアウトするまでの最長時間(秒単位)を指定します。

この値を 0 (ゼロ)に設定すると、タイムアウトは発生しません。

デフォルト: 60

SendTimeOut

selang が情報の送信を待機する場合のタイムアウトするまでの最長時間(秒単位)を指定します。

この値を 0 (ゼロ)に設定すると、タイムアウトは発生しません。

デフォルト: 60

SetBlockRun

Trusted プログラムの確認を行うかどうか、および Untrusted プログラムの実行をブロックするかどうかを指定します。プログラムが setuid か通常のプログラムかどうかに関わらず、実行のブロックが行われます。

有効な値は以下のとおりです。

yes - viapgm アクセス権限ルールで定義されたすべてのプログラムでは、blockrun プロパティが yes に設定されます。

no - viapgm アクセス権限ルールで定義されたすべてのプログラムでは、blockrun プロパティが no に設定されます。

suid - すべての setuid プログラムでは blockrun プロパティが yes に設定され、その他のすべてのプログラムでは blockrun プロパティが no に設定されます。

デフォルト: yes

swap_deletion_order

selang で「ru *userName* unix」コマンド（ユーザ削除）が実行される順序を定義します。通常の場合、このコマンドは AC 環境で最初に実行され、次に UNIX 環境で実行されます。この順序を逆にすることもあります（グループ管理者がユーザを削除する場合など）。

有効な値は以下のとおりです。

no - 最初に AC 環境から、次に UNIX 環境からユーザを削除します。

yes - 最初に UNIX 環境から、次に AC 環境からユーザを削除します。

デフォルト: no

timeout

クライアントが seosd デーモンの応答を待機する最長時間（秒単位）を指定します。この時間内に seosd から応答がない場合、seosd からの応答がないことを知らせるエラー メッセージが送信されます。クライアントはメッセージを受け取ると、seosd への接続を中止します。

デフォルト: 90

use_old_commands

ACF2™ と互換性のある古いコマンド（ag、lg、rg、lu、au など）を無効にするかどうかを指定します。

制限: 0 — 古いコマンドをサポートしない、1— 古いコマンドをサポートする

デフォルト: 1（古いコマンドをサポートす）

use_unix_file_owner

UNIX 環境のファイルの所有者が CA Access Control にファイルを定義できるかどうかを指定します。値が yes の場合、UNIX 環境のファイルの所有者は newres コマンドまたは newfile コマンドを使用して、CA Access Control にファイルを定義できます。

CA Access Control にすでにファイルが定義されている場合、CA Access Control の通常のアクセス権限ルールに従った許可が与えられない限り、ユーザはデータベースのパラメータを変更できません。

有効な値は、yes および no です。

デフォルト: no

ldap

[ldap] セクションのトークンは、LDAP サーバおよび入力データの検索に使用される属性を指定します。これらのパラメータは、*ACInstallDir*/samples/ldap/exits/S50CREATE_Ldap_u.sh にあるサンプルの ldap exit でのみ使用されます。

base_entry

LDAP ディレクトリ ツリーで基本エントリ ポイントとして使用するポイントを指定します。

たとえば、次のように指定します。o=*organization_name*, c=*country_name*

デフォルト: トークンは設定されていません

host

LDAP サーバのホスト名を指定します。

デフォルト: トークンは設定されていません（localhost）

path

LDAP クライアントの基本ディレクトリを指定します。

デフォルト: トークンは設定されていません（/usr/local/ldap）

port

LDAP サーバのポートを指定します（オプション）。

デフォルト: トークンは設定されていません（389）

logmgr

[logmgr] セクションのトークンは、ログ機能の動作を制御します。

audit_back

監査ログのバックアップ ファイルの名前を指定します。このファイルに対する書き込みを実行できるのは CA Access Control のみです。ユーザは、このファイルに対して書き込みアクセス権のみを持ちます。

デフォルト: *ACInstallDir*/log/seos.audit.bak

audit_group

監査ログに対する読み取り権限を持つグループを指定します。このトークンを **none** に設定すると、root のみに監査ログの読み取り権限が付与されます。CA Access Control はこのトークンの値の有効性を確認しないため、無効なグループ名を入力すると、監査ログ ファイルに対するアクセス許可はどのグループにも割り当てられません。

既存の監査ログ ファイルのグループ所有者権限を変更するには、以下の手順に従います。

selang の chgrp コマンドを使用して、ファイルのグループ所有者権限を設定します。

以下のコマンドを入力して UNIX のアクセス許可を変更します。

```
chmod 640 ACInstallDir/log/seos.audit
```

デフォルト: none

audit_log

監査ログ ファイルの名前を指定します。このファイルが *audit_size* で指定されたサイズに達すると、CA Access Control はファイルを閉じて、このファイルの名前を *audit_back* で指定された名前に変更した後、新しい監査ログを作成します。このファイルに対する書き込みを実行できるのは CA Access Control のみです。ユーザは、このファイルに対して書き込みアクセス権のみを持ちます。

デフォルト: *ACInstallDir*/log/seos.audit

audit_max_files

CA Access Control が日付によるバックアップを実行するときに蓄積する監査ログ バックアップ ファイルの最大数を定義します。BackUp_Date の設定が［*なし*］以外の任意の値に設定されている場合は、CA Access Control は引き続き日付によるバックアップ ファイルを蓄積します。この設定を使用すると、CA Access Control が監査ログのバックアップに使用するディスク領域を削減することができます。監査ログのバックアップ ファイル数が設定された制限に達すると、CA Access Control は最新のファイルを作成するときに最も古いバックアップ ファイルを削除します。

値は以下のとおりです。

- **0** - すべての監査ログ バックアップ ファイルを保持します。
- *n* - 0 を超える 正の整数。

注: CA Access Control は重複監査ログ バックアップ ファイルを自動的に保護するため、それらを手動で削除することはできません。さらに、監査レポートが有効な場合、レポート エージェントが処理を完了するまで、CA Access Control はバックアップ ファイルを削除しません。

デフォルト: 0

audit_size

監査ログ ファイルの最大サイズ（KB 単位）を指定します。

最小値は 50 KB です。

デフォルト: 10240

注: 監査ファイルのサイズが 2GB を超える場合、CA Access Control は、監査ファイルへの監査レコードの書き込みを停止します。

BackUp_Date

CA Access Control が監査ログ ファイルをバックアップする条件、および CA Access Control がタイムスタンプをバックアップ ファイル名に追加するかどうかを指定します。

audit_size 設定で指定されたサイズに達すると、CA Access Control は*常に*監査ログ ファイルをバックアップします。

値: none、yes、daily、weekly、monthly

- yes -- audit_size で指定されたサイズに達すると、CA Access Control は監査ログ ファイルをバックアップしし、タイム スタンプをバックアップ ファイル名に追加します。
- none -- audit_size で指定されたサイズに達すると、CA Access Control は監査ログ ファイルをバックアップしますが、タイム スタンプをバックアップ ファイル名に追加しません。
- daily、weekly、monthly -- 指定された時間間隔が経過し、かつ audit_size で指定されたサイズに達すると、CA Access Control は監査ログ ファイルをバックアップし、タイムスタンプをバックアップ ファイル名に追加します。ただし、指定された時間間隔内に監査イベントが監査ログ ファイルに書き込まれない場合、間隔が経過しても、CA Access Control はファイルをバックアップしません。

  注: CA Access Control は、最初の監査ログ ファイルを作成した時間から指定された間隔を数え、適切な日の午前零時にファイルをバックアップします。

例: 設定には週単位の値があり、CA Access Control は 4 月 1 日午前 9 時に監査ログ ファイルを作成します。多くの監査イベントが今週発生し、監査ログ ファイルは 4 月 4 日月曜日上に audit_size 設定で指定された値を超過します。CA Access Control は 4 月 4 日に監査ログ ファイルをバックアップし、タイム スタンプをバックアップ ファイル名に追加します。監査ログ ファイルが最初に作成された一週間後の 4 月 8 日金曜日の午前零時に、CA Access Control は再度監査ログ ファイルをバックアップし、タイムスタンプをバックアップ ファイル名に追加します。

デフォルト: none

error_back

エラー ログ バックアップ ファイルの名前を指定します。

デフォルト: *ACInstallDir*/log/seos.error.bak

error_group

エラー ログ ファイルに対する読み取り権限を持つグループを指定します。このトークンを **none** に設定すると、root のみにエラー ログ ファイルの読み取り権限が付与されます。CA Access Control はこのトークンの値の有効性を確認しないため、無効なグループ名を入力すると、エラー ログ ファイルに対するアクセス許可はどのグループにも割り当てられません。

既存のエラー ログ ファイルのグループ所有者権限を変更するには、以下の手順に従います。

selang の chgrp コマンドを使用して、ファイルのグループ所有者権限を設定します。

以下のコマンドを入力して UNIX のアクセス許可を変更します。

```
chmod 640 ACInstallDir/log/seos.audit
```

デフォルト: none

error_log

エラー ログ ファイルの名前を指定します。このファイルが *error_size* で指定されたサイズに達すると、CA Access Control はファイルを閉じ、このファイルの名前を *error_back* に指定された名前に変更し、新しいエラー ログを作成します。このファイルに対する書き込みを実行できるのは CA Access Control のみです。

デフォルト: *ACInstallDir*/log/seos.error

error_size

エラー ログ ファイルの最大サイズ(KB 単位)を指定します。

制限: 最小値は 50 KB です。

デフォルト: 50

irecorder_audit

IR API ライブラリが、ローカル セキュリティ デーモンの監査イベントだけでなく、既存の PMD の監査イベントも送るかどうかを指定します。

「all」- ローカル セキュリティ デーモンの監査イベントだけでなく、Policy Model の監査イベントも送ります。

「localhost」- ローカル セキュリティ デーモンの監査イベントのみを送ります。

デフォルト: all

logconnected

TCP-CONNECTED クラスのレコードが監査ログに書き込まれないようにします。

この機能を使用するには、logconnected を No に設定します。

デフォルト: no

詳細情報:

seaudit ユーティリティ - 監査ログ レコードの表示 (P. 118)
seerrlog ユーティリティ - エラー ログ レコードの表示 (P. 189)

message

[message] セクションのトークンは、semsgtool メッセージ ユーティリティの動作を制御します。

filename

入力された selang のコマンドに対して表示されるほとんどのメッセージを提供するファイルの場所と名前を指定します。

デフォルト: *ACInstallDir*/data/seos.msg

MessagesDirectory

CA Access Control メッセージ ファイルの場所を指定します。

デフォルト: *ACInstallDir*/data/msg

mfsd

[mfsd] セクションのトークンは、メインフレーム同期デーモン オプションを定義します。

mfsd_trace_file

CA Access Control のメインフレーム同期デーモンである mfsd のトレース メッセージが書き込まれるファイルの場所を指定します。

このトークンを **no** に設定すると、トレース ファイルは作成されません。

デフォルト: *ACInstallDir*/log/mfsd.trace

OS_User

[OS_User] セクションのトークンは、エンタープライズ ユーザおよびエンタープライズ グループに対して、CA Access Control が使用する設定を定義します。

create_user_in_db

CA Access Control に定義されていないユーザがログインしたときに、そのユーザの XUSER レコードを CA Access Control が作成するかどうかを指定します。

注: この設定は、エンタープライズ ユーザを使用する(osuser_enabled が 1 に設定されている)場合にのみ適用されます。

制限: yes、no

デフォルト: yes

nonunix_unabgroup_enabled

CA Access Control が UNIX 認証ブローカ データベースで UNIX でないユーザ グループをサポートするかどうかを指定します。

制限: yes、no

デフォルト: no

osuser_enabled

エンタープライズ ユーザおよびエンタープライズ グループを有効にするかどうかを指定します。

制限: yes、no

デフォルト: yes

UserCache_groups_max

実行時ユーザ キャッシュ テーブル内のグループの最大数を定義します。

デフォルト: 1000

UserCache_max

実行時ユーザ キャッシュ テーブル内のエントリの最大数を定義します。

デフォルト: 20000

UserCache_timeout

実行時ユーザ キャッシュ テーブルからレコードが削除されるまでの期間(分単位)を定義します。

デフォルト: 60

verify_osuser

CA Access Control 内にエンタープライズ ユーザのレコード（XUSER）を作成する前に、エンタープライズ ストアにユーザが存在していることを CA Access Control が確認するかどうかを指定します。

制限： no - ユーザがエンタープライズ ユーザ ストアに定義されている場合のみ、そのユーザはエンタープライズ ユーザ レコードを作成できます。yes - ユーザは常にエンタープライズ ユーザ レコードを作成できます。

デフォルト： no

package

[package] セクションのトークンは、インストール対象として選択したパッケージを指定します。

Client、Server、Admin、Mfsd、Tng、Stop、Api

指定したパッケージをインストールの対象として選択したかどうかを示します。

デフォルト： no

pam_seos

[pam_seos] セクションのトークンは、プログラミング インターフェースである PAM（Pluggable Authentication Module）を最大限に活用するために有用です。

api_update_lastaccterm

ユーザの前回のアクセス日時を API ライブラリが（SEOS_VerifyCreate 経由で）更新するかどうかを指定します。

有効な値は以下のとおりです。

0 - 前回のアクセス日時は更新されません。

1 - 前回のアクセス日時は更新されます。

デフォルト： トークンは設定されていません（0）

bypass_services

PAM がバイパスするサービスを定義します。

デフォルト： ftp,vsftpd

call_segrace

segrace ユーティリティを任意のログインで自動的に呼び出すかどうかを指定します。

有効な値は、yes および no です。

デフォルト: no

call_sepass

pam_seos パスワード管理サービスで sepass ユーティリティを使用するかどうかを指定します。

値: No、Yes

デフォルト: トークン未設定（No）

debug_mode_for_user

ログインの拒否理由をユーザに通知するかどうかを指定します。

有効な値は、yes および no です。

デフォルト: no

failed_login_file

失敗したログインの監査ファイルである pam_seos の場所を指定します。

デフォルト: *ACInstallDir*/pam_seos_failed_logins.log

pam_login_events_enabled

pam_seos がログイン イベントを seosd に送信するかどうかを指定します。

値: **0** -- ログイン イベントを送信しません。**1** -- ログイン イベントを送信します。

デフォルト: 1

pam_get_groups

pam_seos で、オペレーティング システムからユーザ グループの抽出を試行するかどうかを指定します。

値: 0 - グループの抽出を試行しない、1 - グループの抽出を試行する

デフォルト: 1

pam_groups_timeout

CA Access Control PAM で API がユーザ グループを抽出する際に使用するタイムアウト時間を秒数で定義します。

デフォルト: 10

PamPassUserInfo

pam_seos がユーザ情報を seosd に送信するかどうかを指定します。これは、CA Access Control に情報が存在しないエンタープライズ ユーザを使用する場合に必要です。エンタープライズ ユーザを使用しない（osuser_enabled = no）場合は、この値を 0 に設定します。

値：0 -ユーザ情報を送信しない、**1** - ユーザ情報を送信する。

デフォルト： 0

pam_surrogate_events_enabled

pam_seos が代理イベントを seosd に送信するかどうかを指定します。

値：0 -- surrogate イベントを送信しません。**1** -- surrogate イベントを送信します。

デフォルト： 1

process_failed_logins

pam_seos が pam_authenticate を呼び出して、ユーザ パスワードを認証し、失敗ログインを処理するかどうかを指定します。

pam_authenticate を 2 回呼び出さないようにするには、この値を 0（ゼロ）に設定します。

値：0 - CA Access Control の PAM モジュールから call pam_authenticate を呼び出しません。**1** - CA Access Control の PAM モジュールから call pam_authenticate を呼び出します。

デフォルト： 1

serevu_use_pam_seos

ログイン失敗のログ ファイルとして、システム ファイルの代わりに pam_seos を使用するように serevu を設定するかどうかを指定します。

この機能は、serevu の正確性を高めます。

デフォルト： *yes*（HP-UX Itanium（IA64）および Linux）、*no*（その他すべてのオペレーティング システム）

passwd

[passwd]セクションのトークンは、パスワードの変更およびその他のユーザ関連サービスを定義します。

AllowedGidRange

ユーザが追加、更新、および削除できる GID の範囲を指定します。この範囲外の値は、CA Access Control で更新できない予約済みの GID を意味します。

注: 指定された整数が 1 つしかない場合は、1 から指定された整数までのすべての整数が予約済み GID になります。上限よりも大きな数値を指定した場合は、デフォルトの上限(30000)が適用されます。負の数値を指定した場合は、デフォルトの下限(1)が適用されます。

制限: 1 ～ 2147483647

デフォルト: 100,30000

AllowedUidRange

ユーザが追加、更新、および削除できる UID の範囲を指定します。この範囲外の値は、CA Access Control で更新できない予約済みの UID を意味します。

注: 指定された整数が 1 つしかない場合は、1 から指定された整数までのすべての整数が予約済み UID になります。上限よりも大きな数値を指定した場合は、デフォルトの上限(30000)が適用されます。負の数値を指定した場合は、デフォルトの下限(1)が適用されます。

制限: 1 ～ 2147483647

デフォルト: 100,30000

AllowRootProp

sepass -p または sepass -s を使用して行った root のパスワード変更が、Policy Model に送信されるかどうかを指定します。次に、PMD からそのサブスクライバにパスワードが伝達されます。

有効な値は、yes および no です。

デフォルト: no

change_pam

LDAP データベースにおけるパスワードの認証および変更に、ローカル ホストが PAM を使用するかどうかを指定します。

デフォルト: no

Check_Adm_Rules

ADMIN および PWMANAGER ユーザにパスワード ルールを適用するかどうかを指定します。

デフォルト: no

Check_All_User_Rules

selang がすべてのユーザに対してパスワード ルールをチェックするかどうかを指定します。

有効な値は、yes および no です。

トークンが yes に設定されている場合、selang はすべてのユーザに対してパスワード ルールをチェックします。

トークンが no に設定されている場合、selang はパスワードを変更したユーザに対してのみパスワード ルールをチェックします。

デフォルト: no

注: このトークンは、API を使用する場合のみサポートされています。

CreateHashedPasswdDatabase

(DEC UNIX のみ)。exit スクリプトの実行タイミングを、CA Access Control の各コマンドによってユーザ レコードを作成、更新、または削除した後にするか、または sepass ユーティリティを使用して各ユーザのパスワードを変更した後にするかを指定します。

注: 使用方法の詳細については、*ACInstallDir*/samples/exits-src/USER_POST ディレクトリに格納されている README ファイルを参照してください。

デフォルト: no

DefaultHome

システムのデフォルトのホーム ディレクトリを指定します。ユーザのホーム ディレクトリは、指定されたシステム ホーム ディレクトリのサブディレクトリです。たとえば、システムのホーム ディレクトリが /home の場合、新規ユーザのホーム ディレクトリは /home/*username* になります。値を指定した場合、このトークンの値は、クライアントの lang.ini ファイルの値より優先されます。*nohomedir* を指定すると、ホーム ディレクトリは自動的には設定されません。

デフォルト: /home

DefaultPasswdCmd

デフォルトのパスワード プログラムを指定します。指定した場合、このパスワード プログラムは、sepass が開始され、seosd が実行中でないときに使用されます。

デフォルト: /bin/passwd

DefaultPgroup

値が入力されなかった場合に CA Access Control によって新しい UNIX ユーザに割り当てられるプライマリ グループを指定します。

デフォルト: other

DefaultShell

値が入力されなかった場合に CA Access Control によって新しい UNIX ユーザに割り当てられるデフォルトのシェルを指定します。値を指定した場合、このトークンの値は、クライアントの lang.ini ファイルの値より優先されます。

デフォルト: /bin/sh（または、HP-UX では /sbin/sh）

ディクショナリ

パスワードとして使用 できない 語が格納されているファイルの完全パス名を定義します。

注: このファイルを使用するには、*ファイル*に辞書形式パスワード ルール（use_dbdict）を設定し、UseDict 設定を *yes* に設定する必要があります。辞書形式が *db* に設定された場合、使用できないパスワードは CA Access Control データベースから取得され、この設定は無視されます。これは、UNIX のデフォルトの設定です。

重要: このトークンは廃止されています。代わりにデータベース内の辞書を使用します。

デフォルト: /usr/dict/words

GeneratePasswd

sepass が新しいパスワードを生成するかどうかを指定します。

有効な値は、yes および no です。

このトークンを no に設定すると、ユーザは新しいパスワードの入力を要求されます。

デフォルト: no

HomeDirUpd

ユーザのプライマリ グループが変更されたときに、CA Access Control がユーザのホーム ディレクトリのグループ所有者権限を更新するかどうかを指定します。

有効な値は、**yes** および **no** です。

デフォルト: yes

nis_env

ローカル ホストが NIS クライアントまたは NIS+ クライアントかどうかを指定します。

有効な値は no、nis、または nisplus です。

デフォルト: no

NisPlus_server

この端末が NIS+ サーバかどうかを指定します。

有効な値は、yes および no です。

このトークンの値が yes の場合、CA Access Control はパスワードの変更を NIS+ パスワードの変更として扱います。

デフォルト: no

only_local

sepass のデフォルト設定に -l フラグを含めるかどうかを決定します。

有効な値は、yes および no です。

このトークンが yes に設定されている場合、ローカル パスワード ファイル (通常は /etc/passwd)、セキュリティ ファイル、ローカル データベースなどのローカルでのみ、sepass はパスワードを変更します。

デフォルト: no

only_pmdb

sepass のデフォルト設定に -p フラグを含むかどうかを指定します。トークンの値が yes の場合、sepass は指定されたホストの PMDB でのみパスワードを変更します。

データベースが定義されていない場合、sepass はパスワードを変更しません。

デフォルト: no

passwd_distribution_encryption_mode

パスワードが Policy Model サービスの一部として配布されているときに、ユーザのパスワードの暗号化に使用される方法を指定します。

有効な値は以下のとおりです。

1 - 互換モード。長いパスワードを使用しない CA Access Control システム間でパスワードを配布します（r12 より古いバージョンの CA Access Control を実行しているマシンもすべて含まれます）。

2 - MD5 モード。長いパスワードを使用し、Linux も実行している CA Access Control システム間でパスワードを配布します。

3 - 双方向モード。長いパスワードを使用する CA Access Control システム間で暗号化されたメッセージ内の平文として、パスワードを安全に配布します。

デフォルト: 1

passwd_format

パスワードの変更が NT ホストに伝達されるかどうかを示します。

このトークンを **NT** に設定することは、管理しているホストの 1 つが NT ホストであることを示しています。

デフォルト: none

passwd_local_encryption_method

パスワードがローカルに格納されているときに、ユーザのパスワードの暗号化に使用される方法を指定します。

有効な値は以下のとおりです。

crypt - UNIX での標準的な一方向の暗号化で、パスワードの最初の 8 文字のみを（DES キーとして）使用します。crypt を指定すると、長いパスワードの使用が無効になります。

md5 - MD5 のハッシュ関数で、暗号化できるパスワードの長さに制限はありません。md5 を指定すると、長いパスワードの使用が有効になります。

デフォルト: crypt

PromptOldPassword

sepass が /opt/CA/AccessControl// bin/segrace から起動される際に、ローカル ユーザに古いパスワードの入力を促すかどうかを指定します（完全パスを使用する必要があります）。

このトークンを **yes** に設定すると、ユーザは古いパスワードの入力を求められます。

デフォルト: yes

quiet_mode

sepass で著作権に関する情報、および Policy Model へのパスワードの伝達に関するメッセージを表示するどうかを指定します。

デフォルト: no

RootPwAsOwn

sepass により、特権ユーザが、（*-x* オプションを使用して）root で変更するかのように、root のパスワードを変更できるようにするかどうかを指定します。

有効な値は以下のとおりです。

yes - 特権ユーザが、sepass を使用して、root で変更するかのように root のパスワードを変更できます。root のパスワードを本人として変更することはできません（管理者による変更）。

no - 特権ユーザが、sepass を使用して、本人としてのみ root のパスワードを変更できます（管理者による変更）。

たとえば、トークンが *yes* に設定されている場合、特権ユーザは、以下のコマンドを使用して root のパスワードを変更できます。

```
sepass -x root
```

同じユーザでも、以下のコマンドを使用して root のパスワードを変更することはできません。

```
sepass root
```

このトークンが *no* に設定されている場合、上記の説明とは逆になります。

デフォルト: no

SaveGroupAttrs

UNIX 環境でのグループの更新後に以前のグループ ファイルの所有者、グループ、およびモードを保存するかどうかを指定します。

有効な値は、yes および no です。

このトークンを **no** に設定すると、新しい値がそれぞれ 0、0、644 に設定されます。

デフォルト: no

SavePasswdAttrs

UNIX 環境でのユーザの更新後に以前のパスワード ファイルの所有者、グループ、およびモードを保存するかどうかを指定します。

有効な値は、yes および no です。

このトークンを **no** に設定すると、新しい値がそれぞれ 0、0、644 に設定されます。

デフォルト: no

Shadow_Admin_Change

(AIX プラットフォームのみ)。管理者が selang から、または sepass を使用してパスワードを変更したときに、/etc/security/passwd ファイルのユーザ エントリに ADMCHG フラグが追加されるかどうかを指定します。

デフォルト: no

UIDAlgorithm

新しいユーザを追加するときにフリー UID アルゴリズムを採用するかどうかを指定します。*別の任意の値に設定すると、古いプロセスが選択されることになります。new* アルゴリズムは、64 KB を超える UID 番号を提供し、通常はより高速です。

デフォルト: new

UseDict

パスワードの確認時に、(Dictionary 設定で指定された)辞書ファイルを使用するかどうかを指定します。

注: 辞書ファイルを使用するには、*ファイル*に辞書形式パスワード ルール (use_dbdict)を設定する必要があります。辞書形式が *db* に設定された場合、使用できないパスワードは CA Access Control データベースから取得され、この設定は無視されます。

デフォルト: no

YpGrpCmd

NIS グループ マップの作成に使用するコマンドを指定します。

デフォルト: make group

YpMakeDir

NIS マップの作成時に使用される makefile ディレクトリの名前を指定します。

デフォルト: /var/yp

YpPassCmd

NIS パスワード マップの作成に使用するコマンドを指定します。

デフォルト: make passwd

YpServerGroup

NIS グループ マップの作成元となるグループ ファイルを指定します。

デフォルト: /etc/group

YpServerPasswd

NIS パスワード マップの作成元となるパスワード ファイルを指定します。

デフォルト: /etc/passwd

YpServerSecure

NIS パスワード マップの作成に使用されるパスワードを含むセキュリティ ファイルの名前を指定します。

デフォルト: 以下のように、プラットフォームによって異なります。

- IBM AIX: /etc/security/passwd
- HP-UX: /.secure/etc/passwd
- Sun Solaris: /etc/shadow

YpTimeOut

新しいクライアント(selang や Security Administrator など)が ypbind テストを実行できる時間(秒単位)を指定します。このテストにより、ローカル ホストが NIS サーバに接続しているかどうかを確認できます。指定された時間が経過すると、クライアントは終了し、エラー メッセージが表示されます。

このデフォルト値がゼロ(**0**)の場合、ypbind テストは実行されていません。

デフォルト: 0

詳細情報:

sepass ユーティリティ - パスワードの設定または変更 (P. 219)

pmd

[pmd] セクションのトークンは、PMDB の属性を指定します。

注意: 各 Policy Model には、seos.ini ファイル以外に、pmd.ini という名前の環境設定ファイルが含まれています。

_min_retries_

使用不可のサブスクライバに対して、キューに格納されている次の更新の再送信を sepmdd が試行する最小回数を指定します。sepmdd は、サブスクライバのリスト内をループして未処理の更新を見つけます。使用不可のサブスクライバに対して更新を再送信できなかった場合、カウンタの数値を上げます。このトークンで指定した最小試行回数を超えた場合、そのサブスクライバには「使用不可」のマークが付けられます。

デフォルト: 4

_pmd_backup_directory_

CA Access Control が Policy Model のバックアップを格納するために使用するディレクトリを定義します。CA Access Control は各 PMD バックアップを *pmd_name* という名前のサブディレクトリに格納します。

デフォルト: *ACInstallDir*/data/policies_backup

_pmd_directory_

PMDB を格納するディレクトリを指定します。名前は最大 70 文字の英数字で指定できます。ディレクトリの完全パスを指定します。各 Policy Model は、*pmdDirectory*/*pmdName* ディレクトリに格納されます。

デフォルト: *ACInstallDir*/policies

_PMD_DIRECTORY_

_pmd_directory_ と同じ

_PMD_EXEC

Policy Model デーモンの名前を定義します。

_QD_timeout_

sepmdd デーモンがサブスクライバ リストの最初のスキャンでサブスクライバ データベースの更新を試みる際に、sepmdd デーモンが待機する制限時間（秒単位）を指定します。制限時間が経過した時点でサブスクライバを更新できなかった場合、デーモンはそのサブスクライバの更新処理を省略して、サブスクライバ リストにある残りのサブスクライバの更新を試みます。

sepmdd は、サブスクライバ リストの 1 回目のスキャンが終了した後、2 回目のスキャンを実行します。2 回目のスキャンでは、1 回目のスキャンで更新できなかったサブスクライバの更新を試みます。2 回目のスキャンでは、接続システム コールがタイムアウトになるまで（約 90 秒間）サブスクライバの更新を試みます。

デフォルト: 3

_retry_timeout_

_min_retries_ で指定した試行の最小回数に達した後、使用不可のサブスクライバに対して更新を再送信するまでの待機期間（分単位）を指定します。このトークンで定義した期間（分単位）を経過すると、このサブスクライバには「使用可能」のマークが付けられます。

サブスクライバは、以下のいずれかが行われるまで、「使用不可」とマーキングされています。

- 手動でリリースされる。
- sepmdd が手動で停止されて再起動される。sepmdd は以下の場合に再起動されます。
  - 言語機能が sepmdd に接続しようとした場合。
  - 親 PMD が更新を送信しようとした場合。
  - pull オプションがサブスクライバによってトリガされた場合。この現象は、サブスクライバで CA Access Control が起動したときに発生することがあります。
- pull オプションが使用不可のサブスクライバによってトリガされる。

注: sepmdd をあまり頻繁に停止するのは好ましくありません。これは、デーモンの再起動には時間がかかり、結果として伝播プロセス全体の速度が低下するためです。安定性に問題が発生する可能性があるため、停止せずに常時稼動させることもお勧めできません。

デフォルト: 30

_shutoff_time_

sepmdd が終了するまでのアクティビティの時間（分単位）を指定します。このトークンの値がゼロの場合、sepmdd は終了しません。

デフォルト: 0

ClientOperationTimeout

クライアントが Policy モデルからの応答を待機するタイムアウト期間を秒で定義します。

デフォルト: 60

is_maker_checker

デュアル コントロールを使用するかどうかを指定します。

有効な値は、yes および no です。

このトークンの値が **yes** の場合、データベースは直接更新できず、PMDB を使用した場合にのみ更新できます。更新には Maker（作成者）および Checker（チェッカ）という 2 種類の管理者の協力が必要です。

デフォルト: トークンは設定されていません（no）

pass_auth

リモートでのパスワード変更時に、起動したユーザのパスワードを sepass で確認するかどうかを指定します。sepass ユーティリティは、ユーザが入力した古いパスワードと、ローカル prodname データベースに格納されているパスワードを常に比較します。このトークンを yes に設定すると、sepass は、sepass を実行しているユーザが入力した古いパスワードと、リモート prodname データベース（通常は pmdb）に格納されているそのユーザのパスワードを比較します。つまり、sepass ユーザは、自分以外のユーザのパスワードを変更するときにも、自分のパスワードを入力する必要があります。

値: yes、no

デフォルト: yes

pull_option

サブスクライバ データベースが使用可能になったときにデータベースをただちに更新するかどうかを指定します。

有効な値は、yes および no です。

このトークンの値が **yes** の場合、サブスクライバ端末が使用可能になると、seagent はローカル ホストおよびマシン上の任意の Policy Model の両方の親 Policy Model にただちにメッセージを送信します。メッセージが送信されると、sepmdd は次の 30 分後の再試行を待たずに、ただちにサブスクライバを更新します。

デフォルト: yes

send_unix_env

sepmd -n オプションで Policy Model のパスワード ファイルとグループ ファイルの内容を送信するかどうかを指定します。

有効な値は、yes および no です。

yes - *sepmd -n* オプションで Policy Model のパスワード ファイルとグループ ファイルの内容を送信します。

no - *sepmd -n* オプションでは、Policy Model のパスワード ファイルとグループ ファイルの内容は送信されません。

デフォルト: yes

ShutdownWaitingTimeout

Policy モデルが、そのコンポーネントの正常なシャットダウンを待機するタイムアウト期間を秒で定義します。Policy モデルのコンポーネントが正常にシャット ダウンしなかった場合、Policy モデルは強制的にシャット ダウンされます。

デフォルト: 60

synch_uid

新規の UNIX ユーザを作成するときに、親 Policy Model ホストと同じ UID の使用を CA Access Control がサブスクライバに強制するかどうかを指定します。

updates_in_chunk

Policy Model がその各サブスクライバに対してループの各サイクルで送信するコマンドの最大数を定義します。

デフォルト: 10

詳細情報:

sepmd ユーティリティ (P. 222)

policyfetcher

[policyfetcher] セクションのトークンは、ポリシー フェッチャ デーモン（policyfetcher）の動作を制御します。

check_deployment_tasks

分散ホスト上で新規のデプロイ タスク（DEPLOYMENT リソース）を policyfetcher がチェックする頻度（秒単位）を定義します。

デフォルト: 600（10 分ごと）

制限: 最小値は 60

deploy_timeout

デプロイ タスクまたはデプロイ解除タスクがエンドポイントで完了するのを policyfetcher が待つ秒数を定義します。

デフォルト: 900

devcalc_command

policyfetcher で偏差計算の実行に使用する selang コマンドを定義します。

デフォルト: start DEVCALC params(-nonotify)

例: start DEVCALC params(-nonotify -precise)

dh_command_retry_interval

DH 通知コマンドの試行間隔を秒数で定義します。

デフォルト: 30

endpoint_heartbeat

policyfetcher が分散ホスト（DH）にハートビートを送信する頻度を定義します。この頻度は check_deployment_task 設定の要因であり、policyfetcher がハートビートを送信する前にデプロイ タスクをチェックする回数を決定します。たとえば、check_deployment_task がデフォルトの 600 秒（10 分）に設定されているときに 6 に設定すると、policyfetcher は 3600 秒（1 時間）ごとにハートビートを送信します。

ハートビートの送信後、policyfetcher はさらに偏差計算を実行（devcalc コマンドを開始）し、偏差計算が完了するのを 60 秒待ちます。60 秒後、policyfetcher は、ローカル エンドポイント情報が DH 情報と同一であることを確認します。

デフォルト: 10

max_dh_command_retry

policyfetcher が DH から更新通知の取得を再試行する最大回数を定義します。この回数を超えても取得されない場合は、再試行されなくなります。

デフォルト: 3

max_dh_retry_cycles

policyfetcher が本番の DH から更新通知の取得を再試行する最大サイクル数を定義します。このサイクル数を超えても取得されない場合、惨事復旧用の DH に移行します。

デフォルト: 3

policy_verification

policyfetcher デーモンがバックアップ CA Access Control データベース上で新しいデプロイ タスクを実行する前にそれらを検証するかどうかを指定します。

有効な値は以下のとおりです。

1 - ポリシー検証を実行する

0 - ポリシー検証を無効にする

デフォルト: 0

policyfetcher_enabled

policyfetcher デーモンを実行するかどうかを指定します。

有効な値は以下のとおりです。

1 - policyfetcher を実行する

0 - policyfetcher を無効にする

デフォルト: 0

PUPMAgent

[PUPMAgent]セクションでは、トークンによって特権ユーザ パスワード管理エージェントの機能が決定されます。

EnableLogonIntegration

端末統合が有効であると指定します。

制限: 0 - 端末統合は無効です。1 - 端末統合は有効です。

デフォルト: 1

interfaceName

コミュニケーション インタフェース名 (特権ユーザ パスワード管理 エージェントがリクエストを処理する UNIX ソケット名) を定義します。ソケット ファイルは、/opt/CA/AccessControl/data/PUPMAgent ディレクトリにあります。

デフォルト: PUPMAgentInterface

OperationMode

特権ユーザ パスワード管理 エージェントの動作モードを指定します。

制限: 0 - 特権ユーザ パスワード管理 エージェントは無効です。実行されていません。1 - 特権ユーザ パスワード管理 エージェントは有効で、実行されています。しかし、トレース ファイルにデータを記録していません。2 - 特権ユーザ パスワード管理 エージェントは有効で、実行されています。また、トレース ファイルにデータを記録中です。

デフォルト: 0

seagent

[logmgr]セクションのトークンは、seagent デーモンの動作を制御します。

debug_backup

CA Access Control が seagent デバッグ メッセージ バックアップ ファイルを使用するかどうかを指定します。

制限: yes、no

デフォルト: yes

debug_backup_file

seagent デバッグ メッセージ バックアップ ファイルの名前を定義します。

デフォルト: *ACInstallDir*/log/seagent_debug.back

debug_file

CA Access Control が seagent デバッグ メッセージを書き込むファイルの名前を定義します。

デフォルト: *ACInstallDir*/log/seagent_debug

debug_level

CA Access Control がデバッグ ファイルに書き込むデバッグ メッセージの最小レベルを指定します。

制限:

- disabled -- メッセージはデバッグ ファイルに書き込まれません。
- critical -- CRITICAL メッセージはデバッグ ファイルに書き込まれます。
- very_high -- CRITICAL および VERY_HIGH メッセージはデバッグ ファイルに書き込まれます。
- high -- CRITICAL、VERY_HIGH および HIGH メッセージはデバッグ ファイルに書き込まれます。
- normal -- CRITICAL、VERY_HIGH、HIGH および NORMAL メッセージはデバッグ ファイルに書き込まれます。
- low -- CRITICAL、VERY_HIGH、HIGH、NORMAL および LOW メッセージはデバッグ ファイルに書き込まれます。

デフォルト: critical

watchdog_check_interval

seagent が seoswd の存在を確認する時間間隔を秒単位で定義します。

注: このトークンが適用されるには、seagent に対して大量の受信接続がある場合のみです。seagent がビジーでない場合は、seoswd の存在を 3 秒間隔で確認し、このトークンは無視されます。

デフォルト: 30

seauxd

[seauxd] セクションのトークンは、Unicenter TNG カレンダーの用途と更新間隔を指定し、名前解決を管理しやすくします。

client_request_timeout

解決の要求を保持する時間間隔(秒単位)を指定します。

デフォルト: 120

file_time_check

/etc/passwd での変更をチェックする時間間隔(秒単位)を指定します。

0 を指定すると、チェックが無効になります。

デフォルト: 10

init_delay

seauxd の起動を待つ時間(秒単位)を指定します。

デフォルト: 10

log_file_name

補助ログ ファイルの名前を指定します。補助ログ ファイルの場所は SEOSPATH/log です。

デフォルト: seauxd.log

log_file_size

補助ログ ファイルの最大サイズ(KB 単位)を指定します。このサイズを超過した場合は、ファイルが 0 に切り捨てられます。

デフォルト: 100

log_level

使用するログのレベルを指定します。

有効な値は以下のとおりです。

0 - Minimum info
1 - ERR
2 - WARN + ERR
3 - NOTIC + WARN + ERR
4 - DEBUG + INFO + WARN + ERR

デフォルト: 0

req_poll_timeout

入力要求を待機する時間間隔(ミリ秒単位)を指定します。

デフォルト: 200

respawn_seauxd_delay

seauxd が終了した場合に seosd によって再発生する最小時間(秒単位)を定義します。

デフォルト: 60

TNG_cal_lib

Unicenter TNG カレンダーを含む共有ライブラリの名前を指定します。

デフォルト: libcalendar

TNG_calendars

時間間隔の設定時に Unicenter TNG カレンダーを使用してリソースを制限するかどうかを指定します。

デフォルト: no

TNG_lib_path

Unicenter TNG カレンダーを含む共有ライブラリを検索するための CA Access Control のパスを指定します。

デフォルト: /opt/CA/CAlib

TNG_refresh_interval

Unicenter TNG からアクティブなカレンダー情報を取得するための CA Access Control の更新間隔(分単位)を指定します。

デフォルト: 10

trace_cnt

トレース ファイルにカウンタを書き込むかどうかを示します。

有効な値は、yes および no です。

デフォルト: no

segrace

[segrace] セクションのトークンは、segrace ユーティリティの属性を指定します。

sepass_command

ユーザの猶予ログインの回数が残っていないときに実行される CA Access Control のパスワード変更コマンドの場所を指定します。

デフォルト: *ACInstallDir*/bin/sepass

詳細情報:

segrace ユーティリティ - ユーザのログイン情報の表示 (P. 190)

seini

[seini] セクションのトークンは、seini のインテリジェント検索機能の属性を指定します。

get_error_warning

インテリジェント検索機能のエラー メッセージおよび警告メッセージを表示するかどうかを指定します。

デフォルト: yes

perform_action

インテリジェント検索機能で検索されたトークンまたはセクションのどちらで seini がその操作を行うかを指定します。

有効な値は、yes および no です。

このトークンを **yes** に設定すると、高度なインテリジェント検索で見つかったセクションおよびトークンが、要求した seini 操作の実行に使用されます。

デフォルト: no

use_intelligent_search

seini ユーティリティの起動時にインテリジェント検索を実行するかどうかを指定します。

デフォルト: no

詳細情報:

seini ユーティリティ - 環境設定ファイルの管理 (P. 197)

selock

[selock] セクションのトークンは、selock ユーティリティの動作を制御します。

unlocking_user

ロックされた画面のロックを解除できる所有者以外のユーザの名前を指定します。

デフォルト: root

詳細情報:

selock ユーティリティ - X 端末画面のロック (P. 205)

selogrd

[selogrd] セクションのトークンは、ログ ルーティング デーモンの selogrd および selogrcd の動作を制御します。

Caudit_size

監査データ収集ファイルの最大サイズ(KB 単位)を指定します。このサイズに達すると、バックアップ ファイルが作成され、新しいファイルが開きます。

最小値は 50 KB です。

デフォルト: 1024

CBackUp_Date

selogrcd がバックアップを実行する基準を設定します。

有効な値は、none、yes、daily、weekly、および monthly です。

yes を指定すると、CA Access Control はサイズ制限トークンである Caudit_size に従ってバックアップを実行し、バックアップ ファイルにタイムスタンプを追加します。

none を指定すると、CA Access Control は Caudit_size トークンに従ってバックアップを実行しますが、バックアップ ファイルにはタイムスタンプを追加しません。

daily、**weekly**、または **monthly** を指定すると、selogrcd は最初に監査ログ ファイルを作成するときに、タイムスタンプを追加します。現在の日付がこのタイム スタンプを過ぎると、CA Access Control は自動的にバックアップ ファイルを作成し、作成したファイルにタイム スタンプを追加します。

ただし、その前にファイルのサイズが Caudit_size トークンの値を超えた場合、CA Access Control はタイムスタンプを発行せずにバックアップ ファイルを作成します。

デフォルト: none

ChangeLogFactor

ログ ファイルがバックアップ ファイルに変更されたかどうかをテストする前に、*Interval* トークンの値に適用される係数を指定します。たとえば、*Interval* トークンが 5 に設定され、*ChangeLogFactor* トークンが 5 (デフォルト) に設定されている場合、CA Access Control は 25 秒間待機してから、ログ ファイルがバックアップ ファイルに変更されたかどうかをチェックします。

デフォルト: 5

CipherName

UseEncryption トークンが eTrust に設定された場合に selogrd で使用する暗号化関数を含むファイルの名前を指定します。

このファイルは、*ACInstallDir*/lib/ ディレクトリに置く必要があります。

CipherName は、共有オブジェクト ファイルに対するシンボリック リンクです。

デフォルト: adcipher

CollectFile

監査収集デーモンである selogrcd が収集した監査レコードを格納するファイルの名前を指定します。

デフォルト: *ACInstallDir*/log/seos.collect.audit

CollectFileBackup

USR1 シグナルを受信する際に、selogrcd が収集した監査レコードのファイルをバックアップしてファイル名を変更するときに使用される名前を指定します。

デフォルト: *ACInstallDir*/log/seos.collect.bak

ConsolePort

selogrd - secmon 通信の名前またはポート番号を指定します。この指定は、同じホストで selogrcd と secmon を両方とも実行する場合にのみ必要です。

指定した場合、seolgrd - secmon 通信は、指定されたポートを使用して実行されます。指定しなかった場合は、*ServicePort* トークンで指定されたポートを使用します。さらにそのトークンも空の場合は、RPC portmapper を使用して動的にポートを割り当てます。ログ ルーティング デーモンは通信に UDP を使用するため、サービス名に UDP ポートを指定する必要があります。

トークンの値が数字の場合は、指定されたポート番号にデーモンがバインドされます。

トークンの値がサービス名(文字列)の場合は、/etc/services または NIS サービス マップを使用して、ポート番号が解決されます。

デフォルト: トークンは設定されていません(*ServicePort* トークンから取り出された値)

DataFile

指定されたターゲットに送信される前に、ターゲット ルーティング情報が書き込まれるファイルの名前を指定します。

デフォルト: *ACInstallDir*/log/logroute.dat

Interval

selogrd デーモンによるログ ファイルのポーリング間隔(秒単位)を指定します。

デフォルト: 5

KeyFile

監査の暗号化鍵を保持するファイルの名前を指定します。

この鍵は、selogrd が CA Access Control 監査の暗号化を実行するときに使用します。鍵ファイルは、*ACInstallDir*/lib ディレクトリに格納されます。

鍵は、sechkey ユーティリティで変更できます。

デフォルト: adcipher.bin

Mailer

selogrd で電子メールを送信する際に使用するプログラムの名前を指定します。

注: このオプションは、UseSmtpMail トークンを yes に設定した場合にのみ適用されます。

デフォルト: /bin/mail

MaxErrorSending

selogrcd への監査レコード送信時の障害数がこのトークンの値を超えた場合にのみ、この障害に関するエラー メッセージを selogrd が syslog に送信するかどうかを指定します。

デフォルト値は 1 です。つまり、selogrd から selogrcd への送信時に障害が発生するたびに、メッセージが syslog に送信されます。

デフォルト: 1

MaxSeqNoSleep

selogrd がスリープ状態にならずにスキャンするログ レコードの最大数を指定します。

デフォルト: 50

RefuseUnencrypted

selogrcd が非暗号化監査を受け入れるかどうかを指定します。これは UseEncryption トークンと組み合わせて使用し、UseEncryption を **no** に設定した場合は冗長になります。そのため、selogrcd で暗号化を使用する場合にのみ有効です。

有効な値は以下のとおりです。

yes- 非暗号化監査を拒否します。

no- 暗号化監査と非暗号化監査を両方とも受け入れます。

デフォルト: no

RouteFile

ログ ルーティング環境設定ファイルの名前を指定します。selogrd ユーティリティの -config オプションが優先されない限り、このファイルが使用されます。

デフォルト: *ACInstallDir*/log/selogrd.cfg

SavePeriod

送信されたレコード数に関する情報を保存する時間間隔（分単位）を指定します。

デフォルト: 2

sendmail_header_format

selogrd が送信するメールのヘッダのユーザ名形式を指定します。

注: このトークンの値は、selogrd がメールを送信できない場合（つまり、syslog で selogrd のエラー 4634 が発生した場合）にのみ変更してください。

有効な値は以下のとおりです。

1 - ユーザ名の形式は *SmtpMailFrom* です。

例: eTrust_Admin

2 - ユーザ名の形式は *SmtpMailFrom@hostname* です（*hostname* は selogrd を実行するホストです）。

例: eTrust_Admin@machine

デフォルト: 1

ServicePort

ログ ルーティング機能で使用する必要がある名前またはポート番号を指定します。

指定した場合、selogrd および selogrcd は指定されたポートを使用します。指定しなかった場合、selogrd および selogrcd は RPC portmapper を使用して動的にポートを割り当てます。

トークンに値を指定した場合、selogrd および selogrcd は指定されたポートを使用します。値を指定しなかった場合、selogrd および selogrcd は RPC portmapper を使用して動的に UDP ポートを割り当てます。ログ ルーティング デーモンは通信に UDP を使用するため、サービス名に UDP ポートを指定する必要があります。

トークンの値が数字の場合は、指定されたポート番号にデーモンがバインドされます。

トークンの値がサービス名（文字列）の場合は、/etc/services または NIS サービス マップを使用して、ポート番号が解決されます。

UDP ポート/サービスに限り指定できます。

デフォルト: トークンは設定されていません（selogrd および selogrcd は RPC portmapper を使用して動的にポートを割り当てます）

SmtpMailFrom

UseSmtpMail の送信者 ID を指定します。

デフォルト: AccessControl_Admin

SmtpMailServer

リモート メール サーバ ホストのアドレスを指定します。UseSmtpMail が yes に設定された場合に、このトークンを使用します。このトークンを指定しない場合は、ローカル コンピュータがメール サーバとみなされます。

デフォルト:（空白 - ローカル サーバ）

SmtpTimeLimit

selogrd がメール サーバからの応答を待つ制限時間（秒単位）を指定します。この制限時間を過ぎると、タイムアウトします。

デフォルト: 100

tec_conf_file

selogrd デーモンが TEC イベントの作成に使用する環境設定ファイルの名前を指定します。

デフォルト: /etc/tecad_seos.conf

UseEncryption

暗号化のタイプを指定します。

有効な値は以下のとおりです。

native - CA Access Control の標準暗号化を使用します。

eTrust - adcipher で監査ログ暗号化を使用します。

no - 暗号化を使用しません。

デフォルト: no

UseSmtpMail

メールを直接送信する機能を使用するか、以前のメーラを使用するかを指定します。

デフォルト: yes

詳細情報:

seaudit ユーティリティ - 監査ログ レコードの表示 (P. 118)
selogrcd デーモン - 監査レコードの収集 (P. 317)
selogrd デーモン - 監査レコードの送出 (P. 319)

seos

[seos] セクションのトークンは、CA Access Control で使用されるグローバル設定を指定します。

admin_data

CA Access Control Security Administrator のルールおよびその他の環境設定ファイルが保存されるディレクトリを指定します。

デフォルト: *ACInstallDir*/data

auth_login

ログイン権限方法を決定します。有効な値は以下のとおりです。

Native - ログイン時に、UNIX のパスワードまたはシャドウ ファイルと照合して、ユーザのパスワードをチェックします。

eTrust - ネイティブ環境にユーザが存在していないときに、CA Access Control データベースと照合して、ユーザのパスワードをチェックします。

PAM - ネイティブ環境にユーザが存在していないときに、PAM モジュールを使用してログインをチェックします。これは、PAM がサポートされているマシンでのみサポートされます。PAM は LDAP 定義のユーザなどのユーザを検証するために使用されます。

デフォルト: native

auth_module_names

ネイティブ認証以外の認証が許可されている言語クライアント モジュールを定義します。このトークンは、認証前に lca API 呼び出しでクライアントによって設定されます。このトークンを変更すると、非ネイティブ モードで認証する他のクライアントに影響する可能性があります。

デフォルト値なし

fast_create_db

PMDB が高速なデータベース コピー デバイスを使用するかどうかを指定します。

有効な値は以下のとおりです。

no - 古いデバイスを使用します。

yes - 高速データベース コピー デバイスを使用します。

デフォルト: yes

full_year

4 桁または下 2 桁で年を表示する形式を指定します。

たとえば、このトークンを yes に設定すると、年は 00 ではなく 2000 と表示されます。

有効な値は以下のとおりです。

yes - 4 桁

no - 2 桁

このトークンは、secons -tv、dbmgr -d、および seaudit ユーティリティで生成された出力に影響します。

デフォルト: yes (4 桁)

ldap_base

CA Access Control の LDAP 対応ユーティリティ(sebuildla など)によって、LDAP ディレクトリ情報ツリー(DIT)のユーザ データ クエリの検索ベースの識別名を定義します。

たとえば、以下の形式を使用して、独自の入力内容に置換することができます。

```
o=organization_name,c=country_name
```

デフォルト: トークンは設定されていません

重要: sebuildla および必要な LDAP 設定をセットアップするには、LDAP をよく理解していること、および ldapsearch コマンドを実行できることが必要です。ldap(1)、ldapsearch(1)についての man ページ、および LDAP クライアント用のマニュアルでセットアップの説明を参照することをお勧めします。

ldap_hostname

CA Access Control の LDAP 対応ユーティリティに対して LDAP サーバが実行されているホスト名のリストを、スペース区切り形式で定義します。

デフォルト: トークンは設定されていません（localhost）

ldap_certdb_path

Netscape スタイルの証明書データベースが格納されるディレクトリを定義します。

この証明書は、SSL を介した LDAP に Netscape LDAP SDK API を使用するプラットフォーム（Solaris）での sebuildla に必要です。sebuildla が機能するには、証明書データベースに、LDAP サーバの有効な証明書が含まれている必要があります。

注: sebuildla は、サーバ認証（すなわち、クライアントなし認証）に LDAP over SSL を使用します。安全なサービスのセットアップの詳細については、PKI ツールキットのドキュメントを参照してください。

デフォルト: /.netscape

ldap_keydb

キー データベース ファイルの名前を定義します。

注: AIX のキー データベースには任意の名前を付けることができるため、この設定は AIX 用のみです（これに対し、Netscape セキュリティ データベースには、実装バージョンに応じて、certX.db や keyY.db などの名前が付けられるため、検索には ldap_certdb_path のみが必要です）。

デフォルト: トークンは設定されていません

ldap_method

CA Access Control が LDAP サービスにアクセスするために LDAP 対応ユーティリティに使用するバインド方法を指定します。

デフォルトでは、sebuildla は、すべてのセキュリティメカニズムと共に簡単な認証を使用します。簡単な認証では、ldap_userdn および対応するクレデンシャルが LDAP サーバに渡されます。sebuildla は、*ACInstallDir*/etc にある ldapcred.dat に、暗号化された形式でユーザ クレデンシャルを格納します。これらの 2 つのパラメータは、LDAP サーバに必要なアカウントとパスワードの組み合わせの近似値です。

注: SASL または TLSv.1/SSL については、LDAP サーバのマニュアルを参照してください。特定の ldap_method 設定を有効にするには、sebuildla が実行されているコンピュータにデプロイされているネイティブ LDAP クライアントで、対応するメカニズムがサポートおよび設定されている必要があります(つまり、TLS/SSL 操作では、有効な証明書が、サーバとクライアントの両方にインストールされている必要があります)。

有効な値は以下のとおりです。

0 - 標準 LDAP

1 - SASL(RFC 2222)

2 - LDAPS(SSL を介した LDAP - サーバ認証のみ)

注: ここで使用する方法により、ldap_userdn トークン、および(seldapcred ユーティリティを使用して)対応するクレデンシャルをどのように設定する必要があるかが決まります。

デフォルト: 0

ldap_port

CA Access Control の LDAP 対応ユーティリティに対して LDAP サーバのポートを定義します。このトークンは、LDAP サーバが標準 LDAP ポート(389)を使用していない場合にのみ変更する必要があります。

デフォルト: トークンは設定されていません(389)

ldap_query_size

sebuildla が各バッチ クエリで取得する LDAP エントリの最大数を定義します。

このトークンは、LDAP サーバ側のサイズ制限パラメータを変更しない場合に使用します。通常、sebuildla は 1 つのインスタンスですべてのデータを取得しようとしますが、ユーザ エントリの数が多いと、サーバのサイズ制限を超えて LDAP 操作が失敗する場合があります。ldap_query_size を設定した場合、sebuildla はすべてのエントリを取得する必要がないため、操作が失敗することはありません。ユーザ エントリの合計数が、ldap_query_size とサーバ側のサイズ制限のいずれかより大きい場合、取得されたエントリの数はこれら 2 つの設定値の低い方に対応します。

重要: バッチ クエリを有効にすると、sebuildla のパフォーマンスに影響を与える可能性があります。この設定の使用は、LDAP 環境で、DIT(ディレクトリ情報ツリー)に大量のユーザ データ(数千以上の規模のエントリ)がある場合にのみ検討してください。

注: OpenLDAP サーバ(slapd)の sizelimit パラメータなど、サーバ側の LDAP 制御の詳細については、LDAP サーバのマニュアルを参照してください。

デフォルト: トークン未設定(空)

ldap_timeout

CA Access Control の LDAP 対応ユーティリティが、LDAP サービスにバインドして LDAP 検索結果を取得するときに待機する最大時間(秒単位)を定義します。この時間を超えると、接続が終了します。LDAP サービスから情報を取得する際にかかる時間は、LDAP サービスの実行速度、および DIT に格納されているユーザ データ量によって異なります。このトークンを使用するときには、これらの点を考慮してください。

注: 検索結果が切り捨てられないようにするには、サーバ側の LDAP 制御の調整が必要になる場合もあります。たとえば、OpenLDAP サーバ(slapd)の場合、sizelimit パラメータを調整する必要があります。詳細については、LDAP サーバのマニュアルを参照してください。

デフォルト: トークンは設定されていません(15 秒)

ldap_uid_attr

LDAP DIT のユーザ名を含む属性の名前を定義します。RFC 2307（LDAP をネットワーク情報サービスとして使用するためのアプローチ）では、この属性として *uid* が定められ、それがこのトークンのデフォルト値となります。このトークンを変更すると、CA Access Control の LDAP 対応ユーティリティは、標準以外のスキーマを使用して、LDAP DIT に対して操作できます。

デフォルト: トークンは設定されていません（uid）

ldap_uidNumber_attr

LDAP DIT の UID 番号を含む属性の名前を定義します。RFC 2307 では、この属性として *uidNumber* が規定され、それがこのトークンのデフォルト値になります。このトークンを変更すると、CA Access Control の LDAP 対応ユーティリティは、標準以外のスキーマを使用して、LDAP DIT に対して操作できます。

デフォルト: トークンは設定されていません（uidNumber）

ldap_user_class

LDAP DIT のユーザ データを含むオブジェクト クラスの名前を定義します。RFC 2307 では、このオブジェクト クラスとして *posixAccount* が定められ、それがこのトークンのデフォルト値となります。このトークンを変更すると、CA Access Control の LDAP 対応ユーティリティは、標準以外のスキーマを使用して、LDAP DIT に対して操作できます。

デフォルト: トークンは設定されていません（posixAccount）

ldap_userdn

CA Access Control の LDAP 対応ユーティリティが LDAP DIT からユーザ データを取得するときに使用する、LDAP ユーザの識別名（DN）を定義します。RFC 2307 に基づき、CA Access Control は DIT で、*ou=People* レベルの属性が *uid* および *uidNumber* のユーザ データを検索しようとします。セキュリティ上の理由から、このユーザ（ldap_userdn）にのみ、このデータへのアクセス権を付与することをお勧めします。

DIT に対する匿名アクセスが許可されている場合は、このトークンを空のままにしておくことができます。匿名アクセスが許可されていない場合は、このトークンを設定し、CA Access Control の LDAP 対応ユーティリティに seldapcred ユーティリティを実行して、LDAP サービスに対して認証する必要があります（seldapcred は、暗号化されたクレデンシャルを再利用できるようにファイルに格納しているため、この操作が必要なのは一度のみです）。

たとえば、このトークンを以下のように設定します。

```
ldap_userdn = uid=user1,ou=People,dc=myCompany,dc=com
```

デフォルト: トークンは設定されていません

ldap_verbose

sebuildla でのユーザ データ取得に関して、LDAP 操作の詳細なアカウントを有効にするかどうかを指定します。

この設定は、sebuildla で LDAP データ取得を設定するとき、またはトラブルシューティングを行うときに使用します。

有効な値は、**0**（無効）、およびゼロ以外の整数（有効）です。

デフォルト: 0

locale

CA Access Control のデーモンおよびユーティリティに使用する言語を指定します。CA Access Control は、複数の言語で機能します。

対応する言語には、C、日本語、中国語（簡体字）、中国語（繁体字）などがあります。

対応するすべての言語の一覧については、/etc/ca/localeX/calocmap.txt を参照してください。Linux の場合は、*/opt/CA/SharedComponents/cawin/locale/* を参照してください。

デフォルト: C

pam_enabled

SOLARIS、HP-UX、および LINUX でのみ有効。

LDAP データベースでの認証およびパスワード変更のために、ローカル ホストで PAM を使用できるようにするかどうかを指定します。

そのために、PAM ライブラリが動的にロード可能であるかどうかを確認します（そのライブラリがシステムに存在している必要があります）。

有効な値は、「no」および「yes」です。

デフォルト: yes

parent_pmd

このコンピュータが更新を受け入れる Policy Model データベース（PMDB）のカンマ区切りリストを定義します。ローカルの CA Access Control データベースは、このリストに指定されていない PMDB からの更新情報を拒否します。

PMDB の行区切りリストを含むファイル パスを指定することもできます。

ローカルの CA Access Control データベースが PMDB からの更新情報を受け入れるようにするには、このトークンを「_NO_MASTER_」に設定します。

このトークンを設定しない場合、ローカルの CA Access Control データベースはどの PMDB からも更新情報を受け入れません。

各 PMDB は pmd_name@hostname の形式で指定します。

例:

```
parent_pmd = pmd1@host1,pmd2@host1,pmd3@host2
parent_pmd = /opt/CA/AccessControl//parent_pmdbs_file
```

デフォルト: トークンは設定されていません（データベースはどの PMDB からも更新情報を受け入れません）

passwd_pmd

sepass によるパスワードの更新情報の送信先となる PMDB を指定します。

このトークンを設定しない場合、parent_pmd トークンの値が継承されます。

形式は *pmd_name@hostname* です。

parent_pmd トークンと passwd_pmd トークンに同じ値を指定できます。parent_pmd トークンと passwd_pmd トークンの値が異なる場合、passwd_pmd データベースは更新を parent_pmd データベースに送信し、更新内容を伝達します。したがって、parent_pmd データベースは passwd_pmd データベースの子（サブスクライバ）である必要があります。

デフォルト値なし

ReverseIpLookup

接続するクライアントを seagent が識別する方法を制御します。

有効な値は以下のとおりです。

yes - クライアントの開いているソケットの IP アドレスを調べます。

no - クライアントから受け取ったホスト名を使用しますが、ホスト名は解決されません（TERMINAL クラスを無効にすると、同じ結果になる場合があります）。

デフォルト: yes

secondary_pmd

最初のターゲット（passwd_pmd）に定義されていないユーザ用に、パスワード変更の第 2 のターゲットとして使用される PMDB を指定します。

形式は *pmd_name@hostname* です。

デフォルト値なし

SEOSPATH

CA Access Control のインストール ディレクトリを指定します。

NFS がマウントされているファイル システム以外であれば、CA Access Control はどのディレクトリにでもインストールできます。

デフォルト: *ACInstallDir*

SyncUnixFilePerms

CA Access Control の ACL 権限と、ネイティブ UNIX システムの ACL およびその他の権限（存在する場合）を同期させるかどうかを指定します。

有効な値は以下のとおりです。

no - UNIX のファイル権限と CA Access Control ACL の同期をとりません。

warn - ACL 権限の同期はとりませんが、CA Access Control と UNIX の権限が競合する場合は警告を発行します。

traditional - CA Access Control ACL に従ってグループおよび所有者の rwx 権限を変更して、その他すべての場合に警告を発行します。

acl - （ACL をサポートするプラットフォーム上で）CA Access Control ACL に従ってネイティブ ファイル システムの ACL を変更します。

force - （ACL をサポートするプラットフォーム上で）traditional または acl と同様に機能するだけでなく、「他の」権限に対して defaccess を強制的にマッピングします。

注: HP-UX および Sun Solaris 2.5（以上）では、ACL ファイル システムがサポートされます。その他のプラットフォームおよびオペレーティング システムのバージョンでは、traditional 権限モードのファイルのみがサポートされます。

デフォルト: no

TNG_Environment

特別な Unicenter TNG クラスおよびリソースを使用してデータベースを作成するかどうかを指定します。

有効な値は以下のとおりです。

0 - 特別な Unicenter TNG クラスを使用せずにデータベースを作成します。

1 - 特別な Unicenter TNG クラスをすべて使用してデータベースを作成します。

デフォルト: 0

TNGDir

Unicenter TNG のインストール ディレクトリを指定します。

有効な値は、Unicenter TNG の基本ディレクトリ（または .uniprodloc）です。

デフォルト値なし

TRUEPATH

CA Access Control が物理的に格納されているディレクトリを指定します。CA Access Control ディレクトリは別の物理的な場所へのシンボリック リンクとなる場合があります。このトークンは、CA Access Control がインストールされている実際の物理的な場所を参照します。

デフォルト: *ACInstallDir*

use_rpc_protocol

RPC portmapper が必要かどうかを指定します。古い(1.43)CA Access Control のプロトコルを使用する場合は、RPC portmapper が必要です。古いプロトコルは、NIS+ パスワードの変更をサポートするために必要です。

このトークンは、old_protocol トークンに代わるものです。

有効な値は以下のとおりです。

yes - RPC portmapper を使用して、ポートを割り当てます。

no - ServicePort トークンで指定されたポートを使用します。

デフォルト: no

詳細情報:

sebuildla ユーティリティ - lookaside データベースの作成 (P. 128)
seldapcred ユーティリティ - クレデンシャルの暗号化および格納 (P. 203)
sepass ユーティリティ - パスワードの設定または変更 (P. 219)

SEOS_syscall

[SEOS_syscall] セクションのトークンは、SEOS_syscall カーネル モジュールで使用されます。

bypass_NFS

SEOS イベントの NFS ファイルを省略するかどうかを指定します。

有効な値は以下のとおりです。

0 - NFS ファイルを省略しません。
1 - NFS ファイルを省略します。

デフォルト: 0

bypass_realpath

権限付与に関して、実際のファイルのパスの解決を省略するかどうかを指定します。

この設定を有効(1)にすると、CA Access Control は権限付与に関してファイルのパスを解決しません。これによってファイル イベントの処理が促進されます。ただし、リンクを使用して実行されたファイル アクセスに対して汎用ルールは適用されません。

例: /realpath/files/* に対するアクセス拒否ルールは、この設定が有効であっても、ユーザがリンクを使用してこのディレクトリのファイルにアクセスする場合には考慮されません。このリンクに対する汎用ルールも設定する必要があります(/alternatepath/*)。

デフォルト: 0

cache_enabled

ファイルのアクセス許可を指定するために、完全パスの解決にキャッシュを使用するかどうかを指定します。

有効な値は以下のとおりです。

0 - キャッシュを使用しません。
1 - キャッシュを使用します。

デフォルト: 0

cache_rate

完全パスを解決するためにキャッシュを有効にした場合に使用する、キャッシュの割合を指定します。

値を大きくすると、キャッシュがより効果的になります。

デフォルト: 10000

call_tripAccept_from_seload

CA Access Control の開始後、seload コマンドから tripAccept を呼び出すかどうかを判断し、tripAccept が呼び出される場合は、tripAccept が接続するべきカンマ区切りの TCP/IP ポートのリストを定義して、ポートのリスナを起動します。

有効な値は任意の TCP/IP ポート番号です。さらに:

0- seload から tripAccept を呼び出しません。

制限:0 ～ 64000

デフォルト: 0

cdserver_conn_res

UnixWare 上の fiwput ルーチンで T_CONN_RES ストリームのメッセージを高優先順位のメッセージとして処理するかどうかを指定します。

有効な値は以下のとおりです。

1 - fiwput ルーチンで T_CONN_RES ストリームのメッセージを高優先順位のメッセージとして処理します。

0 - fiwput ルーチンで T_CONN_RES ストリームのメッセージを低優先順位のメッセージとして処理します。

デフォルト: 0（UnixWare では 1 になります）

debug_protect

CA Access Control の実行中にプログラムのデバッグを許可するかどうかを指定します。

有効な値は以下のとおりです。

0 - デバッグを許可します。
1 - デバッグを許可しません。

デフォルト: 1

DESCENDENT_dependent

SEOS デーモンの下位プロセスで SEOS サービスを登録できるかどうかを指定します。

有効な値は以下のとおりです。

0 - 誰でも SEOS サービスを登録できます。
1 - 下位プロセスでのみ SEOS サービスを登録できます。

デフォルト: 0

exec_read_enabled

CA Access Control カーネルがスクリプトの実行を識別するかどうか指定します。

有効な値は以下のとおりです。

0 - CA Access Control カーネルはスクリプトの実行を識別しません。

1 - CA Access Control カーネルはスクリプトの実行を識別します。

デフォルト: 0

注: 特権ユーザ パスワード管理 エージェント がエンドポイントにインストールされている場合、デフォルト値は 1 です。有効にすると、特権ユーザ パスワード管理 エージェントは指定されたシェル スクリプトを識別することができます。これらのスクリプトは、PROGRAM リソースとして定義するのではなく、特権ユーザ パスワード管理 Agent ファイル(acpwd)を使用します。

file_bypass

データベースで定義されていないファイルに対するファイル アクセスを CA Access Control でチェックするかどうかを示します。デフォルトでは、CA Access Control はデータベースで定義されていないファイルをチェックしません。

有効な値は以下のとおりです。

-1 - すべてのファイルをチェックするわけではありません。
0 - すべてのファイルをチェックします。

デフォルト: -1

GAC_root

ユーザが root である場合にファイルに対して GAC キャッシュを使用するかどうかを指定します。デフォルトでは、ユーザが root の場合に GAC は使用されません。

有効な値は以下のとおりです。

0 - root ユーザの場合はキャッシュを使用しません。
1 - root ユーザの場合にキャッシュを使用します。

デフォルト: 0

HPUX11_SeOS_Syscall_number

HP-UX 上の SEOS_syscall と通信するために、デフォルトの syscal 番号を定義します。

有効な値としては、sysent で使用されていない syscall エントリ番号があります。

デフォルト: 254

kill_signal_mask

保護対象のシグナルを定義します。

有効な値は、SEOS イベントを必要とするすべてのシグナルの論理和を取るマスク(すべてのシグナルを含むマスク)です。

デフォルト: SIGKILL、SIGSTOP、SIGTERM のいずれかのイベント。以下に示すように、実際の値はプラットフォームによって異なります。

- HP-UX: 0x804100
- Sun Solaris: 0x404100
- IBM AIX および Digital DEC UNIX: 0x14100
- Linux: 0x44100

link_protect

シンボリック リンクを保護するかどうかを指定します。

有効な値は以下のとおりです。

0 - リンクを保護しません。
1 - リンクを保護します。

デフォルト: 0

max_generic_file_rules

データベースで許可される包括的なファイル ルールの最大数を定義します。

注: 大きな数値を指定した場合、さまざまなプラットフォーム上で異常動作の原因となる可能性があります。 詳細については、当社テクニカル サポート(http://www.ca.com/jp/support/)にお問い合わせください。

有効な値は、512 以上の数値です。

注: このトークンは、AIX、HP、Linux、および Solaris でのみサポートされています。

デフォルト: 512

max_regular_file_rules

データベースで許可されるファイル ルールの最大数を定義します。

注: 大きな数値を指定した場合、さまざまなプラットフォーム上で異常動作の原因となる可能性があります。 詳細については、当社テクニカル サポート(http://www.ca.com/jp/support/)にお問い合わせください。

有効な値は、4096 以上の数値です。

注: このトークンは、AIX、HP、Linux、および Solaris でのみサポートされています。

デフォルト: 4096

mount_protect

CA Access Control が使用するディレクトリのマウントとマウント解除を許可するかどうかを指定します。

有効な値は以下のとおりです。

0 - マウントを許可します。
1 - マウントを許可しません。

デフォルト: 1

proc_bypass

ファイルがプロセス ファイル システム(/proc)に属しているときにファイル アクセスをチェックするかどうかを指定します。有効な値は以下のとおりです。

0 - トークンは無視されます。

1 - ファイル アクセス チェックを省略する

デフォルト: 1

SEOS_network_intercept_type

使用するネットワーク インターセプトの種類を指定します(HP-UX のみ)。

注: SEOS_use_streams を yes に設定する必要もあります。

有効な値は以下のとおりです。

0 - TCP フック

1 - ストリーム

デフォルト: 1

重要: このトークンは自分で変更しないでください。 詳細については、当社テクニカル サポート(http://www.ca.com/jp/support/)にお問い合わせください。

SEOS_streams_attach

実行中の STREAMS に CA Access Control が関連付けられるかどうかを指定します。

この設定を変更する場合は、ネットワークをすでに監視しているデーモンを CA Access Control で保護するために、このデーモンを再起動する必要があります。

注: この設定は、9 以前の Solaris に対してのみ適用されます。

デフォルト: yes

SEOS_unload_enabled

SEOS_syscall カーネル モジュールをアンロードできるかどうかを指定します。

有効な値は以下のとおりです。

0 - アンロードできません。
1 - アンロードできます。

デフォルト: 1

SEOS_use_ioctl

CA Access Control のカーネル モジュール通信方法(ioctl またはシステム コール)を指定します。

使用可能なシステム コール番号がオペレーティング システムによってすべて使用中の場合は、通信方法として *ioctl* を使用できます。

値: 0 - システム コール **1** - ioctl

デフォルト: 0

重要: このトークンは自分で変更しないでください。 詳細については、当社テクニカル サポート(http://www.ca.com/jp/support/)にお問い合わせください。

SEOS_use_streams

ネットワーク インターセプトに streams サブシステムを使用するかどうかを指定します(SEOS_load が streams にモジュールを自動的にプッシュするかどうか)。

この設定は、HP-UX と Sun Solaris のバージョン 8 および 9 でのみ使用できます。

デフォルト: no

silent_admin

メンテナンス ユーザのユーザ ID を定義します。このユーザのアクティビティは、セキュリティが停止し、silent_deny が *yes* のときに許可されます。数字で構成されるユーザの UNIX UID を使用して、メンテナンス ユーザを定義します。

デフォルト: 0(root のユーザ ID)

silent_deny

セキュリティが停止しているときにイベントを拒否するかどうかを指定します。

有効な値は以下のとおりです。

yes - silent deny が有効です(メンテナンス モード)。

no - silent deny が無効です。

デフォルト: no

STAT_intercept

stat システム コールが発生したときにファイル アクセスをチェックするかどうかを指定します。

1(ファイル アクセスをチェック)を指定した場合、*read* 権限を持たないユーザは、ファイルに関する情報を取得する操作を実行できません。また、監査ログに記録されているレコードを読み取ることもできません。これを 0 に指定した場合、どのユーザでもファイル情報を取得できます。

値: 0(ファイル アクセスをチェックしません)、1(ファイル アクセスをチェックします)。

デフォルト: 0

STOP_enabled

STOP 機能を使用するかどうかを指定します。これは、スタック オーバーフロー攻撃から保護する機能です。

有効な値は以下のとおりです。

0 - オフ。
1 - オン。

デフォルト: 0

synchronize_fork

fork 同期を管理する方法を指定します。

HP-UX プラットフォームの場合

1 - 親から fork をレポートします。
2 - 子から fork をレポートします。

他のプラットフォームの場合

1 - 親から同期せずにレポートします。
2 - 親から同期してレポートします（Linux ではサポートされていません）。

制限: 1 未満のどんな値も 1 として解釈されます。1 を超えるどんな値も 2 として解釈されます。

注: さまざまなプラットフォーム上で異常動作の原因となる可能性があるため、この設定は変更しないでください。

デフォルト: 1

syscall_monitor_enabled

CA Access Control コードを実行しているプロセスを CA Access Control が監視するかどうかを指定します。監視を有効にしている場合（デフォルト）は、*secons -sc* または *secons -scl* を使用してこれらのプロセスを表示できます。

有効な値は以下のとおりです。

0 - 非アクティブ

1 - アクティブ

デフォルト: 1

threshold_time

インターセプトされたシステム コールを危険であると判断されるまでにブロックできる時間（秒）を定義します。プロセスがこの時間よりも長い時間ブロックされた場合は、CA Access Control は SEOS_syscall モジュールのアンロードに失敗する可能性があることを報告します。

注: この値は、CA Access Control が提供するアンロードの準備状況レポートに影響します。詳細については、「*エンタープライズ管理ガイド*」を参照してください。

デフォルト: 60

trace_enabled

SEOS_syscall の循環トレース バッファを使用するかどうかを指定します。

有効な値は以下のとおりです。

0 - トレースを使用しません。
1 - トレースを使用します。

デフォルト: 0

use_tripAccept

SEOS_syscall をアンロードして、ブロックされている受け入れシステム コールのブロックを解除するときに、tripAccept ユーティリティを使用するかどうかを指定します。これにより、モジュールがアンロードされた後に、SEOS_syscall コードが実行されなくなります。

有効な値は、yes および no です。

デフォルト: yes

seosd

[seosd]セクションのトークンは、パフォーマンスを向上させるために、認証デーモンおよびキャッシュ ユーティリティの動作を指定します。

bypass_filenames

seos イベントから除外されるファイル名のリストを含むファイルを指定します。

たとえば、bypass_filenames = /opt/CA/AccessControl//bin/bypass_filenames のように指定します。

デフォルト: トークンは設定されていません

bypass_nfs_port

CONNECT のために NFS が使用するポート(ポート 2049)をバイパスするかどうかを指定します。このバイパスが存在することで、NFS が正常に機能します。

このトークンの値を *no* に変更すると、このポートではバイパスは行われません。このバイパスを置き換えるために必要な CA Access Control ルールを忘れずに指定してください。そのようなルールの例を以下に示します(例のとおりには使用 *できません*)。

```
nr hostnet all mask (0.0.0.0) match(0.0.0.0)
nr TCP 2049 owner(nobody) defaccess(none)
authorize TCP 2049 hostnet(all) access(w) uid(root)
nr TCP nfsd owner(nobody) defaccess(none)
authorize TCP nfsd hostnet(all) access(w) uid(root)
```

注: このトークンの値を *no* に指定しても、正しい CA Access Control ルールを指定しない場合、NFS は機能を停止します。

デフォルト: yes

bypass_outgoing_TCPIP

カンマで区切られたポートのリストを定義します。このポートに対して、seos_syscall は seosd への外部接続イベントを渡しません。

デフォルト: トークンは設定されていません

bypass_suid_for_login

ダミーの SUID システム コールを無視する必要のあるログイン プログラムのパスを指定します。

ダミーの SUID システム コールを大量に生成する一部のログイン プログラム(samba など)の場合に使用します。これらのシステム コールにより、ログインしているユーザの正しい認識が妨げられる可能性があります。

デフォルト: none

bypass_suid_program

複数の su コマンドを許可します。一部のプラットフォームでは、システムの su プログラムの動作が標準とは異なります。root 以外のユーザに対して su コマンドが要求された場合は、要求されたユーザに対して su が実行される前に、root ユーザに対して su が実行されます。

root ユーザに対して CA Access Control の代理要求保護が設定されている場合は、root 以外のユーザに対して su コマンドを正常に実行できない可能性もあります。

このようなプラットフォームで root ユーザに対して代理要求保護を使用し、さらに割り込みなしで root 以外のユーザに su を実行できるようにするには、bypass_suid_program トークンにシステムの su プログラムの実在パスを含めるように設定します。

デフォルト: none

bypass_system_files

CA Access Control の認証エンジンが、/etc/passwd や /etc/group などのシステム ファイルでは、読み取りアクセスをバイパスするかどうかを指定します。

有効な値は以下のとおりです。

yes - システム ファイルに対する読み取りアクセスをバイパスします。

no - システム ファイルに対する読み取りアクセスをバイパスしません。

デフォルト: yes

bypass_TCPIP

seos_syscall が seosd にイベントを渡さないようにカンマで区切り、1 つ以上のポートを追加できるようにします。

構文は bypass_TCPIP=*port1*[,*port2*,*portx*] です。

デフォルト: トークンは設定されていません

bypass_xdm_ports

CONNECT のために XDM が使用するポート(ポート 6000 ～ 6010)をバイパスするかどうかを指定します。このバイパスが存在することで、XDM が正常に機能します。

このトークンの値を *no* に変更すると、これらのポートではバイパスは行われません。このバイパスを置き換えるために必要な CA Access Control ルールを忘れずに指定してください。そのようなルールの例を以下に示します(例のとおりには使用 *できません*)。

```
nr hostnet all mask (0.0.0.0) match(0.0.0.0)
nr TCP X-Win owner(nobody) defaccess(none)
authorize TCP X_Win hostnet(all) access(r)
authorize TCP X_Win hostnet(all) access(w) uid(root)
authorize TCP X_Win hostnet(all) access(w) gid(mygroup)
nr TCP 6000 owner(nobody) defaccess(none)
authorize TCP 6000 hostnet(all) access(r)
authorize TCP 6000 hostnet(all) access(w) uid(root)
authorize TCP 6000 hostnet(all) access(w) gid(mygroup)
```

注: このトークンの値を *no* に指定しても、正しい CA Access Control ルールを指定しない場合、XDM は機能を停止します。このトークンの値が *yes* で外部接続がポート 6000 ～ 6010 経由で確立されている場合、対応する監査レコード内のクラス名は TERMINAL です。

デフォルト: yes

cron_program

seosd での cron ログインに対するチェックを強化します。

cron_program トークンにシステムの cron プログラムの実在パスを含めるように設定します。

デフォルト: none

dbdir

CA Access Control データベースの場所を指定します。

デフォルト: *ACInstallDir*/seosdb

device_file

/dev ですべてのデバイスをスキャンするかどうかを指定します。

このトークンの値が Yes に設定され、tty が標準のリストで見つからない場合、CA Access Control は /dev にあるすべてのデバイスをスキャンします

（qplib は、標準デバイスから tty 名を解決します）。

注: tty 名のリストにデバイスを追加できます。

デフォルト: no

dns_server

DNS サーバ名を指定します。この名前は、デフォルト サーバから別のサーバにホスト名解決を変更するために使用します。

このトークンは、通常、DNS キャッシュ オプションが有効な場合に使用します。

デフォルト: none

domain_names

完全修飾名を作成するために、承認の目的で受け取る短いホスト名に対して、seosd が追加するドメイン名のリストを指定します。その結果、これらの名前には、関連する HOST クラス、CONNECT クラス、TERMINAL クラスで権限が与えられます。

完全名を識別するために、seosd は短い名前に domain_names リストのドメイン名を追加して承認に使用します。

seosd はまず、短い名前のみを使用してデータベース内の関連するルールを検索します。短い名前に一致するレコードが見つからない場合、domain_names トークンで指定された各ドメイン名を 1 つずつ追加して、一致するレコードが見つかるまで検索を続けます。

たとえば、次のリストを domain_names に割り当てるとします。

domain_names = market.com, journey.com, total.com

データベースにルールとして定義されていない *acme* というサブスクライバから要求を受け取った場合、seosd はこの要求を以下のように処理します。

acme (not found in database)
acme.market.com (not found)
acme.journey.com (not found)
acme.total.com (found)

seosd は一致した最初のレコード（この例では acme.total.com）を承認に使用します。

デフォルト値: /etc/resolv.conf に定義されているとおり

EnablePolicyCache

権限に必要なデータベース値を格納するために、実行時テーブルを使用するかどうかを指定します。この実行時テーブルは、seosd を起動したときにメモリにロードされます。これにより、データベースに接続しなくなるため、権限付与に要する時間が短縮されます。

有効な値は、yes および no です。

デフォルト: no

enf_register

Unicenter NSM Event Notification Facility（ENF）に登録するかどうかを指定します。

有効な値は以下のとおりです。

yes - ENF に登録します。

no - enf に登録しません。

デフォルト: no

FileCache_auths

キャッシュが有効になっている場合、権限プールのレコード数を指定します。キャッシュできる権限レコードの最大数は 800 です。

デフォルト: 80

FileCache_CleanInt

ファイル キャッシュを削除する頻度（分単位）を指定します。

デフォルト: 60

FileCache_files

キャッシュが有効になっている場合、ファイル プールのレコード数を指定します。キャッシュできるファイル レコードの最大数は 200 です。

デフォルト: 20

FileCache_InitPrio

キャッシュ テーブル内にある新規レコードの優先順位の初期値を指定します。

デフォルト: 10

FileCache_PriorInt

キャッシュが有効になっている場合、キャッシュ テーブル内の優先順位を再計算する頻度を指定します。新規レコードを保存するたびに、1 回としてカウントされます。

デフォルト: 1

FileCache_users

キャッシュが有効になっている場合、ユーザ プールのレコード数を指定します。キャッシュできるユーザ レコードの最大数は 500 です。

デフォルト: 50

get_login_terminal

seosd が別の方法でログイン プログラムのピア アドレスの検索を試みるかどうかを指定します。これは、ssh などの接続に有用です。

有効な値は、yes および no です。

デフォルト: yes

grace_admin

管理者がユーザのパスワードを変更する際に設定される猶予ログイン回数を指定します。

デフォルト: トークンは設定されていません（1）

GroupidResolution

CA Access Control で GID 番号をグループ名に変換する方法を指定します。

有効な値は以下のとおりです。

system - CA Access Control は、システム コールを使用して gid 番号を変換します。この値はスタンドアロン端末、DNS クライアント端末、および DNS サーバ端末に使用できます。（この表の resolve_timeout トークンも参照してください）。

cache - gid 番号およびグループ名を seosd にキャッシュします。これは最も速く簡単な変換方法ですが、実行時にはキャッシュを更新できません。

ladb - CA Access Control は、lookaside データベースを使用して gid 番号を変換します。関連するトランザクション テーブルが更新されるたびに、sebuildla ユーティリティを実行して lookaside データベースを再作成する必要があります。

NIS サーバおよび NIS+ サーバの場合は、cache または ladb を指定できます。

Sun Solaris 2.5 以上、および HP-UX 11.x の場合は、cache または ladb を指定できます。

どの端末の場合も、ladb を指定することをお勧めします。

デフォルト: トークンは設定されていません（system）

HostResolution

CA Access Control で IP アドレスをホスト名に変換する方法を指定します。

有効な値は以下のとおりです。

system - CA Access Control は、システム コールを使用して IP アドレスを変換します。この値はスタンドアロン端末、NIS/NIS+ クライアント端末、および DNS クライアント端末に使用できます（この表の resolve_timeout トークンも参照してください）。

cache - ホスト名およびその IP アドレスを seosd にキャッシュします。これは最も速く簡単な変換方法ですが、実行時にはキャッシュを更新できません。

ladb - CA Access Control は、lookaside データベースを使用して IP アドレスを変換します。関連するトランザクション テーブルが更新されるたびに、sebuildla ユーティリティを実行して lookaside データベースを再作成する必要があります。

NIS サーバ、NIS+ サーバ、および DNS サーバの場合は、cache または ladb を指定できますが、ladb を指定することをお勧めします。

デフォルト: トークンは設定されていません（system）

IsolatedDaemon

ファイル記述子（stdin、stdout、および stderr）がデーモンになるときに、seosd がこれらのファイル記述子を閉じるかどうかを指定します。

有効な値は以下のとおりです。

yes - ファイル記述子がデーモンになるときに、seosd はこれらのファイル記述子を閉じます。

no - ファイル記述子がデーモンになるときに、seosd はこれらのファイル記述子を閉じません。

デフォルト: no

kill_ignore

CA Access Control の 3 つの主なデーモンのいずれかに対して実行された「kill -9」コマンドを無視（拒否）するかどうかを指定します。有効な値は以下のとおりです。

yes - kill コマンドを無視します。デフォルト値です。

no - kill コマンドによって seosd が終了します。

デフォルト: yes

login_parent_check

（子プロセスがログインした後）親プロセスがログイン シーケンスを続行するか、そのシーケンスを中止して子からログインを継承するかを指定します。

有効な値は 0 または 1 です。

0 の場合は、親プロセスがログイン シーケンスを続行します。

1 の場合は、親プロセスがログイン シーケンスを中止して子からログインを継承します。

デフォルト: トークンは設定されていません（0）

lookaside_allowdupuid

sebuildla で重複した UID を登録するかどうかを指定します。

有効な値は以下のとおりです。

yes - 重複した UID を登録します。

no - UID が重複している場合は、その UID を 1 つだけ登録します。

注: UID が重複していると、UNIX OS で整合性が失われる場合があります。

デフォルト: no

lookaside_path

lookaside データベースが格納されるディレクトリを指定します。このディレクトリを作成した後に、sebuildla ユーティリティを実行します。

注: lookaside データベース ファイルは、sebuildla ユーティリティを使用して作成および更新されます。

デフォルト: *ACInstallDir*/ladb

max_loggedin_users

ログイン ユーザの最大数を定義します。

注: この値によって、内部メモリ テーブルのうちの 1 つのサイズが決定します。テーブルが大きいほど、より多くのメモリを消費します。

制限:4096 ～ 20480

デフォルト: 8192

MultiLoginPgm

複数のログインを実行するプログラムの名前および完全パスを定義します。このトークンは、これらの特殊なログイン アプリケーションの正しいログイン シーケンスを検出するために使用されます。

MultiLoginPgm は、完全パスを含むログイン アプリケーション名です。

デフォルト: none

network_cache_timeout

ネットワーク キャッシュを使用する場合にネットワーク キャッシュ テーブルを空にする時間間隔(分単位)を指定します。このトークンは、格納されて受け入れられた TCP 着信要求に時間制限を設定するために使用します。

注: ネットワーク キャッシュの使用の詳細については、「*UNIX 版エンドポイント管理ガイド*」を参照してください。

デフォルト: 10

nfs_devices

NFS メジャー デバイス番号が格納されるファイルの名前およびパスを指定します。ファイルは、完全パスで指定します。

CA Access Control では、デバイスおよび i-node を使用し、さらに名前を使用しても、プログラムを取得することに失敗した場合にこのファイルを使用します。このファイルには、各プラットフォームの NFS メジャー デバイス番号のデフォルト値が格納されます。この値はシステムによって異なる場合があります。ご使用のシステムでの番号を確認するには、UNIX getmajor() 機能を含む小規模なプログラムを使用してください。次に、nfsdevs.init ファイル(またはこのトークンにちなんだ名前を付けたファイル)を編集して、確認した番号を格納します。

注: NFS システムをマウントおよび再マウントするたびに、nfsdevs.init ファイルを更新する必要があります。また、デバイスの最初の 4 桁のみを使用することもできます。この数値は、システムをマウント解除および再マウントする場合も変わりません。

デフォルト: *ACInstallDir*/etc/nfsdevs.init

protect_bin

seosd で CA Access Control のバイナリ ファイルを保護するかどうかを指定します。以下のいずれかの値を指定します。

yes - このようなアクセスを許可するルールが定義されていない限り、CA Access Control のバイナリ ファイルを保護します。

注: FILE クラスのレコードの _default アクセス権が none のときは、yes を指定しないでください。指定した場合、すべての /opt/CA/AccessControl//bin ファイルに FILE クラスのレコードがあるとき以外はファイルにアクセスできず、CA Access Control を使用できなくなります。

no - CA Access Control のバイナリ ファイルを保護しません。

デフォルト: no

resolve_rebind

タイムアウト障害後に、seosd で NIS サーバへの接続を再確立するかどうかを指定します。

デフォルト値は変更しないことを強くお勧めします。

デフォルト: yes

resolve_timeout

IP をアドレスに、ユーザ ID をユーザ名に、グループ ID をグループ名に、サービス ポート番号をサービス名にそれぞれ変換することを seosd が試みる最長時間(秒単位)を指定します。

この値は以下の 2 つの場合に有効になります。

seosd がシステム解決を使用している場合 (HostResolution トークン、ServiceResolution トークン、UseridResolution トークン、および GroupidResolution トークンを参照してください)。

under_NIS_server トークンが no に設定されている場合。

指定された時間が経過しても解決できない場合、seosd は指定された IP、ID、またはポートに解決の手段が存在しないとみなします。

この値を 0(ゼロ)に設定すると、タイムアウトは設定されません。

デフォルト: 5

rt_priority

seosd にリアルタイムの優先順位があるかどうかを指定します。

有効な値は、yes および no です。

このトークンが yes に設定された場合、seosd にはリアルタイムの優先順位が与えられます。

デフォルト: yes

ServiceResolution

CA Access Control で TCP ポート番号をサービス名に変換する方法を指定します。

有効な値は以下のとおりです。

system - CA Access Control は、システム コールを使用して TCP ポート番号を変換します。この値はスタンドアロン端末、NIS/NIS+ クライアント端末、DNS クライアント端末、および DNS サーバ端末に使用できます。(この表の resolve_timeout トークンも参照してください)。

cache - サービス名およびその TCP ポート番号を seosd にキャッシュします。これは最も速く簡単な変換方法ですが、実行時にはキャッシュを更新できません。

ladb - CA Access Control は、lookaside データベースを使用して TCP ポート番号を変換します。 関連するトランザクション テーブルが更新されるたびに、sebuildla ユーティリティを実行して lookaside データベースを再作成する必要があります。

NIS サーバおよび NIS+ サーバの場合は、cache または ladb を指定します。

デフォルト: system

sim_login_timeout

アクセサ エレメント エントリ テーブル(ACEE)から、未使用の仮想ログイン ユーザ エントリを CA Access Control が削除するまでのタイムアウト(分単位)を定義します。

CA Access Control は、ACEE に格納されている情報にアクセスする必要があるときに、仮想ログインを実行して ACEE エントリを作成します。

デフォルト: 60

special_check

カーネル モジュールのロード時に、ファイル パスのチェックを有効にするかどうかを指定します。有効にした場合、CA Access Control は、ロードするカーネル モジュールが、Linux 以外のシステムでは KMODULE レコードの filepath プロパティと一致しているかどうかをチェックし、Linux システムでは KMODULE レコードのシグネチャと一致しているかどうかをチェックします。

デフォルト: no

terminal_default_ignore

管理アクセスを許可するときに、_default TERMINAL レコードおよび特定の TERMINAL レコードの defaccess 値を考慮するかどうかを指定します。

有効な値は、yes および no です。

yes - 管理アクセスでは、_default TERMINAL レコードおよび特定の TERMINAL レコードの defaccess 値を無視します。この場合、管理アクセスでは、関連する特定の TERMINAL レコードの明示的な権限ルールが必要です。

no - 管理アクセスでは、_default か特定かに関係なく、関連するすべての TERMINAL レコードの defaccess 値を考慮します。

デフォルト: yes

terminal_search_order

定義済みの TERMINAL を、IP アドレスよりも前に名前でチェックするかどうかを指定します。

有効な値は以下のとおりです。

name - TERMINAL は、IP アドレスよりも前に名前でチェックされます。

ip - TERMINAL は、名前よりも前に IP アドレスでチェックされます。

注: TERMINAL クラスは、ワイルドカードで定義された包括的なルールをサポートしています(IP アドレスまたはホスト名のパターンの一致)。包括的なルールは *常に*、特定(フルネーム)のルールの後にチェックされます。たとえば、これを *ip* に設定した場合、IP アドレスの完全一致、ホスト名の完全一致、IP アドレスのパターン一致、ホスト名のパターン一致の順で seosd は TERMINAL リソースを探します。

デフォルト: name

trace_file

トレース メッセージが要求される場合、トレース メッセージの送信先ファイルの名前を指定します。

デフォルト: *ACInstallDir*/log/seosd.trace

trace_file_type

トレース ファイルにバイナリ フォーマットで書き込むか、テキスト フォーマットで書き込むかを指定します。

有効な値は以下のとおりです。

binary - トレース ファイルはバイナリ フォーマットで書き込まれます。このオプションにより、このファイルが占有する領域は小さくなります。

text - トレース ファイルはテキスト フォーマットで書き込まれます。

seosd デーモンは、このトークンの値をチェックして、トレース ファイルの内容と比較します。トークンの値がトレース ファイルのフォーマットと一致しない場合は、トレース ファイル名に拡張子 .backup が付加されて保存されます。

デフォルト: text

trace_filter

フィルタ データを保存するファイルの名前およびパスを指定します。フィルタ データは、トレース メッセージのフィルタ処理に使用されます。

デフォルト: *ACInstallDir*/data/*language*/etc/trcfilter.init

trace_space_saver

ファイル システムに確保する空き容量(MB 単位)を指定します。空き容量がこの数値を下回ると、CA Access Control ではトレースは無効になります。

注: 使用可能な容量が後で増えた場合でも、トレースは自動的には有効になりません。

デフォルト: 512

trace_to

トレース メッセージの送信先を指定します。

有効な値は以下のとおりです。

file - CA Access Control は、trace_file トークンによって指定されたファイルにトレース メッセージを送信します。トレースを無効にするには、*secons -t-* コマンドを使用します。詳細については、この表の trace_file トークンの説明を参照してください。

file,stop - CA Access Control は、デーモンの初期化時にトレース メッセージを生成します。デーモンが初期化された後は、トレース メッセージの生成は停止します。

none - CA Access Control は、トレース メッセージを発行しません。これは CA Access Control をインストールして実装した後の標準設定です。

注: トークンを **file** または **file,stop** に設定した場合、CA Access Control のトレースは、-t オプションを指定した secons コマンドで切り替えることができます。

デフォルト: file, stop

UpdSurrogLogin

代理ログインにおいて、CA Access Control がユーザの最終アクセス日時を更新するかどうかを指定します。

有効な値は以下のとおりです。

1 - 代理ログインにおいて、CA Access Control がユーザの最終アクセス日時を更新するように指定します。

0 - 代理ログインにおいて、CA Access Control がユーザの最終アクセス日時を更新しないように指定します。

Undef_ForPacl

PACL でアクセサの名前にアスタリスク(*)が含まれている場合、未定義のユーザを seosd でチェックするかどうかを指定します。

有効な値は以下のとおりです。

1 - seosd は、アスタリスクが付いた未定義のユーザを PACL に含めません。

0 - seosd は、アスタリスクが付いた未定義のユーザを PACL に含めます。

デフォルト: 0

under_NIS_server

seosd がシステムの名前解決ではなく、内部の名前解決を使用するかどうかを指定します。

有効な値は以下のとおりです。

yes - seosd は、起動時にすべてのユーザ、グループ、およびポート番号の情報をメモリまたは lookaside データベースに格納します（user_lookaside トークンを参照してください）。

この値は、NIS、NIS+、DNS サーバ マシンの場合、およびオペレーティング システムが Sun Solaris 2.5 以上、HP-UX 11.x、IBM AIX 4.3.x、IRIX 6.5 の場合に必要です。

重要： NIS サーバまたは上記オペレーティング システムのいずれかの場合、トークンを無効にするとコンピュータが停止することがあります。

no - seosd は、システムの名前解決を使用して resolve_timeout トークンを有効にします。

注: このトークンには、インストール時に値が自動的に割り当てられます。

このトークンは、旧バージョンとの互換性を維持するためにのみ残されています。初めて CA Access Control をインストールするか、またはバージョン 2 以上をインストールする場合は、このトークンではなく、HostResolution トークン、ServiceResolution トークン、UseridResolution トークン、および GroupidResolution トークンを使用してください。

デフォルト: インストール時に割り当てられます

use_lookaside

seosd がユーザ、グループ、ホスト、およびポート番号を lookaside データベースまたはメモリのどちらに格納するかを指定します。

注: このトークンは、under_NIS_server トークンと組み合わせて使用します。under_NIS_server トークンを yes に設定しない限り、有効になりません。

有効な値は以下のとおりです。

yes - seosd は、ユーザ、グループ、ホスト、およびサービスの詳細に lookaside データベースを使用します。lookaside データベースは、sebuildla ユーティリティによって作成され、このユーティリティを使用していつでも更新できます。

lookaside データベースの場所は、lookaside_path トークンで指定します。

no - seosd は、起動時にすべてのユーザ、グループ、ホスト、およびサービスの情報をキャッシュします。そのため、すべての変換はメモリ内で実行できます。seosd を毎日再起動してキャッシュを更新することをお勧めします。

このトークンは、旧バージョンとの互換性を維持するためにのみ残されています。初めて CA Access Control をインストールするか、またはバージョン 2 以上をインストールする場合は、このトークンではなく、HostResolution トークン、ServiceResolution トークン、UseridResolution トークン、および GroupidResolution トークンを使用してください。

デフォルト: no

use_mapped_user_name

(CA Access Control と UNIX 認証ブローカ の両方がインストールされている場合、有効) seosd が監査レコード内でユーザ エンタープライズ名を使用するかどうかを指定します。

値: yes、no

デフォルト: no

use_nfs_devices

NFS デバイスを使用するかどうかを指定します。有効な値は、yes および no です。

デフォルト: Yes

use_standard_functions

NIS 環境での sebuildla によるユーザの取得を、標準のシステム機能 getpwent を呼び出して行うか、または ypcat passwd コマンドおよび cat /etc/passwd コマンドの出力を解析して行うかを指定します。

有効な値は以下のとおりです。

yes - 標準のシステム機能 getpwent を使用します。

no - ypcat passwd コマンドおよび cat /etc/passwd コマンドの出力の解析を使用します。

デフォルト: yes

use_trusted_script

seosd が trusted スクリプト メカニズムを使用するかどうかを指定します。

trusted スクリプト メカニズムを使用すると、シェル スクリプト内から呼び出されたプログラムは、CA Access Control の内部テーブルにシェル スクリプトの名前を保持します。

つまり、スクリプトが PACL で使用される場合、これらのプログラムはその権限を継承します。また、CA Access Control を使用してこれらのプログラムを保護することはできません。

trusted スクリプトの最初の行は、#! で始まります。

trusted スクリプト メカニズムを使用**しない**場合、これらのプログラムは、CA Access Control の内部テーブルに独自の名前で登録されます。

デフォルト: yes

use_unab_db

(CA Access Control と UNIX 認証ブローカ の両方がインストールされている場合、有効) 現在の方法でユーザおよびグループ名を解決できない場合、seosd が UNIX 認証ブローカ データベースを使用して解決するかどうかを指定します。このトークンは次のトークンと一致します。use_lookaside、UseridResolution、GroupidResolution。

値: yes、no

デフォルト: no

UseFileCache

パフォーマンス向上のために、ファイル レコードに対してキャッシュ ツールを使用するかどうかを指定します。

デフォルト: yes

UseNetworkCache

CA Access Control で受け入れた TCP 着信要求をキャッシュするかどうかを指定します。

注: ネットワーク キャッシュの使用の詳細については、「*UNIX 版エンドポイント管理ガイド*」を参照してください。

有効な値は、yes および no です。

デフォルト: no

UseridResolution

CA Access Control で UID 番号をユーザ名に変換する方法を指定します。

有効な値は以下のとおりです。

system - CA Access Control は、システム コールを使用して uid 番号を変換します。この値はスタンドアロン端末、NIS/NIS+ クライアント端末、DNS クライアント端末、および DNS サーバ端末に使用できます。

cache - ユーザ名およびその uid 番号は seosd にキャッシュされます。これは最も速く簡単な変換方法ですが、実行時にはキャッシュを更新できません。

ladb - CA Access Control は、lookaside データベースを使用して uid 番号を変換します。関連するトランザクション テーブルが更新されるたびに、sebuildla ユーティリティを実行して lookaside データベースを再作成する必要があります。

オペレーティング システムが NIS サーバ、NIS+ サーバ、Sun Solaris 2.5 以上、または HP-UX 11.x の場合は、cache または ladb を指定する必要があります。

デフォルト: system

watchdog_refresh

ファイル ハンドルごとに特権プログラムと保護対象ファイルをスキャンするために、Watchdog の更新を seosd が実行するかどうかを指定します。

有効な値は以下のとおりです。

yes - seosd は、Watchdog を更新します。

no - seosd は、Watchdog を更新しません。

デフォルト: no

seosdb

[seosdb] セクションのトークンは、データベースのチェックおよび再構築を管理します。

CheckAlways

CA Access Control の初期化時にデータベースの破損をチェックするかどうかを指定します。

有効な値は、yes および no です。

デフォルト: yes

CheckProgram

データベースをチェックするための内部コードの代わりに使用するコマンドの完全パスおよびパラメータを指定します。データベースが有効であればコマンドは 0 を返し、修正が必要であればゼロ以外の数値を返します。

デフォルト: トークンは設定されていません（*dbmgr -u -fast* を使用した場合と同様に、プログラムを実行しません）

CreateNewClasses

seclassadm ユーティリティを使用して作成した新しいクラスをデータベースに追加できるかどうかを指定します。

有効な値は、yes および no です。

デフォルト: yes

CreateNewProps

CA Access Control の sepropadm ユーティリティがデータベースのプロパティを新規作成したときに、新規のプロパティに関するデータをファイルに保存するかどうかを指定します。

有効な値は、yes および no です。

yes の場合、sepropadm は新規のプロパティに関するデータをファイルに保存します。また、後から dbmgr -c ユーティリティが新規の CA Access Control データベースを生成すると、dbmgr はこのファイルを使用して、これらのプロパティをデータベースに追加します。

デフォルト: yes

RebuildAlways

CA Access Control の初期化時に CA Access Control データベースを常に再構築するかどうかを示します。

有効な値は、yes および no です。

デフォルト: no

RebuildProgram

データベースを修正するための内部コードの代わりに使用するコマンドの完全パスおよびパラメータを指定します。

デフォルト: トークンは設定されていません（*dbmgr -u -build all* を使用した場合と同様に、プログラムを実行しません）

seoswd

[seoswd] セクションのトークンは、Watchdog 機能の動作を指定します。

BlockingInterval

watchdog がメイン デーモンからの応答を待機する間隔を秒単位で指定します。この時間を経過すると、watchdog はメイン デーモンに信号を送信します。

デフォルト: 60

IgnoreScanInterval

特定の間隔でプログラムおよびファイルのスキャンを実行するかどうかを指定します。

Watchdog は、トークンの値が no の場合は一定の間隔でスキャンを実行し、yes の場合はスキャンを実行しません。

注: PgmTestTime トークンまたは SecFileTestTime トークンでスキャン時刻を指定していない場合は、このトークンを yes に設定しても、Watchdog は trusted プログラムまたは保護対象ファイルをスキャンしません。

デフォルト: no

PgmRest

最後のイベントの後からプログラムの再チェックの前までの期間を秒単位で指定します。チェック プログラムは、システムの過負荷を防止するために休止します。

デフォルト: 10

PgmTestInterval

trusted プログラムの再スキャンを実行する時間間隔（秒単位）を指定します。

注: この値が 1 日（86400 秒）以上の場合は、IgnoreScanInterval がデフォルト値の *yes* になります。

デフォルト: 18000（5 時間）

PgmTestStartTime

trusted プログラムの初回スキャンの開始時刻を *hh*:*mm* 形式で指定します。

このトークンを設定しない場合、Watchdog は起動後ただちに初回のスキャンを実行します。

デフォルト値なし

PgmTestTime

trusted プログラムの固定スキャン時刻を *hh:mm* 形式で指定します。複数のスキャン時刻を指定する場合は、スペースで区切ります。

注意: スキャン時刻を指定せず、IgnoreScanInterval トークンを yes に設定した場合、Watchdog は trusted プログラムのスキャンを実行しません。

デフォルト値なし

policyfetcher_refresh_interval

policyfetcher デーモンの実行を確認する間隔を秒単位で指定します。

デフォルト: 600

RefreshParams

seos.ini のトークンの Watchdog が連続して読み取りを実行する時間間隔（秒単位）を指定します。

デフォルト: 86400（1 日）

SecFileRest

最後のイベントの後からセキュリティで保護されたファイルの再チェックまでの期間を秒単位で指定します。Watchdog は、システムの過負荷を防止するために休止します。

注: スキャン時刻を指定せず、IgnoreScanInterval トークンを yes に設定した場合、seoswd は保護対象プログラムのスキャンを実行しません。

デフォルト: 10

SecFileTestInterval

保護対象ファイルの再スキャンを実行する時間間隔(秒単位)を指定します。

デフォルト: 36000(10 時間)

SecFileTestStartTime

保護対象ファイルの初回スキャンの開始時刻を *hh*:*mm* 形式で指定します。

値を指定しない場合、Watchdog は CA Access Control デーモンの起動後ただちに初回のスキャンを実行します。

デフォルト値なし

SecFileTestTime

保護対象ファイルの固定スキャン時刻を *hh:mm* 形式で指定します。複数のスキャン時刻を指定する場合は、スペースで区切ります。

デフォルト値なし

SeosAYT

Watchdog が seosd デーモンをチェックする時間間隔(秒単位)を指定します。

重要: 管理者に相談せずに、このトークンに不適切な値を指定すると、CA Access Control の動作に重大な問題が生じるおそれがあります。 詳細については、当社テクニカル サポート(http://www.ca.com/jp/support/)にお問い合わせください。

デフォルト: 60

SignalMinInterval

システムの過負荷を防ぐために、HUP シグナルでオン デマンドの 1 回かぎりのスキャンの実行間隔を秒で指定します。

注: オン デマンドのスキャンは、trusted プログラムおよび保護対象ファイルの両方で実行されます。

デフォルト: 60

UnTrustMissing

Watchdog でプログラムまたはファイルが見つからない場合（たとえば、ファイルが削除されたか、関連する NFS パーティションがマウントされていない場合）でも、プログラムまたはファイルを untrusted にしようとするかどうかを指定します。

有効な値は以下のとおりです。

yes - 存在しないファイルを untrusted にします。

no - 存在しないファイルを untrusted にしません。

デフォルト: yes

unab_check_enabled

認証デーモンを保護するかどうかを指定します。

値: yes、no

デフォルト: no

unab_refresh_interval

認証デーモンの実行を確認する間隔を秒単位で指定します。

デフォルト: 600

VerifyCtime

trusted プログラムおよび保護対象ファイルのファイル ステータス最終変更日時を、CA Access Control の Watchdog がチェックするかどうかを指定します。

有効な値は、yes および no です。

デフォルト: no

serevu

[serevu] セクションのトークンは、serevu ユーティリティの属性を指定します。

config_file

serevu 環境設定ファイルの場所を指定します。

デフォルト: *ACInstallDir*/etc/serevu.cfg

def_diff_time

serevu が関連するシステム ログで失敗ログインをスキャンする時間間隔を指定します。

この値は、秒単位（たとえば 300）または分単位（たとえば 5 m）で指定できます。

たとえば、このトークンを 300 に設定した場合、serevu は直前の 300 秒間に発生した失敗ログインを検索します。

このトークンには、def_sleep_time トークンの値の偶数倍の数値を指定することをお勧めします。

デフォルト: 5 m（5 分）

def_disable_time

ログインの試みに何回も失敗したことによってユーザ アカウントが無効になるまでの時間を指定します。

この値は、秒単位（たとえば 300）または分単位（たとえば 5 m）で指定できます。

デフォルト: 6 m（6 分）

def_fail_count

def_diff_time トークンで各ユーザに許可される失敗ログイン回数（一定の時間範囲あたり）を指定します。

指定された時間範囲中にこの失敗ログイン回数に達したユーザは、無効になります。

注: この失敗ログイン回数は、ご使用のシステムに対して設定された失敗ログインの許容値と常に同じにすることをお勧めします。たとえば、Sun Solaris では、/etc/default/login ファイルの RETRIES トークンを使用して、システム値を設定します。

デフォルト値は、Solaris の場合は 5、HP-UX および AIX の場合は 3 です。詳細については、オペレーティング システムのマニュアルを参照してください。

デフォルト: 5

def_sleep_time

serevu によるチェックが実行される時間間隔を指定します。

この値は、秒単位（たとえば 120）または分単位（たとえば 2 m）で指定できます。

デフォルト: 2 m（2 分）

save_disable_path

無効にしたユーザ アカウントのリストの場所を指定し、serevu の終了時に無効なユーザの処理ができるようにします。

デフォルト: *ACInstallDir*/log/serevu_disable.users

詳細情報:

serevu ユーティリティ - 失敗したログイン試行の処理 (P. 251)

sesu

[sesu] セクションのトークンは、他のユーザのパスワードを入力する必要なく、自分以外のユーザとしてログオンする際の動作を制御します。

AlwaysTargetShell

ターゲット シェル（SysV style）を使用するか、呼び出し元シェル（BSD style）を使用するかを指定します。yes に設定した場合、CA Access Control はターゲット ユーザのシェルを使用します。

有効な値は、yes および no です。

デフォルト: no

FilterEnv

ターゲット ユーザが root の場合に sesu がシェルに渡さない環境変数のリストを指定します。変数名はスペースまたはタブで区切ります。

デフォルト値なし

old_sesu

古い sesu ユーティリティを使用するか、新しい sesu ユーティリティを使用するかを指定します。

有効な値は以下のとおりです。

yes - 旧バージョンのままの古い sesu ユーティリティを使用します。

no - 新しい sesu ユーティリティは、(SystemSu トークンに定義された) ネイティブ su プログラムを呼び出して su と sesu の間の一貫性を確保します。SystemSu トークンが有効ではない場合、sesu は古いメカニズムを使用します。

注: このトークンを no に設定すると、Path トークン、AlwaysTargetShell トークン、sys_env_file トークン、および FilterEnv トークンは無視されます。

デフォルト: yes

パス

sesu が PATH 環境変数の設定に使用する値を指定します。このトークンを設定しない場合、sesu は PATH 変数を設定しません。

デフォルト値なし

request_target_password

old_sesu トークンが no に設定されていて、ターゲット ユーザが root 以外のユーザのために sesu を実行しているときに、そのターゲット ユーザのパスワードを要求するかどうかを指定します。

デフォルト: yes

sys_env_file

sesu セッションの環境変数値を保存する ASCII ファイルを指定します。このトークンは、「-」パラメータを指定して sesu を起動する場合 (sesu -) にのみ使用します。ファイルの各行の形式は、変数 = 値です。

デフォルト: なし (ただし、IBM AIX の場合は */etc/environment*)

SystemSu

/bin/su プログラムの場所を指定します。デフォルト以外の場所にあるプログラムを使用する場合は、このトークンを更新する必要があります。認証デーモンが見つからない場合、sesu はこのトークンに指定されたプログラムを実行します。

注: AIX では、システムの su バイナリを、sesu バイナリではなく sesu ラッパーへのシンボリックリンクで置換します。

デフォルト: /bin/su

UseInvokerPassword

起動したユーザのパスワードの入力を sesu が要求するかどうかを指定します。このトークンの値が no の場合、sesu はパスワードの入力を要求しません。

デフォルト: no

詳細情報:

sesu ユーティリティ - ユーザの代替 (P. 254)

sesudo

[sesudo] セクションのトークンは、sesudo ユーティリティの属性を指定します。

echo_command

sesudo がコマンドの実行前にそのコマンドを表示するかどうかを指定します。コマンドを表示するには、このトークンの値を yes に設定します。

デフォルト: No

echo_success

sesudo コマンドの実行が成功したときに、成功したことを伝えるメッセージを sesudo が端末に出力するかどうかを指定します。

有効な値は、yes および no です。

デフォルト: yes

詳細情報:

sesudo ユーティリティ (P. 257)

standalone

[standalone] セクションのトークンは、スタンドアロンのマシンを使用した管理のオプションを指定します。

full_login_check

standalone を使用したサイト管理をログインとみなすかどうかを指定します。

有効な値は 0 または 1 です。

このトークンが 1 に設定された場合、マシンへのログインとみなされます。

デフォルト: 0

tcp_communication

[tcp_communication] セクションのトークンは、一般的な TCP 接続設定を定義します。

listening_backlog

リスニング ブロックごとに確立できる新しい TCP 同時接続要求の数を定義します。

デフォルト: 128

tng

[tng] セクションのトークンは、Unicenter TNG 環境への CA Access Control の統合を制御します。

defsesid

特定のセッション グループ ID が定義されていないユーザに対して、デフォルトのセッション グループ ID を指定します。

セッション グループは、CA SSO で使用されます。

デフォルト: CAUNICENTER

ssf_numsubp

受信する SSF 要求の処理を sessfgate デーモンが開始するために必要なサブプロセスの数を指定します。

デフォルト: 1

sso_applname

CA SSO の CA-Ticket 機能を使用するサイトに対して、8 文字の文字列を指定します。この文字列は、data/keymgmt フォルダにある seos のホーム ディレクトリ下の keymgmt ファイルに対応している必要があります。これらのファイルの名前は、SSO_APPLNAME_key に基づいています。

たとえば、UNICENTR のデフォルト値を取得した場合、ファイル名は UNICENTR_key になります。

デフォルト: UNICENTR

pmd.ini ファイル

UNIX で該当

pmd.ini ファイルには、特定の PMDB の作成時およびメンテナンス時に CA Access Control が使用する、設定と初期設定のためのさまざまな設定が含まれます。このファイルは複数のセクションで構成され、各セクションに複数の設定があります。

セクション	説明
endpoint_management	Policy Model エンドポイント管理設定。
lang	Policy Model を使用した作業用の、CA Access Control の管理インターフェース(selang)の設定。
logmgr	PMDB のログ機能の設定。
passwd	ユーザおよびパスワードのデータの設定。
pmd	Policy Model デーモン(sepmdd)の設定。
seos	PMDB の汎用設定。

endpoint_management

[endpoint_management] セクションには、Policy Model 用のエンドポイント管理設定を定義するパラメータが含まれています。

debug_mode

CA Access Control が DMS ディレクトリ(1)内の endpoint_management.log ファイルにデバッグ メッセージを書き込むかどうかを指定します。

制限: 0,1

デフォルト: 0 (デバッグは無効になります)

注: ログ ファイルの場所は *ACInstallDir*/log/endpoint_management.log です。

operation_mode

CA Access Control メッセージ キューによる一元(DMS)エンドポイント管理を有効にするかどうかを指定します。

制限: 0、1

デフォルト: 1 (有効)

lang

[lang] セクションには、PMDB の作成時およびメンテナンス時に、CA Access Control の言語プログラム(selang)で使用されるパラメータが含まれています。

pre_user_exit

CA Access Control が UNIX ユーザ データベースを更新する言語コマンドを発行する前に実行される、exit プログラムのパスを指定します。

post_user_exit

CA Access Control が UNIX ユーザ データベースを更新する言語コマンドを発行した後に実行される、exit プログラムのパスを指定します。

pre_group_exit

CA Access Control が UNIX グループ データベースを更新する言語コマンドを発行する前に実行される、exit プログラムのパスを指定します。

post_group_exit

CA Access Control が UNIX グループ データベースを更新する言語コマンドを発行した後に実行される、exit プログラムのパスを指定します。

logmgr

[logmgr] セクションには、PMDB ログ機能で使用されるパラメータが含まれています。

audit_back

PMDB の監査バックアップ ファイルの名前を指定します。

デフォルト: pmd_audit.bak

audit_log

PMDB の監査ログ ファイルの名前を指定します。

デフォルト: pmd_audit

audit_group

PMDB の監査ファイルに対する読み取り権限を持つグループを指定します。グループが指定されていない場合は、root のみに監査ファイルの読み取り権限が付与されます。CA Access Control はこのトークンの値の有効性を確認しないため、無効なグループ名を入力すると、監査ログ ファイルに対するアクセス許可はどのグループにも割り当てられません。

既存の監査ログ ファイルのグループ所有者権限を変更するには、以下の手順に従います。

1. selang の chgrp コマンドを使用して、ファイルのグループ所有者権限を設定します。
2. 以下のコマンドを入力して UNIX のアクセス権限を変更します。

```
chmod 640 /opt/CA/AccessControl//log/seos.audit
```

デフォルト: none

audit_size

PMDB の監査ログ ファイルのサイズ(KB 単位)を指定します。50 KB 以上のサイズを指定してください。

デフォルト: 50 KB

error_back

PMDB のエラー バックアップ ファイルの名前を指定します。

デフォルト: pmd_error.bak

error_log

PMDB のエラー ログ ファイルの名前を指定します。

デフォルト: pmd_error

error_group

PMDB のエラー ファイルに対する読み取り権限を持つグループを指定します。グループが指定されていない場合は、root のみにエラー ファイルの読み取り権限が付与されます。CA Access Control はこのトークンの値の有効性を確認しないため、無効なグループ名を入力すると、エラー ログ ファイルに対するアクセス許可はどのグループにも割り当てられません。

既存のエラー ログ ファイルのグループ所有者権限を変更するには、以下の手順に従います。

1. selang の chgrp コマンドを使用して、ファイルのグループ所有者権限を設定します。
2. 以下のコマンドを入力して UNIX のアクセス権限を変更します。

```
chmod 640 /opt/CA/AccessControl//log/seos.error
```

デフォルト: none

error_size

(error_log で定義されている) PMDB のエラー ログ ファイルの最大サイズ (KB 単位) を定義します。

制限: 最小値は 50 KB です。

デフォルト: 50

max_log_size

PMDB の一般的なログ ファイルのサイズ (KB 単位) を指定します。

デフォルト: 50 KB

pmd_log_level

PMDB のログ ファイルに記録されるメッセージを決定します。

有効な値は以下のとおりです。

0 - エントリを記録しません。

1 - エラー メッセージのみを記録します。

2 - エラー メッセージおよび情報メッセージを記録します。

デフォルト: 2

use_syslog

Policy Model デーモンが syslog メッセージを記録するかどうかを指定します。

デフォルト: yes

passwd

[passwd] セクションには、UID および GID のパラメータが含まれます。

AllowedGidRange

予約済みの数値を指定します。

最初の数より小さい整数と、2 番目の数より大きい整数は予約済み GID です。これは、CA Access Control では更新できません。

注: 指定された整数が 1 つしかない場合は、1 から指定された整数までのすべての整数が予約済み GID になります。上限より大きな数値を指定した場合は、デフォルトの上限(30000)が適用されます。負の数値を指定した場合は、デフォルトの下限(1)が適用されます。

制限: 1 ～ 2147483647

デフォルト: 100,30000

AllowedUidRange

予約済みの数値を指定します。

最初の数より小さい整数と、2 番目の数より大きい整数は予約済み UID です。これは、CA Access Control では更新できません。

注: 指定された整数が 1 つしかない場合は、1 から指定された整数までのすべての整数が予約済み UID になります。

デフォルト: 100,30000

pmd

[pmd] セクションには、PMDB の作成時およびメンテナンス時に、sepmdd デーモンで使用される属性が含まれます。

_min_retries_

使用不可のサブスクライバに対して、キューに格納されている次の更新の再送信を sepmdd が試行する最小回数を指定します。sepmdd は、サブスクライバのリスト内をループして未処理の更新を見つけます。使用不可のサブスクライバに対して更新を再送信できなかった場合、カウンタの数値を上げます。このトークンで指定した最小試行回数を超えた場合、そのサブスクライバには「使用不可」のマークが付けられます。

デフォルト: 4

_QD_timeout_

sepmdd デーモンがサブスクライバ リストの最初のスキャンでサブスクライバ データベースの更新を試みる際に、sepmdd デーモンが待機する制限時間（秒単位）を指定します。制限時間が経過した時点でサブスクライバを更新できなかった場合、デーモンはそのサブスクライバの更新処理を省略して、サブスクライバ リストにある残りのサブスクライバの更新を試みます。

sepmdd は、サブスクライバ リストの 1 回目のスキャンが終了した後、2 回目のスキャンを実行します。2 回目のスキャンでは、1 回目のスキャンで更新できなかったサブスクライバの更新を試みます。2 回目のスキャンでは、接続システム コールがタイムアウトになるまで（約 90 秒間）サブスクライバの更新を試みます。

デフォルト: 3

_retry_timeout_

_min_retries_ で指定した試行の最小回数に達した後、使用不可のサブスクライバに対して更新を再送信するまでの待機期間（分単位）を指定します。このトークンで定義した期間（分単位）を経過すると、このサブスクライバには「使用可能」のマークが付けられます。

サブスクライバは、以下のいずれかが行われるまで、「使用不可」とマーキングされています。

- 手動でリリースされる。
- sepmdd が手動で停止されて再起動される。sepmdd は以下の場合に再起動されます。
  - 言語機能が sepmdd に接続しようとした場合。
  - 親 PMD が更新を送信しようとした場合。
  - pull オプションがサブスクライバによってトリガされた場合。この現象は、サブスクライバで CA Access Control が起動したときに発生することがあります。
- pull オプションが使用不可のサブスクライバによってトリガされる。

注: sepmdd をあまり頻繁に停止するのは好ましくありません。これは、デーモンの再起動には時間がかかり、結果として伝播プロセス全体の速度が低下するためです。安定性に問題が発生する可能性があるため、停止せずに常時稼動させることもお勧めできません。

デフォルト: 30

_shutoff_time_

sepmdd が終了するまでのアクティビティの時間（分単位）を指定します。このトークンの値がゼロの場合、sepmdd は終了しません。

デフォルト: 0

always_propagate

このトークンを no に設定すると、Policy Model による実行が失敗したコマンドはサブスクライバに伝播されません。

デフォルト: none

exclude_file

除外ファイルを指定します。

除外ファイルには、Policy Model の更新情報の受け取りから除外する必要のあるホスト名が含まれています（各行に 1 つずつ）。

デフォルト： none

exclude_localhost

ローカル ホストがサブスクライバとして更新情報を受け取らないよう PMDB に指示します。

可能な値：yes、no。

デフォルト： no

exclude_method

サブスクライバを除外する際の更新ファイルのオフセット促進を有効または無効にします。

値は以下のとおりです。

「pmdwait」- オフセットを促進しない

その他 -「バイパス」

デフォルト： pmdwait

filter

フィルタ ファイルの名前を指定します。

force_auto_truncate

Policy Model のサブスクライバが存在しない場合でも、CA Access Control が更新ファイルを切り捨てるかどうかを指定します。

更新ファイルは（sepmd -t を使用して）手動で切り捨てることができます。また、CA Access Control は、自動切り捨てをトリガするイベントを定義した別の環境設定（trigger_auto_truncate）に基づいて、ファイルを自動的に切り捨てます。

注： Policy Model のサブスクライバがすべて「非同期」の場合、Policy Model には実質的にサブスクライバがありません。

デフォルト： yes

group_file_name

新しい UNIX グループのグループ ファイル名を指定します。sepmdd は、新しい UNIX グループのグループ エントリをこのファイルに保存します。

デフォルト: group

is_maker_checker

デュアル コントロールを使用するかどうかを指定します。このトークンの有効な値は yes と no です。

yes を選択した場合、PMDB の更新はトランザクションを通じてのみ可能になり、直接更新することはできません。また、ある管理者が入力した各トランザクションを別の管理者が処理した後でなければ、PMDB に対してコマンドが実行されません。

デフォルト: no

password_file_name

新しい UNIX ユーザのパスワード ファイル名を指定します。sepmdd は、新しい UNIX ユーザのパスワード エントリをこのファイルに保存します。

デフォルト: passwd

send_unix_env

sepmd が Policy Model のパスワード ファイルおよびグループ ファイルの内容を送信するかどうかを示します。

このトークンを **yes** に設定すると、*sepmd -n* オプションは、Policy Model のパスワード ファイルおよびグループ ファイルの内容を送信します。

このトークンを **no** に設定すると、*sepmd -n* オプションは、Policy Model のパスワード ファイルおよびグループ ファイルの内容を送信しません。

デフォルト: yes

synch_uid

sepmdd が Policy Model とそのサブスクライバの間で UID の同期をとるかどうかを決定します。このトークンの有効な値は yes と no です。

このトークンが **no** の場合、sepmdd は UID の同期をとりません。各サブスクライバ ホストで使用可能な最初の UID がユーザに割り当てられます。

このトークンが **yes** の場合、sepmdd は UID の同期を試みます。たとえば、PMDB で 1000 という UID を指定して新しい UNIX ユーザが作成されると、sepmdd はその UID をサブスクライバに送信します。1000 という UID がすでにいずれかのサブスクライバで使用されている場合、そのサブスクライバの更新は失敗します。

sepmdd が UID の同期を試みるのは、PMDB に送られた元のコマンドでユーザの UID が指定されなかった場合に限定されます。元のコマンドで UID が指定されていた場合、指定された UID がすべてのサブスクライバに送られます。

デフォルト: yes

TNG_Environment

特別な TNG クラスおよびリソースを使用してデータベースを作成するかどうかを指定します。

有効な値は以下のとおりです。

0 - 特別な TNG クラスを使用せずにデータベースを作成します。

1 - 特別な TNG クラスをすべて使用してデータベースを作成します。

デフォルト: 0

transaction_lib

Maker-Checker ポリシーのパスを指定します。

デフォルト: /opt/CA/eTrustAccessControl/policies/maker

trigger_auto_truncate

Policy Model 更新ファイルの自動切り捨てをトリガするサイズ(メガバイト単位)を定義します。

下限より小さな値を使用した場合は、デフォルト値が使用されます。上限より大きな値を使用した場合は、上限の値が使用されます。

制限: 1 ～ 2000 MB

デフォルト: 1024 MB

update_while_processing

Policy Model が受信イベントを処理するときに、サブスクライバにコマンドを伝播する頻度を定義します。

この頻度は updates_in_chunk 設定の要因であり、PMD が、並んでいる次のサブスクライバに一連のコマンドを送信する前に処理するコマンドの数を決定します。たとえば、これを 3 に設定し、updates_in_chunk が 10 に設定されている場合、PMD は、並んでいる次のサブスクライバに一連のコマンド（10 個）を送信する前に、30 個のコマンドを処理します。0 の値は、PMD が受信イベントを処理する一方で、コマンドを伝播しないことを意味します。

デフォルト: 1

updates_in_chunk

Policy Model がその各サブスクライバに対してループの各サイクルで送信するコマンドの最大数を決定します。

デフォルト: 20

UseEncryption

updates.dat ファイルに保存される更新情報を暗号化するかどうかを指定します。

デフォルト: no

UseShadow

PMDB ネイティブ環境を参照するときに shadow ファイルを使用するかどうかを決定します。

デフォルト: no

YpServerSecure

NIS パスワード マップの作成に使用される shadow password ファイル（NIS サーバ上のセキュリティ ファイル）の名前を指定します。このトークンは、UseShadow を yes に設定した場合にのみ適用されます。

デフォルト: /etc/shadow

seos

CA Access Control で使用されるグローバルな設定を含む [seos] セクションのトークンについて、以下の表で説明します。

parent_pmd

この PMDB が更新を受け入れる Policy Model データベース（PMDB）のカンマ区切りリストを定義します。この PMDB は、このリストに指定されていない PMDB からの更新情報を拒否します。

PMDB の行区切りリストを含むファイル パスを指定することもできます。

この PMDB が PMDB からの更新情報を受け入れるようにするには、このトークンを「_NO_MASTER_」に設定します。

このトークンを設定しない場合、PMDB はどの PMDB からも更新情報を受け入れません。

各 PMDB は pmd_name@hostname の形式で指定します。

以下に例を示します。

```
parent_pmd = pmd1@host1,pmd2@host1,pmd3@host2
parent_pmd = /opt/CA/AccessControl//parent_pmdbs_file
```

デフォルト: トークンは設定されていません（PMDB はどの PMDB からも更新情報を受け入れません）

lang.ini ファイル

UNIX で該当

このセクションでは、lang.ini ファイルで設定し、selang ユーティリティで使用されるトークンについて説明します。

lang.ini ファイルは、以下のセクションで構成されています。

general

複数のリソース タイプ、つまり新しいリソースと新しいユーザの両方に適用されるデフォルト パラメータが含まれています。

history

selang の履歴メカニズムに関するデフォルト パラメータが含まれています。

newres

新しいリソース レコードのプロパティに適用されるデフォルト値が含まれています。別の値を明示的に設定しない限り、このデフォルト値が適用されます。

newusr

新しいユーザ レコードのプロパティに適用されるデフォルト値が含まれています。別の値を明示的に設定しない限り、このデフォルト値が適用されます。

properties

ユーザ定義プロパティ向けのファイル保存場所といった、ユーザ定義プロパティに対する値を指定するトークンを含んでいます。このトークンにはデフォルト値がないため、明示的に設定する必要があります。

unix

コマンド シェル内から UNIX に新しいユーザを定義したときに適用されるデフォルト値が含まれています。別の値を明示的に設定しない限り、このデフォルト値が適用されます。

general

[general] セクションには、複数のリソース タイプに適用されるデフォルト パラメータが含まれています。

defaultOwner

新しいレコードに適用される所有者の名前。

値を指定しない場合、新しいレコードの作成者が所有者として割り当てられます。

history

[history] セクションには、selang の履歴メカニズムのデフォルト パラメータが含まれています。

HistFile

履歴リストのコマンドが格納されているファイルの名前。コマンド リストは、各セッションの開始時にロードされます。

デフォルト値はありません。つまり、セッションの終了時に履歴リストは保存されません。

HistSize

履歴メカニズムによって格納されるコマンドの数（10 ～ 100 の正の整数）。

デフォルト: 30

newres

[newres] セクションには、newres コマンドによって適用されるデフォルト値が含まれています。newres は、データベースに新しいリソース レコードを作成するコマンドです。このセクションの各トークンは、newres のパラメータを示しています。lang.ini ファイルに示されていない引数には、CA Access Control でハードコードされているデフォルト値が割り当てられます。 トークンの値を指定しない場合は、表に指定されたデフォルト値が適用されます。

DefaultAudit

新規リソースのデフォルトの監査モード。有効な値は、none、all、success、failure です。

デフォルト: failure

DefaultDay

リソースに適用されるデフォルトの曜日制限。有効な値は、anyday、weekdays、mon、tue、wed、thu、fri、sat、sun です。

デフォルト: anyday

DefaultNotify

リソース レコードに関する警告メッセージの送信先となるデフォルトの電子メール アドレス。

デフォルト値はありません。つまり、通知メッセージは送信されません。

DefaultTime

リソースに適用されるデフォルトの時間帯制限。有効な値は、anytime、startTime:endTime です。

デフォルト: anytime

DefaultWarning

デフォルトで警告モードを有効にするかどうか。有効な値は、yes および no です。

デフォルト: no

newusr

[newusr] セクションには、データベースに新しいユーザ レコードを作成する newusr コマンドによって割り当てられるデフォルト値が含まれています。このセクションの各トークンは、newusr のパラメータを示しています。lang.ini ファイルに示されていない引数には、CA Access Control でハードコードされているデフォルト値が割り当てられます。トークンの値を指定しない場合は、表に指定されたデフォルト値が適用されます。

DefaultAudit

新規ユーザのデフォルトの監査モード。有効な値は、none、all、success、failure、loginsuccess、loginfailure です。

デフォルト: failure loginfailure loginsuccess

DefaultDay

システムにログインしたときにユーザに適用されるデフォルトの曜日制限。有効な値は、anyday、weekdays、mon、tue、wed、thu、fri、sat、sun です。

デフォルト: anyday

DefaultExpire

ユーザ レコードのデフォルトの有効期限。 有効な値は、expire[*dd*/*mm*/*yy*]、expire- です。

デフォルト: expire-

DefaultLocation

ユーザが属しているデフォルトの場所。

デフォルト値なし

DefaultNotify

ユーザがログインしたときに警告メッセージの送信先となるデフォルトの電子メール アドレス。

デフォルト値はありません。つまり、通知メッセージは送信されません。

DefaultOrg

ユーザが属している組織。

デフォルト値なし

DefaultOrgUnit

ユーザが属している組織単位。

デフォルト値なし

DefaultTime

システムにログインしたときにユーザに適用されるデフォルトの時間帯制限。有効な値は、anytime、startTime:endTime です。

デフォルト: anytime

properties

[properties] セクションには、ユーザ定義のプロパティに適用するパラメータが含まれています。

UserDefinedTokensFile

ユーザ定義のプロパティのコンテキスト情報が含まれている定義ファイルのパスです。

デフォルト: none

UserDefinedAttributesFile

ユーザ定義のプロパティの属性情報が含まれている定義ファイルのパスです。

デフォルト: none

ユーザ定義のプロパティ

このセクションは、sepropadm ユーティリティの補足です。sepropadm で作成したデータベース プロパティを認識する selang コンテキストを定義します。この定義は、sepropadm で使用される形式と類似した形式を使用する 2 つの定義ファイルで行います。これらのファイルの場所は、このセクションの 2 つのトークンで指定します。

注: プロパティは、selang によって定義ファイルをロードする前に、(sepropadm ユーティリティを使用して) データベースで定義する必要があります。定義ファイルは、初期化段階で selang が実行されたときに自動的にロードされます。

適切な定義ファイルとデータベースの両方でこれらのプロパティを定義すると、CA Access Control で定義するその他のプロパティと同様に、selang コマンドで使用できます。

重要: sepropadm ユーティリティでは、**必ず**ベンダーのサポート担当者に承認**された**説明ファイルを使用してください。

詳細情報:

sepropadm Utility - データベース プロパティの管理 (P. 240)

定義ファイル

新しいユーザ定義プロパティを selang に認識させるため、selang では初期化中にトークン ファイルと属性ファイルの 2 つの *.def ファイルをロードします。

トークン ファイル

ユーザ定義のトークン ファイル

ベンダーのサポート担当者によって提供される定義ファイルです。定義ファイルの形式は以下のとおりです。

セミコロン (;) で始まる行はコメントであり、処理されません。

シャープ記号 (#) で始まる行が 1 行必要です。この行は、記述行より前に置く必要があります。

説明ファイルは、以下の形式に準拠する必要があります。

```
TOKEN=%s DOMAIN=%d CLASS=%d COMMAND=%d
```

以下に、サンプルのトークン定義ファイルを示します。

```
; Sample Token Definition File for user defined properties
; Copyright 2004 Computer Associates International, Inc.
; ------------------------------------------
; DO NOT USE THIS FILE UNLESS YOU KNOW HOW TO!
# token definition file
; Format is :
TOKEN=EMAIL DOMAIN=1 CLASS=USER COMMAND=206
TOKEN=NOEMAIL DOMAIN=1 CLASS=USER COMMAND=206
TOKEN=EMAIL DOMAIN=1 CLASS=USER COMMAND=218
TOKEN=AGE DOMAIN=1 CLASS=USER COMMAND=206
TOKEN=AGE DOMAIN=1 CLASS=USER COMMAND=218
TOKEN=NOAGE DOMAIN=1 CLASS=USER COMMAND=206
TOKEN=TERMLOCATION DOMAIN=1 CLASS=TERMINAL COMMAND=217
TOKEN=NOTERMLOCATION DOMAIN=1 CLASS=TERMINAL COMMAND=205
TOKEN=TERMLOCATION DOMAIN=1 CLASS=TERMINAL COMMAND=205
```

属性ファイル

ユーザ定義の属性ファイル

ベンダーのサポート担当者によって提供される定義ファイルです。定義ファイルの形式は以下のとおりです。

セミコロン(;)で始まる行はコメントであり、処理されません。

シャープ記号(#)で始まる行が 1 行必要です。この行は、記述行より前に置く必要があります。

説明ファイルは、以下の形式に準拠する必要があります。

```
PROPERTY=%s TYPE=%d FLAGS=%x
```

以下に、サンプルの属性定義ファイルを示します。

```
; Sample Attributes Definition File for user defined properties
; Copyright 2004 Computer Associates International, Inc.
; ------------------------------------------
; DO NOT USE THIS FILE UNLESS YOU KNOW HOW TO!
# attributes definition file
; Format is :
PROPERTY=EMAIL TYPE=306 FLAGS=8000
PROPERTY=EMAIL TYPE=5 FLAGS=8000
PROPERTY=AGE TYPE=306 FLAGS=8000
PROPERTY=AGE TYPE=5 FLAGS=8000
PROPERTY=TERMLOCATION TYPE=306 FLAGS=8000
PROPERTY=TERMLOCATION TYPE=5 FLAGS=8000
```

重要: selang では、**必ず**ベンダーのサポート担当者に承認**された**定義ファイルを使用してください。

unix

[unix] セクションには、UNIX にユーザが追加されたときに、newusr コマンドによって割り当てられるデフォルト値が含まれています。このセクションの各トークンは、*unix* パラメータの引数を示しています。lang.ini ファイルに示されていない UNIX 引数には、CA Access Control にハードコードされているデフォルト値が割り当てられます。

DefaultPGroup

新規ユーザに割り当てられるデフォルトのグループ。サーバの seos.ini ファイルにデフォルトのシェルを指定した場合は、ここで指定した値より優先されます。

デフォルト: other

DefaultShell

新規ユーザのデフォルトのシェル。サーバの seos.ini ファイルにデフォルトのシェルを指定した場合は、ここで指定した値より優先されます。

デフォルト: /bin/sh

DefaultHome

システムのデフォルトのホーム ディレクトリ。サーバの seos.ini ファイルにデフォルトのシェルを指定した場合は、ここで指定した値より優先されます。ユーザのホーム ディレクトリは、指定されたシステム ホーム ディレクトリのサブディレクトリです。たとえば、システムのホーム ディレクトリが /home の場合、新規ユーザのホーム ディレクトリは /home/userName になります。サーバの seos.ini ファイルにホーム ディレクトリのプレフィクスを指定した場合は、ここで指定した値より優先されます。

以前のバージョンを使用されている場合の情報ですが、トークン DefaultHome は HomeDirPrefix に置き換わっています。

デフォルト: /home

trcfilter.init

UNIX で該当

CA Access Control デーモンでは、trcfilter.init 初期設定ファイルも使用します。

このオプション ファイルには、CA Access Control トレース メッセージをフィルタ処理するためのフィルタ マスクを指定するエントリが保存されています。ファイルの各行には、正規表現が含まれています。メッセージがトレース ファイルに送信されるとき、メッセージが trcfilter.init ファイルのいずれかのエントリに一致するかどうかがチェックされます。trcfilter.init ファイルに指定された表現のいずれにも一致しない場合にのみ、トレース メッセージがファイルに書き込まれます。

たとえば、trcfilter.init ファイルに以下の表現を指定すると、「INFO」または「WATCHDOG」で始まるすべてのメッセージがすべて破棄されます。これらのメッセージはトレース ファイルに書き込まれません。

```
WATCHDOG*
INFO*
```

注: このファイルは、ユーザ トレースによって生成された監査レコードをフィルタしません。これらの監査レコードをフィルタするためには、audit.cfg ファイルを編集します。

audit.cfg ファイル - 監査レコードのフィルタ

audit.cfg ファイルは、監査ファイルに送信されないレコードを定義することによって、ホストの監査レコードをフィルタリングします。各行は、監査情報を除外するためのルールを表します。

デフォルトでは、audit.cfg ファイルは以下のディレクトリにあります。

- （UNIX）/opt/CA/AccessControl/etc
- （Windows）C:¥¥ProgramFiles¥CA¥AccessControl¥data

audit.cfg ファイルの場所は、seos.ini ファイル（UNIX）内の［logmgr］ AuditFiltersFile トークンまたは logmgr レジストリ キー（Windows）内の AuditFiltersFile エントリを編集することによって、変更できます。

audit.cfg ファイルを使用して以下の監査イベント タイプのレコードをフィルタリングできます。各タイプは異なる構文でフィルタリングされます。

- リソース アクセス
- ネットワーク接続 (P. 464)
- ログイン イベントおよびログアウト イベント (P. 465)
- セキュリティ データベース管理 (P. 467)
- ユーザのトレース メッセージ

注: 各タイプの構文の列に * がある場合には、「何らかの値」を意味します。

audit.cfg File -- リソース アクセス イベント フィルタ構文

リソース アクセス イベントに属する監査レコードのフィルタ形式は、以下のとおりです。

```
ClassName;ObjectName;UserName;ProgramPath;Access;AuthorizationResult
```

ClassName

アクセスされたオブジェクトが属するクラスの名前を定義します。

注: クラスの名前は大文字で入力してください。

ObjectName

アクセスされたオブジェクトの名前を定義します。

UserName

アクセサの名前を定義します。

ProgramPath

オブジェクトへのアクセスに使用するプログラムの名前を定義します。

Access

オブジェクトへの要求されたアクセスを定義します。

注: 以下の値は、監査レコードをフィルタリングするために audit.cfg ファイルで使用する、このパラメータの値です。audit.cfg ファイルのこのパラメータの値は、CA Access Control がそのイベントに対して監査レコードに書き込む値とは異なる場合があります。この場合、各値の説明の後にその差異が明記されます。パラメータを入力する際には、以下のリストに表示されているものと同じスペルで(大文字と小文字を区別して)入力してください。

値は以下のとおりです。

*

アクセスのいずれかのタイプを表すワイルドカード。

Chdir

ディレクトリの変更 - アクセサは、別のディレクトリにオブジェクトを移動するように要求しました。

Chmod

モードの変更 - アクセサは、オブジェクトのモードを変更するように要求しました。

Chgrp

(UNIX)グループの変更 - アクセサは、オブジェクトが属するグループを変更するように要求しました。

Chown

所有者の変更 - アクセサは、オブジェクトの所有者を変更するように要求しました。

Connect

グループへのユーザの追加 - アクセサは、新しいユーザをグループに追加するように要求しました。

注: Connect の値と Join の値は同一です。

Control

(UNIX) Control - アクセサはオブジェクトに Chown、Chmod、Utime、Sec、Chdir、および Update アクセスを要求しました。

Cre

Create - アクセサは、オブジェクトを作成するように要求しました。

Crrdwr

Create、Read、および Write - アクセサはオブジェクトに Create、Read、および Write アクセスを要求しました。

注: CA Access Control は、対応する監査レコードに、この値を CrRdWrite として書き込みます。

Crread

Create および Read - アクセサはオブジェクトに Create および Read アクセスを要求しました。

注: CA Access Control は、対応する監査レコードに、この値を CrRead として書き込みます。

Crwrite

Create および Write - アクセサはオブジェクトに Create および Write アクセスを要求しました。

注: CA Access Control は、対応する監査レコードに、この値を CrWrite として書き込みます。

Del

削除 - アクセサは、オブジェクトを削除するように要求しました。

注: CA Access Control は、対応する監査レコードに、この値を Erase として書き込みます。

Filereplace

Create および Erasee — アクセサはオブジェクトに Create および Erase アクセスを要求しました。

注: CA Access Control は、対応する監査レコードにこの値を Replace として書き込みます。

Filescan

Filescan - アクセサはオブジェクトに List アクセスを要求しました。

注: CA Access Control は、対応する監査レコードにこの値を Scan として書き込みます。

Join

グループへのユーザの追加 - アクセサは、新しいユーザをグループに追加するように要求しました。

注: Connect の値と Join の値は同一です。

Kill

強制終了 - アクセサは、プロセスを中止するように要求しました。

Modify

Modify - アクセサはオブジェクトに Modify アクセスを要求しました。

OwnGrp

Change owner および Change group - アクセサはオブジェクトに Chown および Chgrp アクセスを要求しました。

PW

Password - アクセサはパスワードを変更するように要求しました。

注: CA Access Control は、対応する監査レコードにこの値を Password として書き込みます。

R

読み取り - アクセサは、オブジェクトへの読み取りアクセスを要求しました。

注: (UNIX) STAT_intercept が 1 に設定されている場合、このパラメータには *stat* interception が含まれます。

Rename

ファイル名の変更 - アクセサは、オブジェクトのファイル名を変更するように要求しました。

Sec

ACL の変更 - アクセサは、オブジェクトの ACL を変更するように要求しました。

注: CA Access Control は、対応する監査レコードに、この値を ACL として書き込みます。

Update

Read、Write、および Execute - アクセサはオブジェクトに Read、Write、および Execute アクセスを要求しました。

注: アクセサがオブジェクトに Read および Write アクセスを要求した場合、Update 値はイベントもフィルタリングします。

Utime

(UNIX) 時刻の変更 — アクセサは、オブジェクトの変更日時を変更するように要求しました。

注: CA Access Control は、対応する監査レコードに、この値を Utimes として書き込みます。

W

書き込み - アクセサは、オブジェクトへの書き込みアクセスを要求しました。

X

実行 - アクセサは、オブジェクトを実行するように要求しました。

注: 一部のクラスでは有効ではない値もあります。たとえば、強制終了アクションは FILE クラスのオブジェクトには使用できないため、強制終了は FILE クラスでは無効な値です。ルールの作成時に無効な値をクラスに入力すると、CA Access Control はファイルの読み取り時にそのルールを無視します。

AuthorizationResult

認証結果を定義します。

値: P (許可されました)、D (拒否されました)、*

例: 監査フィルタ ポリシー

- 監査フィルタ ポリシーの例を以下に示します。

```
env config
er config audit.cfg line+("FIEL;*;*;*;R;P")
```

- このポリシーは、以下の行を audit.cfg ファイルに書き込みます。この行は、ファイル リソースへの読み取りアクセスのためにアクセサが行った許可された試行を記録した監査レコードをフィルタします。

```
FILE;*;*;*;R;P
```

audit.cfg File -- ネットワーク接続イベント フィルタ構文

ネットワーク接続イベントに属する監査レコードのフィルタ形式は、以下のとおりです。

{HOST|TCP};*ObjectName*;*HostName*;*ProgramPath*;*Access*;*AuthorizationResult*

HOST

HOST クラスのオブジェクト、すなわち TCP 受信接続によって生成されたレコードをルールがフィルタリングするように指定します。

TCP

TCP クラスのオブジェクト、すなわちサービス イベントとの接続によって生成されたレコードをルールがフィルタリングするように指定します。

ObjectName

アクセスされたオブジェクトの名前を定義します。*ObjectName* は、サービス名またはポート番号にすることができます。

HostName

ホストの名前を定義します。*HostName* は、HOST クラスのオブジェクトである必要があります。

ProgramPath

ログイン プログラムのタイプを定義します。

(Windows) 送信接続では、このパラメータは接続を確立しようとするプロセスのプログラム パスを定義します。

注: このパラメータは、受信接続イベントでは何も意味がありません。受信接続イベントによって生成された監査レコードをフィルタリングするためには、このパラメータに * を使用してください。

アクセス

試行された接続のタイプを定義します。

値は以下のとおりです。

- (HOST) *
- (TCP) R (受信接続)、W (送信接続)、*

AuthorizationResult

認証結果を定義します。

値: P (許可されました)、D (拒否されました)、*

例: ネットワーク接続イベントのフィルタ

- この例では、正常な受信 telnet 接続によって生成されたホスト ca.com からのすべての監査レコードをフィルタします。

  ```
  HOST;telnet;ca.com;*;*;P
  ```

- この例では、拒否された受信および送信ログイン TCP 接続によって生成されたホスト ca.com からのすべての監査レコードをフィルタします。

  ```
  TCP;login;ca.com;*;*;D
  ```

- この例では、送信 telnet 接続によって生成されたホスト ca.com からのすべての監査レコードをフィルタします。

  ```
  TCP;telnet;ca.com;*;W;*
  ```

audit.cfg File -- ログインおよびログアウト イベント フィルタ構文

ログイン イベントまたはログアウト イベントに属する監査レコードのフィルタ形式は、以下のとおりです。

LOGIN;*UserName*;*UserId*;*TerminalName*;*LoginProgram*;*AuthorizationResultOrLoginType*

LOGIN

ログイン イベントおよびログアウト イベントによって生成された監査レコードを、ルールによってフィルタリングするよう指定します。

ユーザ名

アクセサの名前を定義します。

UserId

(UNIX)アクセサのネイティブ ユーザ ID を定義します。

TerminalName

イベントが発生したターミナルを定義します。

LoginProgram

ログインまたはログアウトを試みたプログラムの名前を定義します。

AuthorizationResultorLoginType

認証結果を定義します。

値は以下のとおりです。

*

認証結果のいずれかのタイプを表すワイルドカード。

D

ログイン試行は拒否されました。

P

ログイン試行は許可されました。

O

(UNIX)アクセサはログアウトしました。

I

(UNIX) serevu デーモンは、アクセサのアカウントを無効にしました。

E

(UNIX) serevu デーモンは、アクセサのアカウントを有効にしました。

A

(UNIX)serevu デーモンまたは Pluggable Authentication Module は、不正なパスワードでログインしようとしたユーザを監査しました。

注: Windows では、ログアウト イベントを記録しません。

例:ログインまたはログアウト イベントのフィルタ

- この例では、root が許可されたアカウントにログインする場合に生成されたすべての監査レコードをフィルタします。

  ```
  LOGIN;root;*;*;*;P
  ```

- この例では、システムの CRON プログラムによって root が正常にログインした場合に生成されたすべての監査レコードをフィルタします。

  ```
  LOGIN;root;*;*;SBIN_CRON;P
  ```

- この例では、_CRONJOB_ process が root ユーザをログアウトした場合に生成されたすべての監査レコードをフィルタします。

  ```
  LOGIN;root;*;_CRONJOB_;*;O
  ```

audit.cfg ファイル -- セキュリティ データベース管理イベント フィルタ構文

セキュリティ データベース管理イベントに属する監査レコードのフィルタ形式は、以下のとおりです。

ADMIN;*ClassName*;*ObjectName*;*UserName*;*EffectiveUserName*;*TerminalName*;*Command*;*CommandResult*

ADMIN

管理者が実行したイベントによって生成された監査レコードを、ルールがフィルタリングするように指定します。

ClassName

管理者が実行するコマンドのクラスを定義します。

ObjectName

管理者のコマンドが更新したオブジェクトを定義します。

UserName

コマンドを実行したユーザの名前を定義します。

EffectiveUserName

(UNIX)ルールが適用される有効なユーザの名前を定義します。

(Windows)ルールが適用されるネイティブ ユーザの名前を定義します。

TerminalName

イベントが発生したターミナルを定義します。

コマンド

管理者が実行した selang コマンドを定義します。

CommandResult

認証結果またはコマンド結果を定義します。

値: S(コマンド成功)、F(コマンド失敗)、D(コマンド拒否)、*

例:セキュリティ データベース管理イベントのフィルタ

この例では、admin01 による正常な FILE 管理コマンドによって生成されたすべての監査レコードをフィルタします。

```
ADMIN;FILE'*;admin01;*;*;*;S
```

audit.cfg ファイル -- ユーザのトレース メッセージ イベント フィルタ構文

ユーザのトレース メッセージ イベントに属する監査レコードのフィルタ形式は、以下のとおりです。

```
TRACE;TracedClassName;TracedObjectName;RealUserName;EffectiveUserName;ACUserName;
AuthorizationResult;TraceMessage
```

注: トレース フィルタの最大数は 1000 レコードに制限されています。

TRACE

ユーザ トレース レコードをルールがフィルタリングするように指定します。

TracedClassName

ユーザがアクセスしようとしたオブジェクト クラスの名前を定義します。

注: クラスの名前は大文字で入力してください。

TracedObjectName

ユーザがアクセスしようとしたオブジェクトの名前を定義します。

RealUserName

(UNIX)トレース レコードを生成した実ユーザの名前を定義します。

(Windows)トレース レコードを生成したネイティブ ユーザの名前を定義します。

EffectiveUserName

(UNIX)トレース レコードを生成した、有効なユーザの名前を定義します。

(Windows)トレース レコードを生成したネイティブ ユーザの名前を定義します。このパラメータは、RealUserName パラメータと同一です。このパラメータには * を使用してください。

ACUserName

イベントの許可に CA Access Control が選択したユーザ名を定義します。

AuthorizationResult

認証結果を定義します。

値: P (許可されました)、D (拒否されました)、*

TraceMessage

生成されたトレース メッセージを定義します。

例:ユーザのトレース メッセージ イベントのフィルタ

この例では、有効なユーザが root であり、root が FILE クラスのオブジェクトにアクセスした場合に生成されたすべてのユーザ トレース レコードをフィルタします。

```
TRACE;FILE;*;*;root;*;*;*
```

auditrouteflt.cfg ファイル - 監査レコード ルーティングのフィルタリング

auditrouteflt.cfg ファイルでは、CA Access Control が配布サーバに送信しないレコードを定義することによって、監査レコードのルーティングをフィルタリングできます。各行は、監査情報を除外するためのルールを表します。ファイルのパス名は ReportAgent セクションの audit_filter 構成設定で定義されます。

注: フィルタリングされた監査イベントはローカルの監査ファイルに書き込まれますが、CA Access Control はそれを配布サーバのメッセージ キューに送信しません。ローカルの監査ファイルから監査メッセージを除外するには、logmgr セクションの AuditFiltersFile 構成設定で定義されているファイル(デフォルトでは audit.cfg)にあるフィルタ ルールを変更します。

auditrouteflt.cfg ファイルを使用して、次の監査イベント タイプ、異なる構文別の各タイプのレコードを除去できます。

- リソース アクセス
- ネットワーク接続
- ログイン イベントおよびログアウト イベント
- セキュリティ データベース管理
- ユーザのトレース メッセージ

注: 各タイプの構文の列に * がある場合には、「何らかの値」を意味します。

リソース アクセス イベントのフィルタ構文

リソース アクセス イベントに属する監査レコードのフィルタ形式は、以下のとおりです。

ClassName;ObjectName;UserName;ProgramPath;Access;AuthorizationResult

ClassName

アクセスされたオブジェクトが属するクラスの名前を定義します。

注: クラスの名前は大文字で入力する必要があります。

ObjectName

アクセスされたオブジェクトの名前を定義します。

ユーザ名

アクセサの名前を定義します。

ProgramPath

オブジェクトへのアクセスに使用するプログラムの名前を定義します。

アクセス

オブジェクトへの要求されたアクセスを定義します。

値は以下のとおりです。

*

アクセスのいずれかのタイプを表すワイルドカード。

Chdir

ディレクトリの変更 - アクセサは、別のディレクトリにオブジェクトを移動するように要求しました。

Chmod

モードの変更 - アクセサがオブジェクトのモードを変更する要求を行った。

Chgrp

(UNIX) グループの変更 - アクセサは、オブジェクトが属するグループを変更するように要求しました。

Chown

所有者の変更 - アクセサは、オブジェクトの所有者を変更するように要求しました。

Cre

作成 - アクセサが新しいオブジェクトを作成する要求を行った。

Del

削除 - アクセサは、オブジェクトを削除するように要求しました。

Join

グループへのユーザの追加 - アクセサは、新しいユーザをグループに追加するように要求しました。

Kill

強制終了 - アクセサは、プロセスを中止するように要求しました。

R

読み取り - アクセサは、オブジェクトへの読み取りアクセスを要求しました。

注: (UNIX) STAT_intercept が 1 に設定されている場合、このパラメータには *stat* interception が含まれます。

名前変更

ファイル名の変更 - アクセサは、オブジェクトのファイル名を変更するように要求しました。

Sec

ACL の変更 - アクセサは、オブジェクトの ACL を編集するように要求しました。

Utime

(UNIX) 時刻の変更 - アクセサは、オブジェクトの変更日時を変更するように要求しました。

W

書き込み - アクセサは、オブジェクトへの書き込みアクセスを要求しました。

X

実行 - アクセサは、オブジェクトを実行するように要求しました。

注: 一部のクラスでは有効ではない値もあります。たとえば、強制終了アクションは FILE クラスのオブジェクトには使用できないため、強制終了は FILE クラスでは無効な値です。ルールの作成時に無効な値をクラスに入力すると、CA Access Control はファイルの読み取り時にそのルールを無視します。

AuthorizationResult

認証結果を定義します。

値: P (許可されました)、D (拒否されました)、*

ネットワーク接続イベントのフィルタ構文

ネットワーク接続イベントに属する監査レコードのフィルタ形式は、以下のとおりです。

{HOST|TCP};*ObjectName*;*HostName*;*ProgramPath*;*Access*;*AuthorizationResult*

HOST

HOST クラスのオブジェクト、すなわち TCP 受信接続によって生成されたレコードをルールがフィルタリングするように指定します。

TCP

TCP クラスのオブジェクト、すなわちサービス イベントとの接続によって生成されたレコードをルールがフィルタリングするように指定します。

ObjectName

アクセスされたオブジェクトの名前を定義します。*ObjectName* は、サービス名またはポート番号にすることができます。

HostName

ホストの名前を定義します。*HostName* は、HOST クラスのオブジェクトである必要があります。

ProgramPath

ログイン プログラムのタイプを定義します。

(Windows) 送信接続では、このパラメータは接続を確立しようとするプロセスのプログラム パスを定義します。

注:このパラメータは、受信接続イベントでは何も意味がありません。受信接続イベントによって生成された監査レコードをフィルタリングするためには、このパラメータに * を使用してください。

アクセス

試行された接続のタイプを定義します。

値は以下のとおりです。

- (HOST) *
- (TCP) R (受信接続)、W (送信接続)、*

AuthorizationResult

認証結果を定義します。

値: P (許可されました)、D (拒否されました)、*

ログイン イベントおよびログアウト イベントのフィルタ構文

ログイン イベントまたはログアウト イベントに属する監査レコードのフィルタ形式は、以下のとおりです。

LOGIN;*UserName*;*UserId*;*TerminalName*;*LoginProgram*;*AuthorizationResultOrLoginType*

LOGIN

ログイン イベントおよびログアウト イベントによって生成された監査レコードを、ルールによってフィルタリングするよう指定します。

ユーザ名

アクセサの名前を定義します。

UserId

アクセサのネイティブ ユーザ ID を定義します。

TerminalName

イベントが発生したターミナルを定義します。

LoginProgram

ログインまたはログアウトを試みたプログラムの名前を定義します。

AuthorizationResultorLoginType

認証結果を定義します。

値は以下のとおりです。

*

認証結果のいずれかのタイプを表すワイルドカード。

D

ログイン試行は拒否されました。

P

ログイン試行は許可されました。

O

(UNIX)アクセサはログアウトしました。

I

(UNIX) serevu デーモンは、アクセサのアカウントを無効にしました。

E

(UNIX) serevu デーモンは、アクセサのアカウントを有効にしました。

A

(UNIX)serevu デーモンまたは Pluggable Authentication Module は、不正なパスワードでログインしようとしたユーザを監査しました。

注: Windows では、ログアウト イベントを記録しません。

セキュリティ データベース管理イベントのフィルタ構文

セキュリティ データベース管理イベントに属する監査レコードのフィルタ形式は、以下のとおりです。

ADMIN;*ClassName*;*ObjectName*;*UserName*;*EffectiveUserName*;*TerminalName*;*Command*;*CommandResult*

ADMIN

管理者が実行したイベントによって生成された監査レコードを、ルールがフィルタリングするように指定します。

ClassName

管理者が実行するコマンドのクラスを定義します。

ObjectName

管理者のコマンドが更新したオブジェクトを定義します。

ユーザ名

コマンドを実行したユーザの名前を定義します。

EffectiveUserName

(UNIX) ルールが適用される有効なユーザの名前を定義します。

(Windows) ルールが適用されるネイティブ ユーザの名前を定義します。

TerminalName

イベントが発生したターミナルを定義します。

コマンド

管理者が実行した selang コマンドを定義します。

CommandResult

認証結果またはコマンド結果を定義します。

値: S (コマンド成功)、F (コマンド失敗)、D (コマンド拒否)、*

ユーザのトレース メッセージ イベントのフィルタ構文

ユーザのトレース メッセージ イベントに属する監査レコードのフィルタ形式は、以下のとおりです。

TRACE;*TracedClassName;TracedObjectName;RealUserName;EffectiveUserName;ACUserName;AuthorizationResult;TraceMessage*

TRACE

ユーザ トレース レコードをルールがフィルタリングするように指定します。

TracedClassName

ユーザがアクセスしようとしたオブジェクト クラスの名前を定義します。

注: クラスの名前は大文字で入力する必要があります。

TracedObjectName

ユーザがアクセスしようとしたオブジェクトの名前を定義します。

RealUserName

(UNIX)トレース レコードを生成した実ユーザの名前を定義します。

(Windows)トレース レコードを生成したネイティブ ユーザの名前を定義します。

EffectiveUserName

(UNIX)トレース レコードを生成した、有効なユーザの名前を定義します。

(Windows)トレース レコードを生成したネイティブ ユーザの名前を定義します。このパラメータは、RealUserName パラメータと同一です。このパラメータには * を使用してください。

ACUserName

イベントの許可に CA Access Control が選択したユーザ名を定義します。

AuthorizationResult

認証結果を定義します。

値: P (許可されました)、D (拒否されました)、*

TraceMessage

生成されたトレース メッセージを定義します。

例: ネットワーク接続イベントのフィルタ

- この例では、正常な受信 telnet 接続によって生成されたホスト ca.com からのすべての監査レコードをフィルタします。

```
HOST;telnet;ca.com;*;*;P
```

- この例では、拒否された受信および送信ログイン TCP 接続によって生成されたホスト ca.com からのすべての監査レコードをフィルタします。

```
TCP;login;ca.com;*;*;D
```

- この例では、送信 telnet 接続によって生成されたホスト ca.com からのすべての監査レコードをフィルタします。

```
TCP;telnet;ca.com;*;W;*
```

例:ログインまたはログアウト イベントのフィルタ

- この例では、root が許可されたアカウントにログインする場合に生成されたすべての監査レコードをフィルタします。

```
LOGIN;root;*;*;*;P
```

- この例では、システムの CRON プログラムによって root が正常にログインした場合に生成されたすべての監査レコードをフィルタします。

```
LOGIN;root;*;*;SBIN_CRON;P
```

- この例では、_CRONJOB_ process が root ユーザをログアウトした場合に生成されたすべての監査レコードをフィルタします。

```
LOGIN;root;*;_CRONJOB_;*;O
```

例:セキュリティ データベース管理イベントのフィルタ

この例では、admin01 による正常な FILE 管理コマンドによって生成されたすべての監査レコードをフィルタします。

```
ADMIN;FILE'*;admin01;*;*;*;S
```

例:ユーザのトレース メッセージ イベントのフィルタ

この例では、有効なユーザが root であり、root が FILE クラスのオブジェクトにアクセスした場合に生成されたすべてのユーザ トレース レコードをフィルタします。

```
TRACE;FILE;*;*;root;*;*;*
```

例: 監査フィルタ ポリシー

監査フィルタ ポリシーの例を以下に示します。

```
env config
er config auditrouteflt.cfg line+("FILE;*;*;R;P")
```

この例は、次の行を auditrouteflt.cfg ファイルに書き込みます。

```
FILE;*;*;R;P
```

この行は、ファイル リソースへの読み取りアクセスのためにアクセサが行った許可された試行を記録した監査レコードをフィルタします。

監査ログ ルーティング環境設定ファイル selogrd.cfg

UNIX で該当

環境設定ファイルの形式は以下のとおりです。詳細については後で説明します。

```
section-name-1
routing-method destination
[{include|exclude} match-field(match-pattern) ...]
...
.
section-name-2
routing-method destination
[{include|exclude} match-field(match-pattern) ...]
...
.
...
```

監査レコードの指定

環境設定ファイルは、さまざまな宛先に転送する（および転送しない）監査レコードを指定したリストです。監査レコードを指定するには、1 つ以上の特定のフィールドの内容を入力します。標準の UNIX パターン マッチング（ワイルドカード * および ?）を使用できます。

たとえば、ユーザ名が「dbms」という文字で始まるユーザに対応するレコードを指定するには、以下のように入力します。

```
User(dbms*)
```

この例では、「dbms1」、「dbms_mgr」などの名前のユーザが一致します。

同じユーザで、ログインの試みを処理するレコードのみを指定するには、以下のように入力します。

```
User(dbms*) Class(LOGIN)
```

注: 複数のフィールドに関係するレコードを 1 行に指定すると、それらすべてのフィールドに該当するレコードのみが指定されます。

レコードを指定する行と同じ行の先頭に、レコードを含めるか、除外するかを指定します。たとえば、これらのレコードをルーティングに含めるには、以下のように入力します。

```
include User(dbms*) Class(LOGIN).
```

このタイプの行の全体的な形式は、以下のとおりです。

```
[{include|exclude} match-field(match-pattern) ... .]
```

「...」は、最初の match-field(match-pattern) のペアの後に、さらにペアを指定できることを意味します。

match-field(match-pattern) には、以下のいずれかを使用できます。

access (*access-type*)

必要なアクセスのタイプを指定します。*access-type* には、以下のいずれか 1 つを指定します。

ACL、Chdir、Chgrp、Chmod、Chown、Connect、Control、Create、Erase、Exec、Kill、Modify、Owngrp、Password、Read、Rename、Replace、Update、Utimes、および Write。

Class(LOGIN)

ログイン レコードを指定します。

Class(LOGOUT)

ログアウト レコードを指定します。

Class(PWCHANGE)

パスワード管理を指定します。

Class(HOST)

TCP/IP レコードを指定します。

Class(UPDATE *CA Access Control-class*)

データベース管理を指定します。CA Access Control-class には、アクセサ クラスまたはリソース クラス（USER、GROUP、FILE、HOSTNP など）、あるいはクラス名が一致するパターンを指定します。したがって、すべてのデータベースを管理するには、UPDATE * を指定します。

Class(*CA Access Control-class*)

保護されているリソースへのアクセスを指定します。たとえば、Class(FILE) は、ファイルへのアクセスの試みを記録するレコードを参照します。

アスタリスクを使用すると、Class(*CA Access Control-class*) および Class(UPDATE *CA Access Control-class*) を *Class(*CA Access Control-class*)* として組み合わせることができます。たとえば、Class(*FILE) を指定することは、Class(FILE) および Class(UPDATE FILE) の両方を指定することと同じです。つまり、ファイルへのアクセスの試み、および FILE クラスのレコードの更新の試みの両方を示します。

Code(*return-code*)

結果を示す CA Access Control リターン コードを指定します。リターン コードの有効な値は以下のとおりです（このセクションの「例 1」も参照してください）。

A - 無効なパスワードを繰り返し入力したため、ログインの試みに失敗しました。

D - アクセサに十分な権限がないため、CA Access Control によりリソースへのアクセスが拒否されたか、ログインまたはデータベースの更新が許可されませんでした。

E - serevu によって、無効化されたユーザ アカウントが有効化されました。

F - データベースの更新が失敗しました。

I - serevu によってユーザ アカウントが無効化された。

M - 実行したコマンドがデーモンを開始または停止しました。

O - ユーザがログアウトしました。

P - CA Access Control により、リソースへのアクセスまたはログインが許可されました。

S - データベースの更新が成功しました。

T - ユーザが実行したすべてアクションがトレース対象のため、監査レコードが書き込まれました。

U - trusted プログラム（setuid または setgid）が変更されたため、trusted ではなくなりました。

W - リソースへのアクセスが、そのリソースのアクセス ルールに違反しました。ただし、そのリソースに警告モードが設定されているため、CA Access Control によりアクセスが許可されました。

Host(*host-name*)

TCP/IP 接続に関係するホストを指定します。

Object(*resource-name*)

ユーザがアクセスを試みているリソースを指定します。

Reason(*reason-number*)

監査レコードに書き込まれた理由を指定します。

Service(*service-name*)

telnet または FTP など、リモート ホストから要求されたサービス名を指定します。

Source Host(*hostname*)

統合監査に対してレコードを構成したホスト名を指定します。

Stage(*stage-number*)

アクセスが許可または拒否された段階を指定します（「リファレンス ガイド」にある stage code のリストを参照）。

Terminal(*terminal-name*)

アクセスまたは管理を試みている端末を指定します。

Uid(*uid-number*)

アクセスまたは管理を試みているユーザの UID を指定します。

User(*username*)

アクセスまたは管理を試みているユーザを指定します。username には、名前またはパターンを指定します。

注: パターンで指定することが多いのは一部の変数のみですが、実際はすべての変数に（必要であれば段階を表す番号のような変数にも）パターンを使用できます。

複数行による絞り込み

指定内容を絞り込む場合は、一度にさまざまな条件を設定してフィルタ処理を行うことができます。このためには、include 行または exclude 行を続けて指定します。例:

```
include User(dbms*) Class(*LOGIN*).
exclude Terminal(console_*).
```

この例では、ユーザ名が「dbms」で始まり、端末名が「console_」で始まらないという条件を満たすユーザによるログインの試みすべてを指定しています。

宛先の指定

include 行および exclude 行の上の行を使用して、挿入する監査レコードの宛先を指定します。例:

```
mail weekwatch
include User(dbms*) Class(*LOGIN*).
exclude Terminal(console_*).
```

この例では、ユーザ名が「dbms」で始まり、端末名が「console_」で始まらないという条件を満たすユーザによるログインの試みすべてについて、電子メール アドレス weekwatch がレポートを受信するように指定しています。

このタイプの行は、ログ ルーティング環境設定ファイルに以下の形式で記述します。

routing-method destination

以下のいずれかの方法を使用できます。

mail *address*

電子メールで監査レコードを送信します。*address* には宛先アドレスを指定します。user@host の形式でない場合は、ローカル ユーザ リストおよび NIS メール別名マップと照合されます。

注: address がユーザ名であり、そのユーザ アカウントへの代理要求が監査される場合は、監査レコードが無制限に蓄積されます。

screen *username*

selogrd が監査レコードを転送するときに、ユーザが現在のホストにログインしている場合は、そのユーザの画面に監査レコードを表示します。ユーザがログインしていない場合、表示は保留されずに取り消されます。

cons *hostname*

指定されたホストの secmon ユーティリティの Security Administrator GUI に監査レコードを送信します。そのホストが使用可能ではない場合、表示は保留されずに終了します。

file *textfilename*

指定された ASCII ファイルに監査レコードを書き込みます。*textfilename* には絶対パス名を指定する必要があります。また、selogrd にはファイルへのアクセス権が必要です。

host *hostname*

指定したホストの監査ログ収集デーモンに監査レコードを送信します。ホストが使用可能でない場合は、後で再送信します。

notify mail または notify default

監査レコード自体が指定するアドレスに、電子メールで監査レコードを送信します。

notify screen

監査レコード自体が指定するユーザの画面に、監査レコードを表示します。ユーザがログオンしていない場合、表示は保留されずに取り消されます。

syslog *priority*

指定されたログ優先度で、監査レコードを syslog に送信します。

- **LOG_EMERG** - システムが使用できません。
- **LOG_ALERT** - アクションを即座に実行する必要があります。
- **LOG_CRIT** - 致命的な状態。
- **LOG_ERR** - エラー状態。
- **LOG_WARNING** - 警告状態。
- **LOG_NOTICE** - 正常ですが、重大な状態。
- **LOG_INFO** - 情報参照用。
- **LOG_DEBUG** - デバッグレベルのメッセージ。

uni hostname

指定されたホストの Unicenter TNG イベント マネージャに監査レコードを送信します。uni.so 共有ライブラリをロードするように selogrd を設定する必要もあります。このライブラリは、*ACInstallDir*/lib ディレクトリにあります。指定されたホスト上に Unicenter TNG がインストールされていることが確認され、このタスクの実行を選択した場合は、インストール時にこのタスクが実行されます。

各行の正しい順序

include 行および exclude 行は、正しい順序で正しく区切って指定する必要があります。

- 単一の複合フィルタとして使用する一連の行（または単一の行）の前にタイトル行を置き、単一のドットだけの終了行で行を終了する必要があります。たとえば、以下のように指定します。

  dbms login from non-console

  ```
  mail weekwatch
  ```

  include User(dbms*) Class(*LOGIN*).
  ```
  exclude Terminal(console_*).
  .
  ```

タイトル行および終了行を含めたこの一連の行を、ファイルの「*セクション*」と呼びます。

- include 行および exclude 行の両方が、同じセクションの同じ監査レコードに一致した場合は、最後に一致した行が最優先されます。
- いずれの行も特定の監査レコードに一致しない場合は、セクションの最初の行によってそのレコードの処置が決定されます（最初の行が include 行の場合、一致しなければレコードは除外されます。最初の行が exclude 行の場合、一致しなければレコードはルーティングに組み込まれます）。
- include 行および exclude 行がセクションに含まれていない場合は、すべての監査レコードがルーティングに組み込まれます。

セクションの共存

環境設定ファイルの 1 セクション内の各行は、レコードを送信するかどうかについての 1 つの決定を行うために相互に機能しますが、各セクションは完全に独立して機能します。監査レコードがあるセクションによって送信されるかどうかは、同じ監査レコードが別のセクションによって送信されるかどうかには影響しません。

監査レコードの同じ選択内容を複数の宛先に送信できます。また、同じ宛先が監査レコードの複数の選択内容を受信することもできます。

環境設定ファイル（すべてのセクションの include 行および exclude 行の合計）は、64 行を超えることはできません。

コメントの挿入

コメント行を環境設定ファイルに追加するには、行の先頭にセミコロンを付けます。

例 1

環境設定ファイルのサンプルとその説明を以下に示します。

```
; Product : CA Access Control
; Module  : selogrd
; Purpose : route table for audit log routing daemon
;
;-----------------------------------------------------
 Rule#1
 mail jones@admhost
 include       Class(*LOGIN*) Code(D).
 .
 Rule#2
 mail smith
 include       Class(*SURROGATE*) Object(USER.root*).
 .
 Rule#3
 host venus
 exclude       Class(UPDATE SU*).
 .
 Rule#4
 host venus
 include       Class(*PROGRAM*) Object(/usr/bin/ps).
 .
```

最初の 5 行は、コメント行です。

次の 4 行は、Rule#1 という名前の最初のセクションを構成しています。このセクションでは、ログイン要求が拒否された（コード D は拒否を表す）場合、常にログ レコードをアドレス jones@admhost に送信するように selogrd に指示します。

```
Rule#1
mail jones@admhost
include       Class(*LOGIN*) Code(D).
.
```

次のセクションの名前は Rule#2 です。このセクションでは、su コマンドによって root アカウントの使用が試みられた場合（SURROGATE クラスのオブジェクトが su コマンドの対象である場合）、常にログ レコードをアドレス smith に送信するように selogrd に指示します。

```
Rule#2
mail smith
include       Class(*SURROGATE*) Object(USER.root*).
.
```

次のセクションの名前は Rule#3 です。このセクションでは、クラス名が SU という文字列で始まる場合（一致するクラスは SURROGATE および SUDO）を除いて、データベースの管理が試みられた場合は、常にログ レコードをホスト venus 上の収集デーモンに送信するように selogrd に指示します。

```
Rule#3
host venus
exclude       Class(UPDATE SU*).
```

最後のセクションの名前は Rule#4 です。このセクションでは、ps コマンドの使用が試みられた場合は、常にログ レコードをホスト venus 上の収集デーモンに送信するように selogrd に指示します。

```
(Code 1 8pt) Rule#4
host venus
include       Class(*PROGRAM*) Object(/usr/bin/ps).
.
```

例 2

以下の環境設定ファイルは、すべての監査レコードを loghost という端末上の収集デーモンに送信します。

```
; Product : CA Access Control
; Module  : selogrd
; Purpose : route table for audit log routing daemon
;
;-----------------------------------------------------
 Rule#1
 host loghost
 .
```

リターン コード

環境設定ファイルの各タイプのレコードを CA Access Control の 1 つまたは複数のリターン コードに関連付けることができます (リターン コードの完全なリストについては、このセクションの「監査レコードの指定」の *code(return-code)* の説明を参照してください)。以下のテーブルでは、レコード タイプとそれらに関連付けられるリターン コードについて説明します。

レコード タイプ	クラスまたはイベント	関連するリターン コード
ログイン	LOGIN LOGINDISABLE LOGINENABLE	D、P、W I E
ログアウト	LOGOUT	O
TCP/IP	HOST	D、P
リソース クラス	*クラス名*	D、P、W
Watchdog	PROGRAM SECFILE	U U
パスワード管理	PWCHANGE	D
停止	SHUTDOWN	D、S
先頭	START	S
CA Access Control データベース管理	UPDATE	D、F、S

uxauth.ini ファイル

UNIX で該当

uxauth.ini 環境設定ファイルには、UNIX 認証ブローカ の機能を制御するさまざまなパラメータが含まれています。UNIX 認証ブローカ 環境設定ファイルは、UNIX 認証ブローカ の機能を制御する異なるパラメータ セットに関係するセクションに分割されています。

セクション	説明
ad	インストール時に入力したパラメータが設定された、Active Directory トークンを含んでいます。
agent	さまざまな UNIX 認証ブローカ パラメータを制御するトークンを含んでいます。
global	UNIX 認証ブローカ の全般設定を制御するトークンを含んでいます。
libdefaults	Kerberos の全般設定を制御するトークンを含んでいます。
logmgr	UNIX 認証ブローカ ログ記録ユーティリティが使用するトークンを含んでいます。
map	Active Directory の属性名を指定するトークンを含んでいます。
message	メッセージ ファイルを定義するために UNIX 認証ブローカ が使用するトークンを含んでいます。
migrate	移行プロセスで、UNIX 認証ブローカ が使用するトークンを含んでいます。
pam	UNIX 認証ブローカ の PAM モジュールを制御するトークンを含んでいます。
passwd	移行プロセス中のパスワード変更を制御するために、UNIX 認証ブローカ が使用するトークンを含んでいます。
register	UNIX 認証ブローカ の登録機能を制御するトークンを含んでいます。

ad

[ad] セクションは、インストール時に入力したパラメータを持つ Active Directory トークンを含んでいます。

ad_domain

Active Directoryドメインの名前を定義します。

注: この環境設定の値は手動で編集しないでください。この値を設定する場合は、uxconsole -register ユーティリティを使用してください。

ad_gc_port

Active Directory グローバル カタログ サービスが使用するポートを指定します。

デフォルト: 3268

ad_site

Active Directory と通信するために UNIX ホストが使用する DC を含む Active Directory サイトの名前を定義します。

lookup_dc_list 内のすべての値は、この設定の値より優先されます。UNIX ホストは、ignore_dc_list 設定のリストに含まれている DC とは通信しません。

注: この環境設定の値は手動で編集しないでください。この値を設定する場合は、uxconsole -register ユーティリティを使用してください。

デフォルト: none

base_dn

Active Directory サーバの base_dn を定義します。CA Access Control は、この設定の値を自動的に設定します。

computer_container

Active Directory での UNIX ホストの場所を定義します。

デフォルト: cn=Computers

domain_query_order

UNIX 認証ブローカ が Active Directory ドメインに対してユーザとグループをクエリする順序を指定します。

オプション: none – 順序は指定されない、Active Directory ドメインのカンマ区切りリスト

デフォルト: none

group_container

Active Directory で UNIX ユーザを検索する基本エントリを指定します。

制限: コンテナ名 (cn=groups)、または完全な Active Directory クエリには ROOT を指定。

デフォルト: ROOT

group_custom_filter

Active Directory でのグループ検索時に適用するカスタム検索フィルタを指定します。

例: gidNumber=*

デフォルト: none

ignore_dc_list

LDAP 接続で無視する Active Directory のドメイン コントローラを指定します。

オプション: none、完全修飾ホスト名のカンマ区切りリスト

デフォルト: none

ignore_domain_list

ユーザおよびグループをクエリする際に UNIX 認証ブローカ で無視する Active Directoryドメインを指定します。

オプション: none - 現在およびすべての信頼済みドメインをクエリする、all - 信頼済みドメインをクエリしない、無視するドメインのカンマ区切りリスト。

デフォルト: none

ignore_group_container

無視するべき Active Directory グループ コンテナを指定します。コンテナは、カンマ区切りの識別名によって定義されます。

制限: none、識別名のカンマ区切りリスト

デフォルト: none

ignore_user_container

無視するべき Active Directory ユーザ コンテナを指定します。コンテナは、カンマ区切りの識別名によって定義されます。

制限: none、識別名のカンマ区切りリスト

デフォルト: none

ldap_port

Active Directory LDAP サービスが使用するポートを定義します。

デフォルト: 389

lookup_dc_list

LDAP 接続に使用する Active Directory のドメイン コントローラを指定します。ドメイン コントローラのリストを指定した場合、UNIX 認証ブローカ は指定されたドメイン コントローラのみを使用します。使用する DC を指定しない場合、UNIX 認証ブローカ はエンドポイントの物理的な場所に最も近い Active Directory サイトを検出し、そのサイトの DC と通信します。

オプション: none、完全修飾ホスト名のカンマ区切りリスト

デフォルト: none

lookup_domain_list

UNIX 認証ブローカ を登録したドメインとの間で双方向の信頼関係を確立した Active Directory ドメインを指定します。

オプション: none – UNIX 認証ブローカ は自動的に信頼されたドメインを検出する、信頼されたドメインのカンマ区切りリスト

デフォルト: none

user_container

Active Directory で UNIX ユーザを検索する基本エントリを指定します。

制限: コンテナ名、完全な Active Directory クエリ用の ROOT。

デフォルト: ROOT

user_custom_filter

Active Directory でのユーザ検索時に適用するカスタム検索フィルタを指定します。

デフォルト: none

agent

[agent]セクションは、さまざまな UNIX 認証ブローカ パラメータを制御するトークンを含んでいます。

ac_registration_interval

CA Access Control エンドポイントに UNIX 認証ブローカ を登録するための間隔を秒単位で指定します。値が 0 の場合、登録は行われません。

デフォルト: 60

注: UNIX 認証ブローカ は、CA Access Control が UNIX ホストにインストールされている場合のみ、エンドポイントへの登録を試行します。

ad_group_deny_gid_list

ログイン不可能な Active Directory グループの GID を(カンマ区切りで)定義します。

例: ad_group_deny_gid_list = 11,14

注: このパラメータは、完全統合モードでのみ有効です。

デフォルト: トークン未設定(デフォルトなし)

ad_group_minimal_gid

ログイン可能な Active Directory グループの最小 GID を定義します。

注: このパラメータは、完全統合モードでのみ有効です。

デフォルト: トークン未設定(デフォルトなし)

ad_user_deny_uid_list

ログイン不可能な Active Directory ユーザの UID を(カンマ区切りで)定義します。

例: ad_user_deny_uid_list = 12,37

注: このパラメータは、完全統合モードでのみ有効です。

デフォルト: トークン未設定(デフォルトなし)

ad_user_minimal_uid

ログイン可能な Active Directory ユーザの最小 UID を定義します。

注: このパラメータは、完全統合モードでのみ有効です。

デフォルト: トークン未設定(デフォルトなし)

debug_backup

デバッグ メッセージ ファイルをバックアップするかどうかを指定します。

制限: yes、no

デフォルト: yes

debug_backup_file

バックアップ デバッグ メッセージ ファイルの名前を定義します。ファイルへのフルパス名を使用しない場合、UNIX 認証ブローカ は *InstallDir*/log/debug/ ディレクトリにファイルを作成します。

デフォルト: agent_debug.back

debug_file

UNIX 認証ブローカ がデバッグ メッセージを書き込むファイル名を定義します。ファイルへのフルパス名を使用しない場合、UNIX 認証ブローカ は *InstallDir*/log/debug/ ディレクトリにこのファイルを作成します。

デフォルト: agent_debug

debug_size

デバッグ メッセージ ファイルの最大サイズ(メガバイト単位)を定義します。

デフォルト: 512

注: ファイルが最大サイズを超過した場合、エージェントはファイル名をバックアップに変更し、新しいメッセージ ファイルを作成します。

debug_level

デバッグ ファイル内のデバッグ メッセージのレベルを指定します。

制限: disabled、high、medium、low

- disabled - デバッグ メッセージをファイルに書き込みません。
- high - 「高」レベルのデバッグ メッセージをファイルに書き込みます。
- medium - 「高」および「中」レベルのデバッグ メッセージをファイルに書き込みます。
- low - 「高」、「中」、「低」レベルのデバッグ メッセージをファイルに書き込みます。

デフォルト: disabled

debug_zones

サブモジュール(ゾーン)に関するデバッグ メッセージをログに記録するかどうかを指定します。複数のゾーンに関するデバッグ メッセージを記録するには、ゾーン値の合計を指定します。

制限: -1、1、2、4、8、16、または正の値の合計。

- ゾーン -1: すべてのゾーンのデバッグ メッセージを書き込みます
- ゾーン 1: General ゾーンのデバッグ メッセージを書き込みます
- ゾーン 2: Entire 通信ゾーンのデバッグ メッセージを書き込みます
- ゾーン 4: Scheduler ゾーンのデバッグ メッセージを書き込みます
- ゾーン 8: PAM 通信ゾーンのデバッグ メッセージを書き込みます
- ゾーン 16: NSS 通信ゾーンのデバッグ メッセージを書き込みます

例: 「General」および「Scheduler」ゾーンのデバッグ メッセージをログに記録するには、debug_zones の値を 5 に設定します。

デフォルト: -1

default_login_access

ユーザおよびグループのアクセスを定義するルールが存在しない場合、デフォルトのアクセス モードを指定します。

制限: 0 - アクセスなし、1 - アクセス許可

デフォルト: 0

注: このパラメータは、完全統合モードでのみ有効です。

groups_allow_file

ローカル groups.allow ファイルの場所を指定します。

デフォルト: /opt/CA/uxauth/etc/groups.allow

注: このパラメータは、完全統合モードでのみ有効です。

groups_deny_file

ローカル groups.deny ファイルの場所を指定します。

デフォルト: /opt/CA/uxauth/etc/groups.deny

注: このパラメータは、完全統合モードでのみ有効です。

heartbeat_send_interval

CA Access Control 分散ホストにハートビートを送信する頻度（秒単位）を定義します。

デフォルト: 3600

ldap_connection_lifetime

使用されていない LDAP 接続を開いたままにしておく最大時間を定義します。 0 に設定されている場合、LDAP 処理後に、接続は UNIX 認証ブローカによってただちに解除されます。

デフォルト: 60

LIC98Dir

CA ライセンス ライブラリの場所を定義します。

デフォルト: /opt/CA/SharedComponents/ca_lic

login_name_type

マップされたユーザがその UNIX ユーザ名またはエンタープライズ ユーザ名を使用してログインできるかどうかを指定します。

制限: 1 - UNIX ログイン名、2 - エンタープライズ ログイン名

デフォルト: 1

message_read_interval

CA Access Control ポリシー キューの読み取り間隔を秒単位で指定します。

デフォルト: 60

message_read_timeout

CA Access Control ポリシー キューの読み取りタイムアウト期間をミリ秒単位で指定します。

デフォルト: 1

nss_cache_update_grp_login

ユーザ ログインのたびに、NSS がグループ キャッシュを更新するかどうかを指定します。

制限: yes、no

デフォルト: yes

注: このパラメータは、完全統合モードでのみ有効です。

nss_cache_update_grp_mode

グループ キャッシュの更新方法を指定します。

制限: 0 - 更新なし、1 - 増分更新、2 - 完全更新

デフォルト: 1

注: このパラメータは、完全統合モードでのみ有効です。

nss_cache_update_interval

ユーザおよびグループ キャッシュの更新間隔を分単位で定義します。

デフォルト: 60

注: このパラメータは、完全統合モードでのみ有効です。

nss_cache_update_startup

エージェント起動時に NSS ユーザおよびグループ キャッシュを更新する方法を指定します。

制限: 0 - 更新なし、1 - 増分更新、2 - 完全更新

デフォルト: 1

注: このパラメータは、完全統合モードでのみ有効です。

nss_cache_update_usr_login

ユーザ ログインのたびに、NSS がユーザ キャッシュを更新するかどうかを指定します。

制限: yes、no

デフォルト: yes

注: このパラメータは、完全統合モードでのみ有効です。

nss_cache_update_usr_mode

ユーザ キャッシュの更新方法を指定します。

制限: 0 - 更新なし、1 - 増分更新、2 - 完全更新

デフォルト: 1

注: このパラメータは、完全統合モードでのみ有効です。

ntp_server

NTP サーバの名前または IP アドレスを定義します。

デフォルト: none

offline_logon

Active Directory が利用できない場合に、ユーザが継続して UNIX ホストにアクセス可能かどうかを指定します。

制限: no - オフライン接続無効、yes - オフライン接続有効

デフォルト: yes

offline_logon_max_fail

失敗したオフライン ログイン試行の最大数を定義します。

デフォルト: 5

offline_logon_period

成功した最後のオンライン認証の後、オフライン認証が許可される最大期間を日単位で指定します。

デフォルト: 30

report_user_mapped_name

監査ファイル内の表示ユーザ名を指定し、ユーザがマップされたモードであるときに報告します。

制限: no - レポートは UNIX ユーザ名で表示されます。yes - レポートはマップされたユーザ名で表示されます。

デフォルト: no

tgt_renew_interval

TGT (発券許可証) 更新間隔を秒単位で定義します。

デフォルト: 7200

tgt_renewable_lifetime

TGT (発券許可証) 更新最大期間を日数で定義します。

デフォルト: 30d

time_sync_interval

クロック同期間隔を秒数で定義します。

デフォルト: 300

unix_shells

Active Directory ユーザ シェルをサポートされる UNIX シェルに変換するためのルールを定義します。一致するものが存在しない場合、other に定義されたシェルが使用されます。

デフォルト(HP-UX):
sh=/sbin/sh,csh/sbin/csh,bash=/sbin/bash,ksh=/sbin/ksh,tcsh=/sbin/tcsh,other=/sbin/sh

デフォルト(他のすべての OS):
sh=/bin/sh,csh/bin/csh,bash=/bin/bash,ksh=/bin/ksh,tcsh=/bin/tcsh,other=/bin/sh

注: このパラメータは、完全統合モードでのみ有効です。

use_local_policy

ローカル ログイン ポリシー(.allow および .deny ファイル)を使用するかどうかを指定します。

制限: no - エンタープライズ ログイン ポリシーのみを使用します。yes - エンタープライズ ログイン ポリシー、次にローカル ログイン ポリシーを使用します。

デフォルト: no

use_nested_group_acl

ネストされたグループがユーザ アクセス制御リスト(ACL)で使用されるかどうかを指定します。

制限: no - ネストされたグループは使用されません。yes - ネストされたグループは使用されます

デフォルト: yes

use_time_sync

クロック同期オプションを指定します。

制限: no - 手動同期、yes - 自動同期

デフォルト: no

use_wingrp

CA Access Control で使用するために、UNAB が Active Directory グループをデータベースに格納するかどうかを指定します。

CA Access Control が統合されない場合に、部分統合モードで動作するには、UNAB を設定するときにグループ データベース作成を無効にします。

制限: no、yes

デフォルト: yes

users_allow_file

ローカル users.allow ファイルの場所を指定します。

デフォルト: /opt/CA/uxauth/etc/users.allow

注: このパラメータは、完全統合モードでのみ有効です。

users_deny_file

ローカル users.deny ファイルの場所を指定します。

デフォルト: /opt/CA/uxauth/etc/users.deny

注: このパラメータは、完全統合モードでのみ有効です。

user_ticket_cleanup_interval

失効したユーザ チケットのクリーンアップ間隔を秒単位で指定します。

制限: 正の整数

デフォルト: 3600

wingrp_update_interval

UNIX 認証ブローカ Active Directory グループ データベースの更新間隔を分単位で定義します。

デフォルト: 60

注: このパラメータは、完全統合モードでのみ有効です。

wingrp_update_login

ユーザ ログインのたびに、Windows グループ データベースを更新するかどうかを指定します。

制限: yes、no

デフォルト: yes

注: このパラメータは、完全統合モードでのみ有効です。

windgrp_update_mode

UNIX 認証ブローカ Active Directory グループ データベースを更新する方法を指定します。

制限: 0 - 更新なし、1 - 増分更新、2 - 完全更新

デフォルト: 1

注: このパラメータは、完全統合モードでのみ有効です。

wingrp_update_startup

UNIX 認証ブローカ 起動中に Active Directory グループ データベースを更新する方法を指定します。

制限: 0 - 更新なし、1 - 増分更新、2 - 完全更新

デフォルト: 1

注: このパラメータは、完全統合モードでのみ有効です。

working_threads

エージェントで実行するスレッドの数を定義します。

デフォルト: 64

global

[global]セクションは、UNIX 認証ブローカ の一般設定を制御するパラメータを含んでいます。

activation

ホストのアクティベーション レベルを指定します。

制限: 0、1、2

- 0 - 登録なし
- 1 - 登録済み(ローカル ユーザ ストアのみに定義されているユーザのログインを許可)。
- 2 - 有効(ローカル ユーザ ストアに定義されているユーザ、または .allow ファイル、UNIX 認証ブローカ ログイン ポリシーに定義されているユーザのログインを許可)。

デフォルト: 0

CASHCOMP

CA 共有コンポーネントのインストール ディレクトリへのパスを指定します。

デフォルト: /opt/CA/SharedComponents

integration_mode

UNIX 認証ブローカ のインストール方法を指定します。

制限: 1 - 部分統合、2 - 完全統合

注: 部分統合モード(1)は、UNIX ユーザ ストアを保守する場合に使用します。

デフォルト: 2

locale

UNAB エージェントおよびユーティリティ用の言語を定義します。

例: C(英語)、japanese、chinese-s、chinese-t

デフォルト: C

kerberos_configuration

UNIX 認証ブローカ により支援される Kerberos シングル サインオン(SSO)の実装時に、Kerberos の環境設定がどのように使用されるかを指定します。

制限:

- internal -- 設定ファイルとユーザ クレデンシャルのキャッシュが /opt/CA/uxauth および opt/CA/uxauth/etc ディレクトリに格納されるように指定します。
- external -- 設定ファイルとユーザ クレデンシャルのキャッシュがネイティブな場所に格納されるように指定します。

注: このトークンは、UNIX 認証ブローカ 登録中に自動的に設定されます。

注: Linux、HPUX、および Solaris は、ユーザ クレデンシャルを /tmp ディレクトリに格納します。AIX はユーザ クレデンシャルを /var/krb5/security/creds ディレクトリに格納します。

デフォルト: internal

product_path

UNIX 認証ブローカ インストール ディレクトリの名前を定義します。

デフォルト: /opt/CA/uxauth

libdefaults

[libdefaults]セクションには、Kerberos 設定を制御するトークンが含まれています。

default_realm

UNIX 認証ブローカ エンドポイント用のデフォルトの Kerberos 領域を定義します。値「*unregistered*」を指定すると、UNIX 認証ブローカ は Kerberos を使用しません。

デフォルト: unregistered

dns_lookup_kdc

UNIX 認証ブローカ が DNS SRV (サービス ロケータ)レコードを使用して、KDC (鍵配布センター)サービス サービス ロケーションを検索するように指定します。

制限: true、false

デフォルト: true

dns_lookup_realm

UNIX 認証ブローカ が DNS TXT を使用して、領域マッピングするドメインを検索するように指定します。

制限: true、false

デフォルト: false

ticket_lifetime

チケットの有効期限を秒単位で定義します。

デフォルト: 2400

logmgr

[logmgr]セクションは、UNIX 認証ブローカ ログ記録ユーティリティが使用するトークンを含んでいます。

audit_back

監査ログ バックアップ ファイルの完全パスと名前を定義します。

デフォルト: /opt/CA/uxauth/log/uxauth.audit.bak

audit_group

監査ログ ファイルの読み取りを許可されているグループの名前を指定します。

制限: none、group_name

- none - グループのアクセス権限は許可せず、root にのみ監査ログ ファイルの読み取り権限が付与されます。
- *group_name* - 監査ログ ファイルを読み取ることができるグループ名を定義します。

注: UNIX 認証ブローカ が監査ログ ファイルを作成した後にトークンの値を変更する場合、selang コマンドを使用してファイル グループの所有者権限、およびログを読み取ることができるグループのアクセス権限を設定する必要があります。トークンの値を設定した後に作成されたファイルには、指定した権限が付与されています。

デフォルト: none

audit_log

監査ログ ファイルの完全パスと名前を定義します。

デフォルト: /opt/CA/uxauth/log/uxauth.audit

audit_max_files

指定した各バックアップ モードに対して、保存する監査ログ ファイルの最大数を定義します。バックアップ監査ログ ファイルが最大数に達した場合、UNIX 認証ブローカ は新しいファイルの作成時に最も古いバックアップ ファイルを削除します。値に 0 を指定すると、UNIX 認証ブローカ はバックアップ ファイルを蓄積します。

デフォルト: 0

audit_size

監査ログ ファイルの最大サイズ(KB 単位)を定義します。

注: このトークンに指定できる最小値は 50 KB です。

デフォルト: 1024

audit_to_syslog

監査イベントを syslog ファイルにログ記録するべきかどうかを指定します。

制限: yes、no

デフォルト: no

BackUp_Date

監査ログ ファイルをバックアップする間隔を指定します。

制限: none、yes、daily、weekly、monthly

- none - ファイルが audit_size トークンに指定した値に達した場合にバックアップを実行しますが、タイム スタンプはファイル名に追加されません。
- yes - 監査ファイルが audit_size トークンに指定したサイズに達した場合に監査ログ ファイルのバックアップを実行します。
- daily - 監査ログ ファイルのバックアップは、日単位で実行されます。
- weekly - 監査ログ ファイルのバックアップは、週単位で実行されます。

monthly - 監査ログ ファイルのバックアップは、月単位で実行されます。

注: このトークンに daily、weekly、monthly を指定すると、UNIX 認証ブローカ はタイム スタンプを作成し、現在の日付が指定した間隔を超えた場合に監査ログ ファイルをバックアップします。次に、バックアップ ファイルの名前にタイム スタンプを追加します。ただし、現在の日付が指定された間隔を越える前に監査ログ ファイルのサイズが audit_size トークンに指定したサイズに達した場合、UNIX 認証ブローカ は監査ログ ファイルをバックアップしますが、バックアップ ファイルの名前にタイム スタンプは追加されません。このトークンを yes に指定すると、タイムスタンプがバックアップ ファイル名に常に追加されます。

デフォルト: none

error_back

エラー ログ ファイルのバックアップ コピーの完全パスと名前を定義します。

デフォルト: /opt/CA/uxauth/log/uxauth.error.bak

error_group

エラー ログ ファイルの読み取りを許可されているグループ名を指定します。

制限: none、group_name

- none - グループのアクセス権限は許可せず、root にのみエラー ログ ファイルの読み取り権限が付与されます。
- *group_name* - エラー ログ ファイルを読み取ることができるグループ名を定義します。

注: UNIX 認証ブローカ がエラー ログ ファイルを作成した後にトークンの値を変更する場合、selang コマンドを使用してファイル グループの所有者権限、およびログを読み取ることができるグループのアクセス権限を設定する必要があります。トークンの値を設定した後に作成されたファイルには、指定した権限が付与されています。

デフォルト: none

error_log

エラー ログ ファイルの完全パスと名前を定義します。

デフォルト: /opt/CA/uxauth/log/uxauth.error

error_size

エラー ログ ファイルの最大サイズ(KB 単位)を指定します。

注: このトークンに指定できる最小値は 50 KB です。

デフォルト: 50

map

完全統合モードで有効

[map] セクションは、UNIX 認証ブローカ が Active Directory の属性名の指定に使用するトークンを含んでいます。

group_gid_attr_name

UNIX グループ ID を示す Active Directory の属性名を指定します。

デフォルト: gidNimber

group_member_attr_name

グループのメンバをリスト表示する Active Directory 属性名を指定します。

制限: member、memberUid

注: user_name_attr_name=msSFU30Name の場合のみ、値 memberUid を使用します。

デフォルト: member

user_gecos_attr_name

UNIX ユーザの gecos を示す Active Directory の属性名を指定します。

デフォルト: gecos

user_gid_attr_name

UNIX グループ ID を示す Active Directory の属性名を指定します。

デフォルト: gidNumber

user_homedir_attr_name

UNIX ユーザのホーム ディレクトリを示す Active Directory の属性名を指定します。

デフォルト: unixHomeDirectory

user_loginshell_attr_name

UNIX ユーザのログイン シェルを示す Active Directory の属性名を指定します。

デフォルト: loginShell

user_name_attr_name

UNIX ユーザ名に対する Active Directory 属性名を指定します。

デフォルト: sAMAccountName

user_uid_attr_name

UNIX ユーザ ID を示す Active Directory の属性名を指定します。

デフォルト: uidNumber

できませんでした。

[message]セクションは、UNIX 認証ブローカ がメッセージ ファイルの定義に使用するトークンを含んでいます。

filename

メッセージ ファイルの完全パスと名前を定義します。

デフォルト: /opt/CA/uxauth/data/uxauth.msg

migrate

[migrate]セクションは、UNIX 認証ブローカ がマイグレーション処理中に使用するトークンを含んでいます。

conflicts_file

移行競合ファイルの完全パスと名前を定義します。

デフォルト: /opt/CA/uxauth/log/migrate.conflicts

create_ad_groups

同一のグループが Active Directory の中で検索されなかった場合、移行の間に新しい Active Directory グループを作成するかどうかを指定します。

制限: yes、no

デフォルト: yes

disable_mapped_user

部分的に移行された(マップされた)ユーザの UNIX パスワードを無効にするかどうかを指定します。

制限: yes、no

デフォルト: yes

ignore_gecos_conflict

UNIX 認証ブローカ によってマイグレーション処理中に検出される競合に関連した gecos ユーザ属性を無視するかどうかを定義します。

制限: yes、no

デフォルト: yes

is_gid_migration_a_prerequisite

ユーザを移行するために、ユーザのプライマリ グループが必要かどうかを指定します。

制限: yes、no

デフォルト: no

journal

移行ジャーナル ファイルの完全パスと名前を定義します。

デフォルト: /opt/CA/uxauth/log/migrate.journal

minimal_gid

移行処理中に Active Directory に移行される最小グループ ID を定義します。指定した値よりも小さい GID のグループは移行されません。

デフォルト: 101

minimal_uid

移行処理中に Active Directory に移行される最小ユーザ ID を定義します。指定した値よりも小さい UID のユーザは移行されません。

デフォルト: 101

remove_migrated_user

移行の後にローカル ユーザ アカウントを消去するかどうかを指定します。

制限: yes、no

デフォルト: yes

try_to_map_on_conflict

フルレベルの移行処理が失敗する場合、競合するアカウントをマップするかどうかを指定します。

制限: yes、no

デフォルト: yes

passwd

[passwd] セクションは、移行処理時に UNIX 認証ブローカ が使用してパスワード変更を制御するトークンを含んでいます。

YpGrpCmd

NIS グループ マップを生成するコマンドを定義します。

デフォルト: make group

YpMakeDir

NIS マップを作成するときに使用する makefile ディレクトリを定義します。

デフォルト: /var/yp

YpPassCmd

NIS パスワード マップの作成に使用するコマンドを指定します。

デフォルト: make passwd

YpServerGroup

NIS サーバ上のグループ ファイルの完全パス名を指定します。

デフォルト: /etc/group

YpServerPasswd

NIS サーバ上のパスワード ファイルの完全パス名を指定します。

デフォルト: /etc/passwd

YpServerSecure

オペレーティング システムのパスワード ファイルへの完全パス名を指定します。

デフォルト(AIX): /etc/security/passwd

デフォルト(HP-UX): /.secure/etc/passwd

デフォルト(Solaris): /etc/shadow

デフォルト(他のすべての OS): /etc/shadow

pam

[pam] セクションは、PAM モジュールと対話するために UNIX 認証ブローカ が使用するトークンを含んでいます。

debug_mode_for_user

PAM モジュールがログイン中にユーザ画面にメッセージを出力できるかどうかを定義します。

オプション: yes、no

デフォルト: yes

pam_exit_on_deny

企業またはローカルのポリシー設定、または Active Directory アカウント状態のためにログインが拒否された場合の PAM モジュールの動作を定義します。

オプション: yes − PAM モジュールはシーケンスを閉じ、他の PAM モジュールが認証ユーザを認証しないようにします。no - PAM モジュールはシーケンスを閉じず、他の PAM モジュールがユーザを認証できるようにし、ログイン サーバが PAM シーケンス コールを再試行することを許可します。

デフォルト: yes

pam_receive_timout

UNIX 認証ブローカ エージェント（uxauthd）の応答を PAM モジュールが待機する時間を秒数で指定します。

制限: 正の整数

デフォルト: 10

register

[register]セクションは、UNIX 認証ブローカ 登録機能を制御するトークンを含んでいます。

start_uxauthd

インストール処理の最後に uxactivate ユーティリティを実行するかどうかを指定します。

制限: yes、no

デフォルト: yes

verbose

インストール処理中に使用する詳細レベルを定義します。

デフォルト: 0

UNIX 認証ブローカ 競合ファイル

ユーザおよびグループを Active Directory に移行しようとした後に、UNIX 認証ブローカ 競合ファイルが作成されます。このファイルには、移行処理中に UNIX 認証ブローカ によって検出された競合の詳細が記述されます。このファイルを確認して、報告されている競合を解決します。

このファイルには以下のフィールドが含まれています。

`Solution Entity Type、Solution Entity Name、Solution Operation、Solution AD Mapped Name、Conflicts、UID、Home Directory、GID、Member of、Members、GECOS`

Solution Entity Type（**ソリューション エンティティタイプ**）

移行するエンティティのタイプを表示します。

制限: ユーザ、グループ

Solution Entity Name（**ソリューション エンティティ名**）

エンティティの名前が表示されます。

Solution Operation（**ソリューション操作**）

エンティティ移行ステータスを表示します。

制限: Keeplocal、Migrate、Map

Solution AD Mapped Name（**ソリューション AD マップ名**）

ローカル アカウントのマップ先となる Active Directory アカウント名を表示します。

Conflicts（**競合**）

移行中に発見された競合を表示します。

UID

ユーザ ID を表示します。

Home Directory（**ホーム ディレクトリ**）

ユーザ ホーム ディレクトリを表示します。

GID

グループ ID を表示します。

Member Of（**所属先**）

ユーザが所属するグループを表示します。

Members（**メンバ**）

グループ内のメンバであるユーザのリストを表示します。

GECOS

GECOS 情報を表示します。

特権ユーザ パスワード管理 SSH デバイス XML ファイル

SSH Device XML ファイルによって、特権ユーザ パスワード管理 の SSH デバイス エンドポイントへの接続方法の設定、ユーザ アカウントの検出、およびエンドポイント上の特権アカウント パスワードの変更を行うことができます。

異なる SSH Device XML ファイルで、SSH デバイス エンドポイントの異なるタイプとの連携を設定します。たとえば、aix_connector_conf.xml ファイルは AIX エンドポイントへの接続を設定します。また、device_connector_conf.xml ファイルはルータなどの SSH デバイスへの接続を設定します。

注: SSH デバイス XML ファイル タイプの詳細については、「*エンタープライズ管理ガイド*」を参照してください。

SSH デバイス XML ファイルは、以下のディレクトリにあります。

ACServerInstallDir/Connector Server/conf/override/sshdyn

必要に応じて、ユーザの組織の要件に合わせて SSH デバイス XML ファイルをカスタマイズできます。

構造

SSH デバイス XML ファイルには以下のエレメントが含まれています。

- <class name="SSHConnectionManager"> -- SSH 接続を管理するパラメータが含まれています。
- <class name="CommandProcessor"> -- 接続設定を指定するパラメータが含まれています。
- <class name="CommandSet"> -- 特権ユーザ パスワード管理 がエンドポイント上で実行するコマンドを指定する配列エレメントが含まれています。

<class name="CommandSet"> エレメントには、以下に示すように、コマンド セットをグループ化する配列エレメントが含まれています。

- <array name="oGetUsers"> -- ユーザを取得するために 特権ユーザ パスワード管理 が実行するコマンドが含まれています。
- <array name="oChangePassword"> -- ユーザ パスワードを変更するために 特権ユーザ パスワード管理 が実行するコマンドが含まれています。
- <array name="oSubstituteUser"> -- 特権ユーザ パスワード管理 が別のユーザに対して su を実行するコマンドが含まれています。

  注: <array name="oSubstituteUser"> エレメントは、aix_connector_conf.xml、checkpoint_connector_conf.xml、および ssh_connector_conf.xml ファイルに対してのみ有効です。

各配列エレメントには、複数の <item> エレメントが含まれています。<項目> エレメントは、特権ユーザ パスワード管理 がエンドポイント上で実行する特定のコマンド用のパラメータを定義します。たとえば、<array name="oGetUsers"> エレメント内の <item> エレメントによって、以下が指定されます。

- ローカル ユーザを取得するために 特権ユーザ パスワード管理 が実行するコマンド
- 特権ユーザ パスワード管理 が応答を待機する時間の長さ
- 処理を続行する前に、特権ユーザ パスワード管理 が受信待機するテキスト文字列
- コマンドの失敗を示す応答内のテキスト文字列

注: SSH Device XML ファイル内の <item> エレメントが SSH Device エンドポイントとの連携を設定する方法の例については、「*エンタープライズ管理ガイド*」を参照してください。

以下のように、入れ子になったパラメータを使用して、各エレメントの設定を定義します。

- <class name="SSHConnectionManager"> および <class name="CommandProcessor"> エレメントには、接続設定を定義するパラメータが含まれています。
- <item> エレメントには、特定のコマンドのパラメータを定義するパラメータが含まれています。

入れ子のパラメータは、それぞれ以下のような形式になっています。

```
<param name="name" value="value" />
```

以下の SSH デバイス XML ファイルの一部は、エレメントがネストされる方法を示しています。

```
<package name="com.ca.jcs.sshdyn">
        <class name="SSHConnectionManager">
                <param name="name" value="value" />
        </class>
</package>
<package name="com.ca.sessame.conn.unix">
        <class name="CommandProcessor">
                <param name="name" value="value" />
        </class>
        <class name="CommandSet">
                <instance name="ssh">
                        <array name="oGetUsers">
                                <item>
                                        <param name="name" value="value" />
                                </item>
                        </array>
                        <array name="oChangePassword">
                                <item>
                                        <param name="name" value="value" />
                                </item>
                        </array>
                        <array name="oSubstituteUser">
                                <item>
                                        <param name="name" value="value" />
                                </item>
                        </array>
                </instance>
        </class>
</package>
```

エレメント

SSHConnectionManager

SSH 接続を管理するために 特権ユーザ パスワード管理 が使用する設定を指定します。

このクラス エレメントには、以下のパラメータが含まれています。

I_CONNECTIONS

エンドポイントへの同時接続数を定義します。

デフォルト: 10

CommandProcessor

SSH デバイス エンドポイントに接続するために、特権ユーザ パスワード管理が使用する設定を指定します。

このクラス エレメントには、以下のパラメータが含まれています。

bToLog

特権ユーザ パスワード管理 がメッセージを sLogFileName に書き込むかどうかを指定します。

制限: true、false

デフォルト: true

sLogFileName

ログ ファイルへの相対パス名を定義します。

デフォルト: ..¥logs¥uxlog.txt

limitResultCharsToLog

CA Access Control が各接続のログ ファイルに書き込む最大文字数を定義します。

デフォルト: 1500

bSkipOperationAdminTestConnection

指定内容

制限: true、false

デフォルト: true

maxTimeLimit

特権ユーザ パスワード管理 が値を待機する最大時間をミリ秒単位で定義します。

デフォルト: 1500

waitIntervalDefault

特権ユーザ パスワード管理 が待機する時間をミリ秒単位で定義します。

デフォルト: 500

login_str

ユーザ名の Telnet リクエスト コマンドを指定します。

例: login

password_str

パスワードの Telnet リクエスト コマンドを指定します。

例: password

AYT_answer

デバイスの Telnet コマンド "Are You There" への応答を指定します。

デフォルト: Solaris-Yes、Linux-yes、AIX-here

注: 環境設定がそれぞれ異なるため、各 SSH デバイスの AYT コマンドへの応答が異なります。これらにしたがって、SSH XML ファイルを変更できます。

形式を検出するには、デバイスに対して Telnet セッションを開き、以下を実行します。

```
^+]
send ayt
```

iPort

SSH ポート番号を定義します。

注: デフォルトでは、このパラメータはコメントアウトされます。

デフォルト: 22

CommandSet

特権ユーザ パスワード管理 がエンドポイント上で実行するコマンドを指定します。

このクラス エレメントには、特権ユーザ パスワード管理 がエンドポイント上で実行するコマンドをグループ化する配列エレメントが含まれています。

oGetUsers

ユーザを取得するために 特権ユーザ パスワード管理 が実行するコマンドを指定します。

この配列エレメントには、ユーザを取得するために 特権ユーザ パスワード管理 が実行する特定のコマンドのパラメータを定義するアイテム エレメントが含まれています。

oChangePassword

ユーザ パスワードを変更するために 特権ユーザ パスワード管理 が実行するコマンドを指定します。

この配列エレメントには、ユーザ パスワードを変更するために 特権ユーザ パスワード管理 が実行する特定のコマンドのパラメータを定義するアイテム エレメントが含まれています。

oSubstituteUser

特権ユーザ パスワード管理 が su を実行して別のユーザの代理実行を行うコマンドを指定します。

この配列エレメントには、su を実行して別のユーザの代理実行を行うために 特権ユーザ パスワード管理 が実行する特定のコマンドのパラメータを定義するアイテム エレメントが含まれています。

注: このエレメントは、aix_connector_conf.xml、checkpoint_connector_conf.xml、および ssh_connector_conf.xml ファイルでのみ有効です。

item

特権ユーザ パスワード管理 がエンドポイント上で実行する特定のコマンドのパラメータを指定します。

各アイテム エレメントには、以下のパラメータが含まれる場合があります。

sCommand

特権ユーザ パスワード管理 がエンドポイントに送信するコマンドを定義します。

iWait

次の手順を実行するまで 特権ユーザ パスワード管理 が待機する間隔をミリ秒単位で定義します。

デフォルト: 500

sWaitForText

sCommand 内に定義されたコマンドへの応答として 特権ユーザ パスワード管理 が受信待機するテキスト文字列を定義します。

sFailureResult

特権ユーザ パスワード管理 がエンドポイントから受信する、コマンドが失敗したことを示すテキスト文字列を定義します。

sToFilterOut

特権ユーザ パスワード管理 がエンドポイント出力から削除するテキスト文字列を定義します。

bHideSentLog

ログ ファイルにコマンドを書き込むかどうかを指定します。

制限: true - 特権ユーザ パスワード管理 はコマンドをログ ファイルに書き込まない、false - 特権ユーザ パスワード管理 はコマンドをログ ファイルに書き込む

デフォルト: true

sTrueResultRegex

(オプション)コマンド実行結果を指定された文字列と比較するように指定します。結果が文字列と一致しない場合、エラー メッセージが表示されます。

注: デフォルトでは、このパラメータはコメントアウトされます。

iXMLVersion

XML ファイルのバージョンを示します。XML バージョンは、SSL コネクタ内に定義されている XML バージョンより新しいものは使用できません。

デフォルト: 0

ToReport

XML プロセス データを $XML_NAME..lodaing_report.xml にログ記録するかどうかを指定します。ログ ファイルは、以下のディレクトリにあります。

ACServerInstallDir/Connector Server/conf/override/sshdyn

制限: true、false

デフォルト: true

FileIsLoaded

XML ファイルが正常にロードされたことを示します。

デフォルト: OK

特権ユーザ パスワード管理 自動ログイン アプリケーション Visual Basic スクリプト

特権ユーザ パスワード管理 自動ログイン アプリケーションでは、Visual Basic スクリプトを使用して自動ユーザ ログインを有効にします。新しいログイン アプリケーションを作成または既存のログイン アプリケーションを変更するために Visual Basic スクリプトをカスタマイズできます。

特権ユーザ パスワード管理 自動ログイン アプリケーション スクリプトには、エンタープライズ管理サーバからクライアント マシン上へのダウンロード時に ActiveX によって値が置換される変数が含まれています。エンタープライズ管理サーバによりスクリプトが処理され、キーワードが値に置換されます。次に、ActiveX によりクライアント マシン上でスクリプトが実行されます。

特権ユーザ パスワード管理 自動ログイン アプリケーション スクリプトは以下のディレクトリにあります。

JBOSS_HOME/server/default/deploy/IdentityMinder.ear/config/sso_scripts

要素

特権ユーザ パスワード管理 ログイン アプリケーション スクリプトには以下のキーが含まれます。

#host#

ユーザが自動的にログインするエンドポイントの名前を指定します。

#username#

チェックアウトされた特権アカウントを指定します。

#password#

チェックアウトする特権アカウントのパスワードを指定します。

#userdomain#

（Active Directory）特権アカウントドメイン名を指定します。

#isActiveServletUrl#

ACLauncher ActiveX でアカウント パスワード チェックイン イベントを確認するために使用する URL を指定します。

#CheckinUrl#

ACLauncher ActiveX で、ユーザがエンドポイントからログアウトした場合にアカウント パスワードをチェックインするために使用する URL を指定します。

#SessionidUrl#

ACLauncher ActiveX で、セッションが ObserverIT Enterprise に記録された場合に記録されたセッション ID を送信するために使用する URL を指定します。

特権ユーザ パスワード管理 自動ログイン アプリケーションの以下のコードの一部は、変数がどのように表示されるかを示しています。

```
Set pupmObj = CreateObject("ACLauncher.ACWebLauncher")
hwnd = pupmObj.LauncheRDP("#host#", "#userDomain#¥#userName#", "#password#")
' Set window close event
pupmObj.SetWindowCloseEvent(hwnd)
' Set server checkin event
pupmObj.SetServerCheckinEvent("#isActiveServletUrl#")
' Wait until one of the events signaled
rc = pupmObj.WaitForEvents()
If rc = 1 Then 'user has closed the window - notify the server side
        pupmObj.SendCheckinEvent("#CheckinUrl#")
ElseIf rc = 2 Then 'timeout elapsed - close the window
    call pupmObj.CloseWindow(hwnd, 0)
ElseIf rc = 3 Then 'the account was checkedin at the server side - close the window
    call pupmObj.CloseWindow(hwnd, 120)
End If
```

構造

特権ユーザ パスワード管理 の自動ログイン アプリケーション スクリプトの構造は以下のとおりです。

- COM オブジェクトの初期化

  ```
  Set pupmObj = CreateObject("ACLauncher.ACWebLauncher")
  ```

- 自動ログイン アプリケーションの実行

  ```
  hwnd = pupmObj.LauncheRDP("#host#", "#userDomain#¥#userName#", "#password#")
  ```

- 実行後タスク -- パスワード チェックイン、対話型ログイン、またはタイムアウト

  ```
  ' Wait until one of the events signaled
  rc = pupmObj.WaitForEvents()
  If rc = 1 Then 'user has closed the window - notify the server side
      pupmObj.SendCheckinEvent("#CheckinUrl#")
  ElseIf rc = 2 Then 'timeout elapsed - close the window
      call pupmObj.CloseWindow(hwnd, 0)
  ElseIf rc = 3 Then 'the account was checkedin at the server side - close the window
      call pupmObj.CloseWindow(hwnd, 120)
  End If
  ```

ログイン アプリケーション セッションを記録するには、スクリプトに記録命令を、以下に従って追加します。

- 初期化セクションで、以下の作業を実行します。以下を追加します。

```
Set observeIT = CreateObject("ObserverIT.AgentAPI.Proxy")
```

- アプリケーション実行セクションで、以下を追加します。

```
'Get application processid
processID = pupmObj.GetWindowProcessID(hwnd)
'Start recording
sessionid = observeIT.StartByProcessID(processID, true)
'Send the sessions if to the ENTM server
pupmObj.AssignSessionID "#SessionidUrl#" ,sessionId
```

- 実行後セクションで、以下を追加します。

```
'Stop recording

observeIT.StopBySessionId sessionId, true
```

メソッド

ACLauncher ActiveX では以下のメソッドを使用します。

```
LaunchеRDP (BSTR bsHostName, BSTR bsUserName, BSTR bsPassword, VARIANT *phWindow);
```

入力クレデンシャルでリモート デスクトップ セッションを開始し、リモート デスクトップ ウィンドウ ハンドルを返します。

例: Dim test Set test = CreateObject("ACLauncher.ACWebLauncher") Hwnd = test.LaunchеRDP("hostname.com", "hostname¥administrator", "password")

```
LaunchePUTTY (BSTR bsHostName, BSTR bsUserName, BSTR bsPassword, VARIANT *phWindow);
```

入力クレデンシャルで PuTTY セッションを開始し、PuTTY ウィンドウ ハンドルを返します。

例: Dim test Set test = CreateObject("ACLauncher.ACWebLauncher") Hwnd = test. LaunchePUTTY ("hostname.ca.com", "root", "password")

```
LaunchеProcessAsUser (BSTR bsApplication, BSTR bsCommandline, BSTR bsUsername, BSTR bsPassword, VARIANT *phWindow);
```

入力クレデンシャルでプロセスを開始し、プロセス ウィンドウ ハンドルを返します。

例: Dim test Set test = CreateObject("ACLauncher.ACWebLauncher") Hwnd = test.LaunchеProcessAsUser("cmd.exe", "/k echo This console is run under %USERNAME% account...", "administrator" , "password")

```
GetWindowProcessID(VARIANT *phWindow, LONG *pProcessID);
```

指定されたウィンドウ ハンドルのプロセス ID を返します。

例: Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") id = test.GetWindowProcessID(hwnd) test.Echo "Process ID = " & id

```
GetWindowTitle(VARIANT *phWindow, BSTR *pbsTitle);
```

指定されたウィンドウ ハンドルのタイトルを返します。

例: Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") title = test.GetWindowTitle(hwnd)

```
CloseWindow(VARIANT *phWindow, LONG Seconds);
```

ウィンドウが X 秒後に閉じることを通知するメッセージを含むダイアログ ボックスを表示し、指定されたウィンドウ ハンドルのウィンドウを閉じます。

例: Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") test.Sleep(5000) test.CloseWindow(hwnd, 60)

```
SetTimeoutEvent(LONG seconds);
```

"WaitForEvents" メソッドのタイムアウトを指定します。タイムアウト値に達すると、WaitForEvents メソッドは、タイムアウトに達したことを示す戻り値で、ブロックしているコールから戻ります。

例: Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") test.SetTimeoutEvent(10)

```
SetWindowCloseEvent(VARIANT *phWindow);
```

"WaitForEvents" メソッドに対してウィンドウを閉じるイベントを指定します。ウィンドウが閉じられた後、"WaitForEvents" メソッドは、ブロックしているコールから戻り、ウィンドウが閉じられたことを示す戻り値を表示します。

例: Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") test.SetWindowCloseEvent(hwnd)

```
SetServerCheckinEvent(BSTR bsURL);
```

特権ユーザ パスワード管理 チェックイン イベントを、実行ブロック条件として設定します。ActiveX は 5 秒ごとに 特権ユーザ パスワード管理 をクエリします。

例: Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") test.SetServerCheckinEvent("http://server.com/__azy?djfhwek5jy34brfhwkeb") (replace with variable)

```
WaitForEvents(VARIANT *pRetVal);
```

レジスタ条件の 1 つに該当するまで、スクリプトの実行をブロックします。

オプション: 1 -- ユーザによってウィンドウが閉じられました、2 -- タイムアウトが経過しました、3 -- がサーバ側でチェックインされました

例: Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") test.SetServerCheckinEvent("http://server.com/__azy?djfhwek5jy34brfhwkeb")

test.SetWindowCloseEvent(hwnd) test.SetTimeoutEvent(360) rc = test.WaitForEvents() If rc = 3 Then call test.CloseWindow(hwnd, 10) End If

```
SwitchToThisWindow(VARIANT *phWindow);
```

ウィンドウを Z 順の最前面に移動させます

例: Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") test.SwitchToThisWindow(hwnd)

```
SendCheckinEvent(BSTR bsURL);
```

ユーザがウィンドウを閉じたら、チェックイン イベントを送信します。

例: Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password")

```
Sleep(LONG milliseconds);
```

スクリプトの実行を一時停止します。

Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.Sleep(2000)

```
Echo(VARIANT* pArgs);
```

メッセージを画面に出力します、

```
Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd =
test.Echo("Password Checkin")
```

第 4 章: レジストリ エントリ

このセクションには、以下のトピックが含まれています。

CA Access Control のレジストリ

CA Access Control は、以下のレジストリ キーの下に、レジストリ エントリを作成します。このレジストリ キーは、CA Access Control エンドポイント管理 リモート環境設定の ACROOT と呼ばれます。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl

メインのレジストリ キーには、以下のレジストリ エントリが含まれています。

CurrentVersion

製品の現在のバージョンとビルドを定義します。

Encryption Package

対称暗号化の実装に使用する DLL の完全パス名を定義します。

デフォルト: *ACInstallDir*¥bin¥aes256enc.dll

<Build_Number>

CA Access Control は製品の現在のバージョンおよびビルドを以下のレジストリ キーに定義します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥*Build_Number*

このオプションは内部使用専用です。

AccessControl

CA Access Control は、使用する汎用設定を以下のキーの下で保守します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥AccessControl

AccessControl レジストリ キーには、以下のレジストリ エントリが含まれています。

AccessControl Services

CA Access Control のサービス名および実行可能ファイルのリストを定義します。

デフォルト: 「SeOSAgent;SeOS Agent」、「SeSudo;SeOS TD"」、「seoswd;SeOS Watchdog」

注: エンタープライズ管理サーバの一部であるエンドポイントには、このレジストリ エントリの以下のデフォルト値も含まれています。"Sepmdd;SeOS Policy Model(DMS__)"、"Sepmdd;SeOS Policy Model(DH__)"、"Sepmdd;SeOS Policy Model(DH__WRITER)"

admin_default_check

リモート端末リソースの *defaccess* プロパティが *all* に設定されているか、または _default 端末リソースへのアクセスが許可されている場合でも、CA Access Control による CA Access Control サーバへのログイン アクセスを拒否するかどうかを指定します。

下位互換性のために維持。

デフォルト: 0（アクセスを拒否しません）

AdminInst

内部的使用のみ。

デフォルト: 0

auth_login

管理目的でユーザを認証する方法を指定します。

有効な値は以下のとおりです。

native - ネイティブのオペレーティング システム（OS）のユーザを対象に、OS に対してユーザのパスワードをチェックします。

eTrust - ネイティブのオペレーティング システムに存在していないユーザを対象に、CA Access Control データベースに対してユーザのパスワードをチェックします。

デフォルト: native

auth_module_names

ネイティブ認証以外の認証が許可されている言語クライアント モジュールのリスト。クライアント モジュール名は、認証前に、LCA API 呼び出し内のクライアントによって設定されます。このレジストリ値を変更すると、非ネイティブ モードで認証する他のクライアントに影響する可能性があります。

デフォルト: none

CPF_TARGETS

CPF サービスが通信するターゲット メインフレーム CPF システム(リモート CPF ターゲット ノード)のリスト。

デフォルト: ACF2 TOP RACF

eACPipePrefix

新しいパイプ サーバとパイプ クライアントが使用するパイプ名の一部としての値。システムが CA Access Control の古いクライアントを保持している場合は、古いクライアントが機能するためにこの値が必須になります。それ以外の場合は、この値をより安全なパイプ名に変更してください。

デフォルト: SEOS

eACPipeTranslator

使用されなくなりました。

full_year

secons -tv、seaudit、および dbmgr ユーティリティを使用する際に、年を 2 桁で表示するか(値が no の場合)、4 桁で表示するか(値が yes の場合)を指定します。

デフォルト: yes

GenerateMemDump

CA Access Control サービスのコード例外を処理したときに、CA Access Control がメモリ ダンプ(1)を作成するかどうかを指定します。CA Access Control は、*ACInstallDir*¥bin¥*serviceProcessName*.*PID*.dmp にメモリ ダンプを作成します。ダンプの名前は、SeOSAgent.5704.dmp のようになります。

注: メモリ ダンプはユーザ モードでのみ使用可能であり、カーネル モードでは使用できません。

デフォルト: 1

parent_pmd

このワークステーションが *pmdb@host* 形式でサブスクライブする PMDB。このデータベースは、ローカル データベースを更新できる唯一の Policy Model です。

値を指定しない場合、ワークステーションはどの PMDB からの更新情報も受け付けません。エントリを _NO_MASTER_ に設定すると、すべての PMDB でこのワークステーションを更新できます。

デフォルト値なし

例: pmd1@host1;pmd2@host1;pmd3@host2

passwd_pmd

pmdb@host 形式での Policy Model のパスワード置換のターゲット。

parent_pmd レジストリ値と passwd_pmd レジストリ値に同じ値を指定できます。parent_pmd レジストリ値と passwd_pmd レジストリ値が異なる場合、passwd_pmd データベースが更新情報を parent_pmd データベースに送信し、更新内容を伝達します。したがって、parent_pmd データベースは passwd_pmd データベースのサブスクライバである必要があります。

この値を設定しない場合、parent_pmd レジストリ キーの値が継承されます。

デフォルト値なし

ReverseIpLookup

ユーザがその端末からログインする権限があるかどうかを判定するために、クライアントの IP アドレスを解決する方法を制御します。

有効な値は以下のとおりです。

yes - クライアントの開いているソケットの IP アドレスを調べ、それに従ってログオンが許可されます。

no - クライアントから受け取ったホスト名を使用しますが、ホスト名は解決されません（TERMINAL クラスを無効にすることにより、同じ結果を得られます）。

デフォルト: yes

secondary_pmd

パスワード置換のセカンダリ ターゲットとして使用される Policy Model データベース。

デフォルト値なし

SeOSPath

CA Access Control のインストール先ディレクトリ。

SplashEnable

対話形式(GINA)のログイン プロセス中に保護メッセージを有効または無効にするための切り替え設定。このメッセージは、CA Access Control がコンピュータを保護することをユーザに通知します。値 1 はメッセージが有効であることを示し、値 0 はメッセージが無効であることを示します。

デフォルト: 1

TNG_Environment

Unicenter 統合を有効または無効にするための切り替え設定。

値: 1 — Unicenter 統合を有効にし、Unicenter TNG クラスでデータベースを作成します。0 — Unicenter 統合を無効にし、Unicenter TNG クラスなしでデータベースを作成します

デフォルト: 0

TrustedServices

trusted プログラムのリスト。

デフォルト値なし

UseFsiDrv

ドライバのロードを有効または無効にするための切り替え設定。

値: 1 — ドライバのロードを有効にします。0 — ドライバのロードを無効にします

デフォルト: 1

Agent

CA Access Control は、使用するエージェント設定を以下のキーの下で保守します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Agent

Agent キー エントリ（およびサブキー）は、内部でのみ使用されます。

ShutdownWaitingTimeout

CA Access Control エージェントがそのコンポーネントの正常シャットダウンを待機するタイムアウト期間をミリ秒単位で定義します。CA Access Control コンポーネントが正常にシャット ダウンしない場合、エージェントは強制シャットダウンを行います。

注: このレジストリ エントリは内部使用のみです。

デフォルト: 60000

Applications

CA Access Control は、使用するアプリケーション設定を以下のキーの下で保守します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Applications

Applications レジストリ キーには、以下のレジストリ エントリが含まれています。

OperationMode

制御されているアプリケーション モードがアクティブ（1）かどうかを指定します。

この値は 1 に設定する必要があります。

デフォルト: 1

<Application_Name>

CA Access Control は、使用する特定のアプリケーション設定を以下のキーの下で保守します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Applications¥*Application_Name*

それぞれの Applications¥*Application_Name* レジストリ キーには、以下のレジストリ エントリが含まれています。

ApplicationName

制御されるプロセスの名前を定義します。

完全パス名を *device*:¥*path*¥*name*.exe 形式で指定する必要があります。

デフォルト: 実行可能ファイルのフルパス名

引数

アプリケーションの起動時に CA Access Control が使用する引数を定義します。

デフォルト: ""(引数なし)

Desktop

ワークステーションおよびセッション名を定義します。

デフォルト: デフォルトなし

OperationMode

アプリケーションがアクティブ(1)かどうかを指定します。

デフォルト: 1

RestartApplication

アプリケーションが終了または停止した場合に再起動する(1)かどうかを指定します。

デフォルト: 1

StartAplication

Watchdog が起動したときに、CA Access Control がアプリケーションを起動する(1)かどうかを指定します。

デフォルト: 1

WorkingDirectory

アプリケーションが起動される作業ディレクトリを定義します。

デフォルト: *ACInstallDir*¥bin

クライアント

CA Access Control は、使用するクライアント アプリケーション設定を以下のキーの下で保守します。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Client
```

Client レジストリ キーには、以下のレジストリ エントリが含まれています。

ConnectTo

CA Access Control のクライアント管理アプリケーション(selang など)がデフォルトで接続するホスト名を定義します。

デフォルト: localhost

Standalone

CA Access Control は、使用するスタンドアロン クライアント アプリケーション設定を以下のキーの下で保守します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Client¥Standalone

Client¥Standalone レジストリ キーには、以下のレジストリ エントリが含まれています。

full_login_check

追加のユーザ プロパティ(grace や max_login)を確認し、スタンドアロンのアプリケーションからの接続要求中にログインを実行するために、CA Access Control サーバを有効にするための切り替え設定。

この値は、リモート パスワードの有効期限が切れる直前にパスワードを変更する場合に役立ちます。

値が 1 に設定されている場合、チェックが有効になります。

デフォルト: 0

Common

CA Access Control は、以下のキーの下にある共通コンポーネントで使用される設定を管理します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Common

Common キーには、レジストリ エントリが含まれていません。このキーには、共通コンポーネント用のレジストリ サブキーが存在します。

AgentManager

CA Access Control は、エージェント マネージャ関連の設定を以下の場所に保存します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥common¥AgentManager

エージェント マネージャ レジストリ キーには、以下のレジストリ エントリが含まれています。

RefreshTimeout

エージェント マネージャの更新間隔を秒単位で定義します。

タイプ: REG_DWORD

デフォルト: 600

StandAloneService

このサービスがスタンドアロン サービスかどうかを指定します。

タイプ: REG_DWORD

デフォルト: 0

TraceEnabled

CA Access Control エージェント マネージャトレース モードを定義します。

オプション: 0、1

デフォルト: 1

WorkSpace

CA Access Control エージェント マネージャ ワークスペースの完全パス名を指定します。

デフォルト:
¥ProgramFiles¥CA¥AccessControlShared¥APMS¥AccessControl¥Data¥AgentManager

Plugins

CA Access Control は、プラグインによって使用される設定を以下のキーの下に保存します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Common¥AgentManager¥Plugins

Plugins キーには、レジストリ エントリが含まれていません。このキーには、プラグイン用のレジストリ サブキーが存在します。

AccountManager

CA Access Control は、アカウント マネージャ関連の設定を以下の場所に保存します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥common¥AgentManager¥Plugins¥AccountManager

アカウント マネージャ レジストリ キーには、以下のレジストリ エントリが含まれています。

Interval

プラグイン スケジュールを秒単位で定義します。

デフォルト: 1

注: ScheduleType が 2 に設定されている場合にのみ適用されます。

OperationMode

プラグインの操作モードを定義します。

オプション: 0 - プラグイン無効、1 - プラグイン有効

デフォルト: 1

PluginPath

プラグインの完全パス名を定義します。

タイプ: REG_SZ

デフォルト:
¥ProgramFiles¥CA¥AccessControlServer¥APMS¥AccessControl¥bin¥AccountManager.dll

QueryFilter

メッセージ キューの受信キュー フィルタに追加される追加値を指定します。

オプション: ENDPOINT_CUSTOM 1...5=、ENDPOINT_OWNER=、ENDPOINT_DEPARTMENT=

以下の点に注意してください。

- プロパティ値はアポストロフィで囲みます。
- 複数のプロパティを指定する場合は、オペランド AND および OR を使用します。
- 必要に応じて丸かっこを使用します。

Schedule

プラグイン スケジューリング文字列を定義します。

デフォルト: 00:00@Sun.Mon,Tue,Wed,Thu,Fri,Sat

注: ScheduleType が 2 に設定されている場合にのみ適用されます。

ScheduleType

プラグイン スケジュール タイプを定義します。

オプション: 0 - 1 回実行、1 - オン デマンドで実行、2 - 指定間隔で実行、3 - スケジュールにしたがって実行

デフォルト: 1

通信

CA Access Control は、使用するメッセージ キュー サーバ通信設定を以下のキーの下で保守します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥common¥communication

communication レジストリ キーには、以下のレジストリ エントリが含まれています。

certificate

SSL 接続に対する証明書ファイルを定義します。

制限: 証明書データが含まれているファイルへの完全パス名。

Distribution_Server

配布サーバの URL を定義します。カンマ区切りリストに複数の配布サーバを定義できます。

例: tcp://ds.comp.com:7222, tcp://ds_dr.comp.com:7222

デフォルト: none

endpoint_to_server_queue

エンドポイントが CA Access Control エンタープライズ管理 への情報の送信に使用するメッセージ キューの名前を定義します。

デフォルト: ac_endpoint_to_server

server_to_endpoint_broadcast_queue

CA Access Control エンタープライズ管理 がすべてのエンドポイントへメッセージをブロードキャストするために使用するメッセージ キューの名前を定義します。

デフォルト: ac_server_to_endpoint_broadcast

server_to_endpoint_queue

CA Access Control エンタープライズ管理 がエンドポイントへのメッセージの送信に使用するメッセージ キューの名前を定義します。

デフォルト: ac_server_to_endpoint

ssl_custom

ホスト名の検証機能を使用するかどうかを指定します。

制限: 0 - ホスト名の検証機能を使用しない、1 - ホスト名の検証機能を使用する。

デフォルト: 0

ssl_hostname

SSL のホスト名を定義します。

デフォルト: none

ssl_identity

レポート エージェントの ID を定義します。

制限: 証明書データが含まれているファイルへの完全パス名。

デフォルト: none

ssl_issuer

SSL 接続に対する発行元の証明書を定義します。

制限: 証明書データが含まれているファイルへの完全パス名。

デフォルト: none

ssl_key

レポート エージェントの秘密鍵を定義します。

制限: 証明書データが含まれているファイルへの完全パス名。

デフォルト: none

ssl_noverifyhost

ホスト証明書の検証を有効にするかどうかを指定します。

制限: 0 - ホスト証明書の検証を無効にする、1 - ホスト証明書の検証を有効にする。

デフォルト: 0

ssl_noverifyhostname

ホスト名の検証を有効にするかどうかを指定します。

制限: 0 - ホスト名の検証を無効にする、1 - ホスト名の検証を有効にする。

デフォルト: 0

ssl_trace

SSL トレースを有効にするかどうかを指定します。

制限: 0 - SSL トレースを無効にする、1 - SSL トレースを有効にする。

デフォルト: 0

ssl_trusted

SSL 接続に対して信頼されている証明書を定義します。

制限: 証明書データが含まれているファイルへの完全パス名。

デフォルト: none

crypto

CA Access Control は、使用する暗号モジュール設定を以下のキーの下で保守します。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥crypto
```

crypto レジストリ キーには、以下のレジストリ エントリが含まれています。

ca_certificate

認証局(CA)の証明書データベースへの完全パス名を定義します。

デフォルト: *ACInstallDir*¥data¥crypto¥def_root.pem

communication_mode

Secure Socket Layer(SSL)のプロトコルを有効にするかどうかを指定します。

これを ssl_only に設定した場合は、SSL V2、SSL V3、TLS の各接続のみが有効になります。つまり、このコンピュータは、SSL をサポートしていないコンピュータと通信できないため、SSL をサポートしていない、r12.0 より前の各バージョンの Access Control を実行しているコンピュータと通信できません。

注: CA Access Control r12.0 以降が実行されているコンピュータでは、SSL がサポートされています。

fips_only トークンが 1 に設定されている場合は、FIPS モード(つまり TLS)では実際の通信モードは ssl_only に設定され、communication_mode トークンは無視されます。

有効な値は以下のとおりです。

- all_modes
- ssl_only
- non_ssl

デフォルト: non_ssl

encryption_methods

メッセージを復号化するために CA Access Control エージェントが使用する暗号化ライブラリを指定します。復号化が成功するまで、エージェントはリスト内の各ライブラリを順番に使用します。

制限: aes256enc、aes192enc、aes128enc、desenc、tripledesenc、defenc

デフォルト: aes256enc、aes192enc、aes128enc、desenc、tripledesenc

fips_only

このトークンは、CA Access Control が FIPS 専用モードで機能するかどうかを制御します。このモードでは、FIPS 以外のすべての機能が無効になります。

有効な値は以下のとおりです。

1 CA Access Control は FIPS 専用モードで機能します。

0 CA Access Control は FIPS 以外のモードで機能します。

デフォルト: 0

private_key

所有者の秘密鍵への完全パス名を定義します。

デフォルト: *ACInstallDir*¥data¥crypto¥sub.key

ssl_port

CA Access Control のクライアントとサービスの間の SSL 通信のポートを定義します。

デフォルト: 5249

subject_certificate

所有者の証明書への完全パス名を定義します。

デフォルト: *ACInstallDir*¥data¥crypto¥sub.pem

データ

CA Access Control は、使用する内部設定を以下のキーに保持します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Data

データ キー エントリは、内部使用のみです。このキーは開けません。

Dependency

CA Access Control は、使用する依存関係設定を以下のキーの下で保守します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Dependency

CA Access Control のコンポーネント モジュールが、他の製品の埋め込みコンポーネントとしてインストールされているときは、このレジストリ キーのすべてのサブキーが CA Access Control に依存する製品の名前になります。CA Access Control をアップグレードまたはアンインストールする場合、CA Access Control がこのレジストリを確認し、プロセスを続行できるかどうか、または中止する必要があるかどうかを判断します。

devcalc

CA Access Control は、使用するポリシー偏差計算機能設定を以下のキーの下で保守します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥devcalc

devcalc レジストリ キーには、以下のレジストリ エントリが含まれています。

dms_cmd_retry_interval

DMS 通知コマンドの試行間隔を秒数で定義します。

デフォルト: 60

max_dms_cmd_retry

ポリシー偏差計算機能が DMS に更新通知の送信を再試行する最大回数を定義します。この回数を超えても送信されないと、再試行しなくなります。

デフォルト: 3

max_lines_request

get devcalc selang コマンドが任意の時点で(ポリシー偏差データ ファイルから)返す最大行数を定義します。以下のコマンドを使用して、追加行を取得する必要があります。

```
get devcalc params("offset=X")
```

X

前の *get devcalc* 出力で返された行オフセットを定義します。

デフォルト: 50

Exits

CA Access Control は、使用するエージェント終了設定を以下のキーの下で保守します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Exits

Exits レジストリ キーには、レジストリ エントリは含まれていません。含まれているのは、エージェント終了のレジストリ サブキーです。

AuthenticatePassword

CA Access Control は、使用するパスワード認証エージェント終了設定を以下のキーの下で保守します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Exits¥AuthenticatePassword

Exits¥AuthenticatePassword レジストリ キーには、以下のレジストリ エントリが含まれています。

有効

パスワード ルール適用エージェント終了を有効または無効にするための切り替え設定。この値を 0 に設定すると、終了は無効になります。それ以外の値を設定すると、終了は有効になります。

デフォルト: 0

EnforcePasswordControl

CA Access Control クライアントを使用したパスワード ルール適用の条件。

0 - パスワード ルール適用はありません。

1 - 一般ユーザが自分のパスワードを変更したときに、パスワード ルール適用が有効になります。

2 - admin またはパスワード マネージャが、他人または本人のパスワードを変更したときに、パスワード ルール適用が有効になります。

3 - 値 1 および 2 の蓄積。

デフォルト: 1

Engine

CA Access Control は、使用する CA Access Control エンジン（seos）エージェント終了設定を以下のキーの下で保守します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Exits¥Engine

Exits¥Engine レジストリ キーには、デフォルトでレジストリ エントリが含まれていません。

Remote Grace Info

CA Access Control は、使用するリモート猶予情報エージェント終了設定を以下のキーの下で保守します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Exits¥Remote Grace Info

Exits¥Remote Grace Info レジストリ キーには、以下のレジストリ エントリが含まれています。

DefaultWarningDays

segrace¥SegraceW ユーティリティのユーザに対して、パスワード失効警告が表示されるデフォルトの日数を定義します。つまり、これらのユーティリティのいずれかが適用されたが、このレジストリ値で指定した日数よりも少ない日数でユーザのパスワードが失効する場合、そのユーザに警告メッセージが表示されます。

デフォルト: 7

Remote Shutdown

CA Access Control は、使用するリモート シャットダウン エージェント終了設定を以下のキーの下で保守します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Exits¥Remote Shutdown

Exits¥Remote Shutdown レジストリ キーには、以下のレジストリ エントリが含まれています。

パス

リモート シャットダウン DLL の完全パス名。

デフォルト *ACInstallDir*¥bin¥remshut.dll

Prefix

リモート シャットダウン DLL によって使用される定義済みプレフィクス。

デフォルト: SD

FsiDrv

CA Access Control は、使用するドライバ設定を以下のキーの下で保守します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥FsiDrv

FsiDrv レジストリ キーには、以下のレジストリ エントリが含まれています。

AuditRefreshPeriod

同じソースの連続する 2 つの監査イベントの間の最小時間(秒単位)を定義します。CA Access Control では、この期間内に発生する同じソースの連続イベントの監査メッセージをログに記録しません。

デフォルト: 0(すべての監査イベントがログに記録されます)

BatchOplockStatus

ファイル全体のバッチ Oplocks（オポチュニスティック ロック）を無効にするかどうかを指定します。無効（値を 0）にすると、ドライバはファイル アクセスに関する監査情報を 100% 収集しますが、パフォーマンスは低下します。0 以外の値を指定すると、バッチ OpLocks は定期的に動作しますが（有効）、関連ファイルにアクセスしない場合があり、不完全な監査情報を提供する可能性があります。

注: 新しい設定を使用するには、ドライバを再ロードする必要があります。CA Access Control を停止（secons -s）した後に、ドライバをアンロード（net stop seosdrv）します。

デフォルト: 1（有効）

CacheLimit

seosdrv カーネル メモリ キャッシュの制限サイズを MB 単位で定義します。

タイプ: REG_DWORD

制限: 8 ～ 64

デフォルト: 16

directory

ドライバの場所。

デフォルト: *system_drive*¥*Windows_path*¥system32¥drivers

DynamicSysThreadDetection

Trend Micro™ PC-cillin Antivirus など、システム スレッドを作成する別の製品によって作成されたすべてのカーネル スレッドを CA Access Control でトレースするように指定します。

注: このレジストリ値を有効にすると、パフォーマンスの問題を引き起こすことがあります。このレジストリ値を有効にする前に、まず、CA Technologies に問い合わせることをお勧めします。 詳細については、当社テクニカル サポート（http://www.ca.com/jp/support/）にお問い合わせください。

タイプ: REG_DWORD

デフォルト: 0（無効）

FileCacheDisabled

汎用のファイル キャッシュを有効または無効にするための切り替え設定。

値: 0 — 汎用ファイル キャッシュを有効にします。1 — 汎用ファイル キャッシュを無効にします

デフォルト: 0

LoopHoleProtectionDisabled

ループホール防止を無効にするかどうかを指定します。ループホール防止とは、Process Monitor(procmon.exe)のようにハンドルを閉じる可能性のあるアプリケーションから CA Access Control を保護するものです。

値: 0 - ループホール防止を有効にします。**1** - ループホール防止を無効にします。

デフォルト: 0

注: このキーは、32 ビットの Windows 環境に適用されます。

MaxAuditRecordLimit

監査キューの制限を定義します。キューの長さがこの制限を超えると、CA Access Control は意図的に監査イベントを生成するスレッドのスピードを減速して、追加項目がキューに追加されるよりも早く、キューを読み取り、ログファイルに書き込めるようにします。

注: CA Access Control が新規項目を読み取って処理するよりも新規項目がキューに追加される方が速い場合、システムのメモリが枯渇する可能性があります。

デフォルト: 200

MaxTimeoutLimit

連続するタイムアウトの数を定義します。CA Access Control がこの数を検出すると、ドライバのバイパスを起動します。この制限に達すると、ドライバは、認証エンジンがイベント処理をできるようになるまで、認証エンジンに認証要求を送信するのを停止します。

この値を 0 に設定すると、このバイパスは無効になります。

デフォルト: 5

NetworkDispatchLevelAccess

インターセプトされたネットワーク イベント中に、IRQL でのディスパッチ時に、ドライバの応答を定義します

値: 0 と 1

デフォルト:

QueueTimeoutatch

seosd の応答を待つ最長時間(秒単位)。

デフォルト: 10

QueueTimeoutAnswer

タイムアウト後のドライバの応答。

デフォルト: 0(拒否)

RegistryCacheDisabled

汎用のレジストリ キャッシュを有効または無効にするための切り替え設定。

値: 0 — 汎用レジストリ キャッシュを有効にします。1 — 汎用レジストリ キャッシュを無効にします

デフォルト: 0

SilentModeAdmins

メンテナンス モード(SilentModeEnabled = 1)でコンピュータを管理できるユーザ名の行区切りのリスト。

デフォルト値なし

SilentModeEnabled

メンテナンス モードがアクティブ(1)かどうかを指定します。

デフォルト: 0(無効)

SystemBypassRestricted

CA Access Control がシステム プロセスのアクセス チェックをバイパスするかどうかを指定します。デフォルトでは、CA Access Control はシステム プロセスを信頼できると見なさず、システム プロセスのアクセス チェックをバイパスしません。

値: **0** - アクセス チェックをバイパスします。**1** - アクセス チェックをバイパスしません。

デフォルト: 1

Instrumentation

CA Access Control は、使用する（ロードされるすべてのプラグインに適用される）cainstrm.dll の動作設定を以下のキーの下で保守します。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Instrumentation
```

Instrumentation レジストリ キーには、以下のレジストリ エントリが含まれています。

アクティブ

cainstrm.dll がアクティブ（1）かどうかを指定します。

0 を指定した場合、cainstrm.dll はプラグインをロードしますが、処理は行いません。

タイプ： REG_DWORD

デフォルト： 1

ApplyOnProcess

計測が適用されるプロセスのリストを定義します。

サービス名または完全パス名を定義できます。名前は大文字と小文字を区別*しません*。たとえば、「services.exe」、「¥system32¥services.exe」、「c:¥windows¥system32¥services.exe」のように定義します。

タイプ： REG_MULTI_SZ

デフォルトでは、このトークンは設定されていません（計測はどのプロセスにも計測適用されます）。

ExcludeProcess

計測が適用*されない*プロセスのリストを定義します。

注：このエントリは、ApplyOnProcess が設定されていない場合にのみ有効です。

タイプ： REG_MULTI_SZ

デフォルトでは、このトークンは設定されていません。

OperationMode

cainstrm.dll がメモリにプラグインをロードする（1）かどうかを指定します。

タイプ： REG_DWORD

デフォルト： 1

RunTimeInstrumentationDisabled

ランタイムで CA Access Control 計測ポリシーを指定します。

タイプ: REG_DWORD

制限: 0 - ランタイム計測を有効にします。1 - ランタイム計測を無効にします。

デフォルト: 0

RunTimeInstrumentationIncludeList

ランタイム計測を適用するプロセスのリストを定義します。

タイプ: REG_MULTI_SZ

デフォルト: 空白

TraceDbgEnable

cainstrm モジュールのステータス フラグをトレースするかどうか、つまり、DbgView または Kernel Debugger へのトレースを有効にするかどうかを指定します。

タイプ: RED_DWORD

制限: 0 - false。1 - true

デフォルト: 0

TraceFileIsCyclic

トレース ファイルのタイプを指定します。

タイプ: REG_DWORD

制限: 0 - トレース ファイルは循環しません。1 - トレース ファイルは循環します。

デフォルト: 0

TraceFileSizeLimit

トレース ファイルの最大サイズをバイト単位で定義します。この値が 0 の場合、トレース ファイルに対して最大サイズの制限が適用されません。

タイプ: REG_DWORD

デフォルト: 0

TraceFilteringMask

各プラグインのフィルタリング マスクを定義します。このレジストリ値の有効値は、対象となるソフトウェア コンポーネントのステータスによって異なります。定義済みの値は次の 2 つです。0 - すべての情報がフィルタされます（情報は何も表示されません）。0x0fffffff - どの情報もフィルタされません（すべての情報が表示されます）。

タイプ: REG_DWORD

デフォルト: 0

注: ユーザ自身がこのレジストリ エントリの値を変更しすることはお勧めできません。 詳細については、当社テクニカル サポート（http://www.ca.com/jp/support/）にお問い合わせください。

TraceFolderPath

トレース ファイルへの完全パス名を定義します。

タイプ: REG_SZ

デフォルト: 空白

TraceOutputMask

トレース出力チャネル（デバッグ ストリーム、ファイル、または ETW）のフィルタリング マスクを指定します。トレースの出力先として、ファイル、DbgView デバッグ チャネル、または WinDbg デバッグ チャネルを指定できます。この値が 0 の場合、出力は無効になります。

タイプ: REG_DWORD

デフォルト: 0

注: ユーザ自身がこのレジストリ エントリの値を変更しすることはお勧めできません。 詳細については、当社テクニカル サポート（http://www.ca.com/jp/support/）にお問い合わせください。

UnloadIfNoPlugins

現在のプロセスにプラグインが割り当てられているときに、cainstrm.dll が自動的にアンロードされる（1）かどうかを指定します。

0 を指定した場合、cainstrm.dll はプラグインをロードしますが、処理は行いません。

タイプ: REG_DWORD

デフォルト: 1

.NET

CA Access Control は、使用する .NET 設定を以下のキーに保持します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Instrumentation¥.NET

Instrumentation¥.NET レジストリ キーには、レジストリ エントリが含まれていません。このキーには、.NET プロファイラのレジストリ サブキーが含まれています。

プロファイラ

CA Access Control は、使用するプロファイラ設定を以下のキーに保持します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Instrumentation¥.NET¥Profiler

Instrumentation¥.NEt¥Profiler レジストリ キーには、以下のレジストリ エントリが含まれています。

ApplyOnProcess

計測が適用されるプロセスのリストを定義します。

サービス名または完全パス名を定義できます。名前は大文字と小文字を区別*しません*。たとえば、「services.exe」、「¥system32¥services.exe」、「c:¥windows¥system32¥services.exe」のように定義します。

タイプ: REG_MULTI_SZ

デフォルト: w3wp.exe MultiCLRs.exe

CLSID

プロファイラの CLSID を定義します。

タイプ: REG_SZ

デフォルト {753C5090-0ADD-41B9-B074-8B9A7B833D7E}

OperationMode

プロファイラをメモリにロードするかどうかを指定します。

タイプ: REG_DWORD

制限: 0、1

デフォルト: 1

ReadConfigPeriodSec

変更用にレジストリをプールする間隔を指定します。
タイプ: REG_DWORD

デフォルト: 0x600

TraceDbgEnable

cainstrm モジュールのステータス フラグをトレースするかどうか、つまり、DbgView または Kernel Debugger へのトレースを有効にするかどうかを指定します。

タイプ: RED_DWORD

制限: 0 - false。1 - true

デフォルト: 0

TraceFileEnable

ファイルへのトレースを有効にします。

タイプ: REG_DWORD

デフォルト: 0（無効）

TraceFileIsCyclic

トレース ファイルのタイプを指定します。

タイプ: REG_DWORD

制限: 0 - トレース ファイルは循環しません。1 - トレース ファイルは循環します。

デフォルト: 0

TraceFileSizeLimit

トレース ファイルの最大サイズをバイト単位で定義します。この値が 0 の場合、トレース ファイルに対して最大サイズの制限が適用されません。

タイプ: REG_DWORD

デフォルト: 0

TraceFilteringMask

各プラグインのフィルタリング マスクを定義します。このレジストリ値の有効値は、対象となるソフトウェア コンポーネントのステータスによって異なります。定義済みの値は次の 2 つです。0 - すべての情報がフィルタされます（情報は何も表示されません）。0x0fffffff - どの情報もフィルタされません（すべての情報が表示されます）。

タイプ： REG_DWORD

デフォルト： 0

注：ユーザ自身がこのレジストリ エントリの値を変更しすることはお勧めできません。 詳細については、当社テクニカル サポート（http://www.ca.com/jp/support/）にお問い合わせください。

TraceFolderPath

トレース ファイルへの完全パス名を定義します。

タイプ： REG_SZ

デフォルト：空白

TraceOutputMask

トレース出力チャネル（デバッグ ストリーム、ファイル、または ETW）のフィルタリング マスクを指定します。トレースの出力先として、ファイル、DbgView デバッグ チャネル、または WinDbg デバッグ チャネルを指定できます。この値が 0 の場合、出力は無効になります。

タイプ： REG_DWORD

デフォルト： 0

注：ユーザ自身がこのレジストリ エントリの値を変更しすることはお勧めできません。 詳細については、当社テクニカル サポート（http://www.ca.com/jp/support/）にお問い合わせください。

TraceReadParamsSec

トレース パラメータを更新する時間間隔を定義します。WinServicePlg.dll は、TraceReadParamsSec ごとにトレース パラメータの更新を読み込みます。

タイプ： REG_DWORD

アセンブリ

CA Access Control は、使用する .NET プロファイラ アセンブリ設定を以下のキーに保持します。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Instrumentation¥.NET
¥Profiler¥Assemblies
```

.NET¥Profiler¥Assemblies レジストリ キーには、レジストリ エントリが含まれていません。このキーには、.NET プロファイラ アセンブリのレジストリ サブキーが含まれています。

CAPUPM.NETDBPlg

CA Access Control は、使用する CAPUPM.NETBDPlg 設定を以下のキーに保持します。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Instrumentation¥.NET
¥Profiler¥Assemblies¥CAPUPM.NETDBPlg
```

Instrumentation¥.NEt¥Profiler¥Assemblies¥CAPUPM.NETDBPlg レジストリ キーには、以下のレジストリ エントリが含まれています。

BuildNumber

.NET アセンブリのビルド バージョンを定義します。

タイプ: REG_DWORD

デフォルト: 0

MajorVersion

.NET アセンブリのメジャー バージョン番号を定義します。

タイプ: REG_DWORD

デフォルト: 1

MinorVersion

.NET アセンブリのマイナー バージョン番号を定義します。

タイプ: REG_DWORD

デフォルト: 0

PublicKeyToken

.NET アセンブリ公開鍵トークンを定義します。

タイプ: REG_BINARY

デフォルト: 5e 84 2e 72 e9 8c 10 e0

RevisionNumber

.NET アセンブリのレビジョン番号を定義します。

タイプ: REG_DWORD
デフォルト: 0

Plugins

CA Access Control は、使用する .NET プロファイラ プラグイン設定を以下のキーに保持します。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Instrumentation¥.NET¥Profiler¥Plugins
```

Instrumentation¥.NET¥Profiler¥Plugins レジストリ キーには、レジストリ エントリは含まれていません。このキーには、.NET プロファイラ プラグインのレジストリ サブキーが含まれています。

DB

CA Access Control は、使用する DB 設定を以下のキーに保持します。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Instrumentation¥.NET¥Profiler¥Plugins¥DB
```

Instrumentation¥.NET¥Profiler¥Plugins¥DB レジストリ キーには、以下のレジストリ エントリが含まれています。

Altitude

プラグインのロード順序を定義します。
タイプ: REG_DWORD

デフォルト: 1

ApplyOnProcess

計測が適用されるプロセスのリストを定義します。

サービス名または完全パス名を定義できます。名前は大文字と小文字を区別*しません*。たとえば、「services.exe」、「¥system32¥services.exe」、「c:¥windows¥system32¥services.exe」のように定義します。

タイプ: REG_MULTI_SZ

デフォルト: w3wp.exe MultiCLRs.exe

AutoBlockNativeAssemblies

CAPUPMProfilerDBPlg.dll のロードを阻止し、バイト コード バックアップをロードするかどうかを定義します。

タイプ: REG_DWORD

デフォルト: 1

OperationMode

CAPUPMProfilerDBPlg.dll プラグインをメモリにロードするかどうかを指定します。

タイプ: REG_DWORD

制限: 0、1

デフォルト: 1

PluginPath

CAPUPMProfilerDBPlg.dll プラグインのパス名を指定します。

タイプ: REG_SZ

デフォルト: C:¥Program Files¥CA¥AccessControl¥bin¥CAPUPMProfilerDBPlg.dll

TraceDbgEnable

cainstrm モジュールのステータス フラグをトレースするかどうか、つまり、DbgView または Kernel Debugger へのトレースを有効にするかどうかを指定します。

タイプ: RED_DWORD

制限: 0 - false。1 - true

デフォルト: 0

TraceFileEnable

ファイルへのトレースを有効にします。

タイプ: REG_DWORD

デフォルト: 0（無効）

TraceFileIsCyclic

トレース ファイルのタイプを指定します。

タイプ: REG_DWORD

制限: 0 - トレース ファイルは循環しません。1 - トレース ファイルは循環します。

デフォルト: 0

TraceFileSizeLimit

トレース ファイルの最大サイズをバイト単位で定義します。この値が 0 の場合、トレース ファイルに対して最大サイズの制限が適用されません。

タイプ: REG_DWORD

デフォルト: 0

TraceFilteringMask

各プラグインのフィルタリング マスクを定義します。このレジストリ値の有効値は、対象となるソフトウェア コンポーネントのステータスによって異なります。定義済みの値は次の 2 つです。0 - すべての情報がフィルタされます(情報は何も表示されません)。0x0fffffff - どの情報もフィルタされません(すべての情報が表示されます)。

タイプ: REG_DWORD

デフォルト: 0

注: ユーザ自身がこのレジストリ エントリの値を変更しすることはお勧めできません。 詳細については、当社テクニカル サポート (http://www.ca.com/jp/support/) にお問い合わせください。

TraceFolderPath

トレース ファイルへの完全パス名を定義します。

タイプ: REG_SZ

デフォルト: 空白

TraceOutputMask

トレース出力チャネル（デバッグ ストリーム、ファイル、または ETW）のフィルタリング マスクを指定します。トレースの出力先として、ファイル、DbgView デバッグ チャネル、または WinDbg デバッグ チャネルを指定できます。この値が 0 の場合、出力は無効になります。

タイプ: REG_DWORD

デフォルト: 0

注: ユーザ自身がこのレジストリ エントリの値を変更しすることはお勧めできません。 詳細については、当社テクニカル サポート（http://www.ca.com/jp/support/）にお問い合わせください。

PluginManagement

CA Access Control は、使用するプラグインの動的ロードおよびアンロードの設定を以下のキーの下で保守します。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥
Instrumentation¥PluginManagement
```

Instrumentation¥PluginManagement レジストリ キーには、以下のレジストリ エントリが含まれています。

アクティブ

プラグインの動的ロードがアクティブ（1）かどうかを指定します。

タイプ: REG_DWORD

デフォルト: 1

Altitude

チェーン内の動的管理スタブの順序を定義します。

タイプ: REG-DWORD

デフォルト: 0x0fffffff（予約値）

ApplyOnDLL

読み取り専用の値。

デフォルト: Kernel32.dll

ApplyOnProcess

動的ロードが適用されるプロセスのリストを定義します。

サービス名または完全パス名を定義できます。名前は大文字と小文字を区別*しません*。たとえば、「services.exe」、「¥system32¥services.exe」、「c:¥windows¥system32¥services.exe」のように定義します。

タイプ: REG_MULTI_SZ

デフォルトでは、このトークンは設定されていません(どのプラグインにも動的ロードは適用されません)。

ExcludeProcess

動的ロードが適用*されない*プロセスのリストを定義します。

注: このエントリは、ApplyOnProcess が設定されていない場合にのみ有効です。

タイプ: REG_MULTI_SZ

デフォルトでは、このトークンは設定されていません。

LoadLibraryA

内部的使用のみ。

デフォルト: 0

LoadLibraryExA

内部的使用のみ。

デフォルト: 0

LoadLibraryExW

内部的使用のみ。

デフォルト: 1

LoadLibraryW

内部使用のみ。

デフォルト: 0

OperationMode

内部的使用のみ。

デフォルト: 1

ProcessCommanArguments

インストルメンテーション モジュールがプロセス作成イベント時に CA Access Control セキュリティ サービスに通知するかどうかを指定します。

タイプ: REG_DWORD

値:

0 -- インストルメンテーション モジュールは、プロセス作成時に CA Access Control セキュリティ サービスに通知しません。

1 -- インストルメンテーション モジュールは、プロセス作成時に CA Access Control セキュリティ サービスに通知します。

注: レジストリ キー値は、設定およびデータベース定義に応じて、CA Access Control セキュリティ サービスによって自動的に変更されます。レジストリ キー値を手動で変更しないでください。

PluginName

読み取り専用の値。

デフォルト: *ACInstallDir*¥bin¥cainstrm.dll

PlugIns

CA Access Control は、使用するプラグイン設定を以下のキーの下で保守します。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Instrumentation¥PlugIns
```

Instrumentation¥PlugIns レジストリ キーには、レジストリ エントリが含まれていません。含まれているのは、ロードされたすべてのプラグインのレジストリ サブキーです。

CMDPlg

CA Access Control は、使用する CMD プラグイン設定を以下のキーの下で保守します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Instrumentation¥PlugIns¥CMDPlg

Instrumentation¥PlugIns¥CMDPlg レジストリ キーには、以下のレジストリ エントリが含まれています。

Altitude

プラグインのロード順序を定義します。

制限: 1 ～ 1000（これらの制限を上回る値および下回る値は、内部的使用のために予約されています）

タイプ: REG_DWORD

デフォルト: 5

ApplyOnDLL

現在のプラグインが適用される DLL 名（モジュール）を定義します。

タイプ: REG_SZ

デフォルト: Kernel32.dll

ApplyOnProcess

現在のプラグインが適用されるプロセスを定義します。

サービス名、ファイル名、または完全パス名を定義できます。たとえば、「services.exe」、「¥system32¥services.exe」、「c:¥windows¥system32¥services.exe」のように定義します。

タイプ: REG_MULTI_SZ

注: このレジストリ エントリの値が 1 つのみの場合、REG_SZ も有効なタイプです。

デフォルト: CMD.exe

CommunicationWaitTimeout

プラグインがトランザクションを送受信するときに待機する最大時間を秒単位で定義します。

タイプ: REG_DWORD

デフォルト: 15

ExcludeProcess

プラグインが適用されないプロセスを定義します。

注: このエントリは、ApplyOnProcess が設定されていない場合にのみ有効です。

タイプ: REG_MULTI_SZ

デフォルトでは、このトークンは空白です。

OperationMode

メモリにプラグインをロードする(1)かどうかを指定します。

タイプ: REG_DWORD

デフォルト: 1

PluginName

プラグインのダイナミック リンク ライブラリ(DLL)の名前を定義します。

タイプ: REG_SZ

デフォルト: *ACInstallDir*¥bin¥CMDPlg.dll

ServiceTimeOut

seosd のトランザクションを待つ最大間隔(ミリ秒単位)を定義します。

注: タイムアウトの値を超えると、要求が許可されます。

タイプ: REG_DWORD

デフォルト: 0x00000bb8(10 進数字で 3000)

TraceDbgEnable

cainstrm モジュールのステータス フラグをトレースするかどうか、つまり、DbgView または Kernel Debugger へのトレースを有効にするかどうかを指定します。

タイプ: RED_DWORD

制限: 0 - false。1 - true

デフォルト: 0

TraceFileEnable

ファイルへのトレースを有効にします。

タイプ: REG_DWORD

デフォルト: 0(無効)

TraceFileIsCyclic

トレース ファイルのタイプを指定します。

タイプ: REG_DWORD

制限: 0 - トレース ファイルは循環しません。1 - トレース ファイルは循環します。

デフォルト: 0

TraceFileSizeLimit

トレース ファイルの最大サイズをバイト単位で定義します。この値が 0 の場合、トレース ファイルに対して最大サイズの制限が適用されません。

タイプ: REG_DWORD

デフォルト: 0

TraceFilteringMask

各プラグインのフィルタリング マスクを定義します。このレジストリ値の有効値は、対象となるソフトウェア コンポーネントのステータスによって異なります。定義済みの値は次の 2 つです。0 - すべての情報がフィルタされます(情報は何も表示されません)。0x0fffffff - どの情報もフィルタされません(すべての情報が表示されます)。

タイプ: REG_DWORD

デフォルト: 0

注: ユーザ自身がこのレジストリ エントリの値を変更しすることはお勧めできません。 詳細については、当社テクニカル サポート (http://www.ca.com/jp/support/) にお問い合わせください。

TraceFolderPath

トレース ファイルへの完全パス名を定義します。

タイプ: REG_SZ

デフォルト: 空白

TraceOutputMask

トレース出力チャネル(デバッグ ストリーム、ファイル、または ETW)のフィルタリング マスクを指定します。トレースの出力先として、ファイル、DbgView デバッグ チャネル、または WinDbg デバッグ チャネルを指定できます。この値が 0 の場合、出力は無効になります。

タイプ: REG_DWORD

デフォルト: 0

注: ユーザ自身がこのレジストリ エントリの値を変更しすることはお勧めできません。 詳細については、当社テクニカル サポート (http://www.ca.com/jp/support/) にお問い合わせください。

TraceReadParamsSec

トレース パラメータを更新する時間間隔を定義します。WinServicePlg.dll は、TraceReadParamsSec ごとにトレース パラメータの更新を読み込みます。

タイプ: REG_DWORD

デフォルト: 60

OCIPlg

CA Access Control は、使用する OCI プラグイン設定を以下のキーの下で保守します。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Instrumentation¥PlugIns¥OCIPlg
```

Instrumentation¥PlugIns¥OCIPlg レジストリ キーには、以下のレジストリ エントリが含まれています。

Altitude

プラグインのロード順序を定義します。

制限: 1 ～ 1000(これらの制限を上回る値および下回る値は、内部的使用のために予約されています)

タイプ: REG_DWORD

デフォルト: 5

ApplyOnDLL

現在のプラグインが適用される DLL 名（モジュール）を定義します。

タイプ： REG_SZ

デフォルト： oci.dll

ApplyOnProcess

現在のプラグインが適用されるプロセスを定義します。

サービス名、ファイル名、または完全パス名を定義できます。たとえば、「services.exe」、「¥system32¥services.exe」、「c:¥windows¥system32¥services.exe」のように定義します。

タイプ： REG_MULTI_SZ

注： このレジストリ エントリの値が 1 つのみの場合、REG_SZ も有効なタイプです。

デフォルト： sqlplus.exe w3wp.exe

CommunicationWaitTimeout

プラグインがトランザクションを送受信するときに待機する最大時間を秒単位で定義します。

タイプ： REG_DWORD

デフォルト： 15

EnvironmentVariables

特権ユーザ パスワード管理 エージェントへ転送される環境変数を指定します。

タイプ： REG_MULTI_SZ

デフォルト： TNS_ADMIN ORACLE_HOME

注： ユーザ自身がこのレジストリ エントリの値を変更しすることはお勧めできません。 詳細については、当社テクニカル サポート（http://www.ca.com/jp/support/）にお問い合わせください。

ExcludeProcess

プラグインが適用されないプロセスを定義します。

注： このエントリは、ApplyOnProcess が設定されていない場合にのみ有効です。

タイプ： REG_MULTI_SZ

デフォルトでは、このトークンは空白です。

OperationMode

メモリにプラグインをロードする(1)かどうかを指定します。

タイプ: REG_DWORD

デフォルト: 0

PluginName

プラグインのダイナミック リンク ライブラリ(DLL)の名前を定義します。

タイプ: REG_SZ

デフォルト: *ACInstallDir*¥bin¥OCIPlg.dll

TraceDbgEnable

cainstrm モジュールのステータス フラグをトレースするかどうか、つまり、DbgView または Kernel Debugger へのトレースを有効にするかどうかを指定します。

タイプ: RED_DWORD

制限: 0 - false。1 - true

デフォルト: 0

TraceFileEnable

ファイルへのトレースを有効にします。

タイプ: REG_DWORD

デフォルト: 0(無効)

TraceFileIsCyclic

トレース ファイルのタイプを指定します。

タイプ: REG_DWORD

制限: 0 - トレース ファイルは循環しません。1 - トレース ファイルは循環します。

デフォルト: 0

TraceFileSizeLimit

トレース ファイルの最大サイズをバイト単位で定義します。この値が 0 の場合、トレース ファイルに対して最大サイズの制限が適用されません。

タイプ: REG_DWORD

デフォルト: 0

TraceFilteringMask

各プラグインのフィルタリング マスクを定義します。このレジストリ値の有効値は、対象となるソフトウェア コンポーネントのステータスによって異なります。定義済みの値は次の 2 つです。0 - すべての情報がフィルタされます（情報は何も表示されません）。0x0fffffff - どの情報もフィルタされません（すべての情報が表示されます）。

タイプ: REG_DWORD

デフォルト: 0

注: ユーザ自身がこのレジストリ エントリの値を変更しすることはお勧めできません。 詳細については、当社テクニカル サポート（http://www.ca.com/jp/support/）にお問い合わせください。

TraceFolderPath

トレース ファイルへの完全パス名を定義します。

タイプ: REG_SZ

デフォルト: 空白

TraceOutputMask

トレース出力チャネル（デバッグ ストリーム、ファイル、または ETW）のフィルタリング マスクを指定します。トレースの出力先として、ファイル、DbgView デバッグ チャネル、または WinDbg デバッグ チャネルを指定できます。この値が 0 の場合、出力は無効になります。

タイプ: REG_DWORD

デフォルト: 0

注: ユーザ自身がこのレジストリ エントリの値を変更しすることはお勧めできません。 詳細については、当社テクニカル サポート（http://www.ca.com/jp/support/）にお問い合わせください。

TraceReadParamsSec

トレース パラメータを更新する時間間隔を定義します。WinServicePlg.dll は、TraceReadParamsSec ごとにトレース パラメータの更新を読み込みます。

タイプ: REG_DWORD

デフォルト: 60

UpgradeWaitTimeOutMaxTries

プラグインを更新する再試行の試行の数を指定します。

タイプ: REG_DWORD

デフォルト: 3

注: ユーザ自身がこのレジストリ エントリの値を変更しすることはお勧めできません。 詳細については、当社テクニカル サポート（http://www.ca.com/jp/support/）にお問い合わせください。

UpgradeWaitTimeOutMilliseconds

アップグレードの失敗を宣言するまでのタイムアウト期間をミリ秒単位で指定します。

タイプ: REG_DWORD

デフォルト: 0x1ffff（131071）

注: ユーザ自身がこのレジストリ エントリの値を変更しすることはお勧めできません。 詳細については、当社テクニカル サポート（http://www.ca.com/jp/support/）にお問い合わせください。

ODBCPlg

CA Access Control は、使用する 特権ユーザ パスワード管理 Agent ODBC プラグイン設定を以下のキーの下で保守します。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Instrumentation¥PlugIns¥ODBCPlg
```

Instrumentation¥PlugIns¥ODBCPlg レジストリ キーには、以下のレジストリ エントリが含まれています。

Altitude

プラグインのロード順序を定義します。

制限: 1 ～ 1000（これらの制限を上回る値および下回る値は、内部的使用のために予約されています）

タイプ: REG_DWORD

デフォルト: 5

ApplyOnDLL

現在のプラグインが適用される DLL 名（モジュール）を定義します。

タイプ: REG_MULTI_SZ

デフォルト: ODBC32.dll

ApplyOnProcess

現在のプラグインが適用されるプロセスを定義します。

サービス名、ファイル名、または完全パス名を定義できます。たとえば、「services.exe」、「¥system32¥services.exe」、「c:¥windows¥system32¥services.exe」のように定義します。

タイプ: REG_MULTI_SZ

注: このレジストリ エントリの値が 1 つのみの場合、REG_SZ も有効なタイプです。

デフォルト: w3wp.exe

CommunicationWaitTimeout

プラグインがトランザクションを送受信するときに待機する最大時間を秒単位で定義します。

タイプ: REG_DWORD

デフォルト: 15

EnvironmentVariables

特権ユーザ パスワード管理 エージェントへ転送される環境変数を指定します。

タイプ: REG_MULTI_SZ

デフォルト: TNS_ADMIN ORACLE_HOME

注: ユーザ自身がこのレジストリ エントリの値を変更しすることはお勧めできません。 詳細については、当社テクニカル サポート（http://www.ca.com/jp/support/）にお問い合わせください。

ExcludeProcess

プラグインが適用されないプロセスを定義します。

注: このエントリは、ApplyOnProcess が設定されていない場合にのみ有効です。

タイプ: REG_MULTI_SZ

デフォルトでは、このトークンは空白です。

OperationMode

メモリにプラグインをロードする(1)かどうかを指定します。

タイプ: REG_DWORD

デフォルト: 0

PluginName

プラグインのダイナミック リンク ライブラリ(DLL)の名前を定義します。

タイプ: REG_SZ

デフォルト: *ACInstallDir*¥bin¥ODBCPlg.dll

TraceDbgEnable

cainstrm モジュールのステータス フラグをトレースするかどうか、つまり、DbgView または Kernel Debugger へのトレースを有効にするかどうかを指定します。

タイプ: RED_DWORD

制限: 0 - false。1 - true

デフォルト: 0

TraceFileEnable

ファイルへのトレースを有効にします。

タイプ: REG_DWORD

デフォルト: 0(無効)

TraceFileIsCyclic

トレース ファイルのタイプを指定します。

タイプ: REG_DWORD

制限: 0 - トレース ファイルは循環しません。1 - トレース ファイルは循環します。

デフォルト: 0

TraceFileSizeLimit

トレース ファイルの最大サイズをバイト単位で定義します。この値が 0 の場合、トレース ファイルに対して最大サイズの制限が適用されません。

タイプ: REG_DWORD

デフォルト: 0

TraceFilteringMask

各プラグインのフィルタリング マスクを定義します。このレジストリ値の有効値は、対象となるソフトウェア コンポーネントのステータスによって異なります。定義済みの値は次の 2 つです。0 - すべての情報がフィルタされます（情報は何も表示されません）。0x0fffffff - どの情報もフィルタされません（すべての情報が表示されます）。

タイプ: REG_DWORD

デフォルト: 0

注: ユーザ自身がこのレジストリ エントリの値を変更しすることはお勧めできません。 詳細については、当社テクニカル サポート（http://www.ca.com/jp/support/）にお問い合わせください。

TraceFolderPath

トレース ファイルへの完全パス名を定義します。

タイプ: REG_SZ

デフォルト: 空白

TraceOutputMask

トレース出力チャネル（デバッグ ストリーム、ファイル、または ETW）のフィルタリング マスクを指定します。トレースの出力先として、ファイル、DbgView デバッグ チャネル、または WinDbg デバッグ チャネルを指定できます。この値が 0 の場合、出力は無効になります。

タイプ: REG_DWORD

デフォルト: 0

注: ユーザ自身がこのレジストリ エントリの値を変更しすることはお勧めできません。 詳細については、当社テクニカル サポート（http://www.ca.com/jp/support/）にお問い合わせください。

TraceReadParamsSec

トレース パラメータを更新する時間間隔を定義します。WinServicePlg.dll は、TraceReadParamsSec ごとにトレース パラメータの更新を読み込みます。

タイプ: REG_DWORD

デフォルト: 60

UpgradeWaitTimeOutMaxTries

プラグインを更新する再試行の試行の数を指定します。

タイプ: REG_DWORD

デフォルト: 3

注: ユーザ自身がこのレジストリ エントリの値を変更しすることはお勧めできません。 詳細については、当社テクニカル サポート（http://www.ca.com/jp/support/）にお問い合わせください。

UpgradeWaitTimeOutMilliseconds

アップグレードの失敗を宣言するまでのタイムアウト期間をミリ秒単位で指定します。

タイプ: REG_DWORD

デフォルト: 0x1ffff（131071）

注: ユーザ自身がこのレジストリ エントリの値を変更しすることはお勧めできません。 詳細については、当社テクニカル サポート（http://www.ca.com/jp/support/）にお問い合わせください。

OLEDBPlg

CA Access Control は、使用する 特権ユーザ パスワード管理 Agent OLEDB プラグイン設定を以下のキーの下で保守します。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Instrumentation¥PlugIns¥OLEDBlg
```

Instrumentation¥PlugIns¥OLEDBPlg レジストリ キーには、以下のレジストリ エントリが含まれています。

Altitude

プラグインのロード順序を定義します。

制限: 1 ～ 1000（これらの制限を上回る値および下回る値は、内部的使用のために予約されています）

タイプ: REG_DWORD

デフォルト: 5

ApplyOnDLL

現在のプラグインが適用される DLL 名（モジュール）を定義します。

タイプ: REG_MULTI_SZ

デフォルト: kernel32.dll

ApplyOnProcess

現在のプラグインが適用されるプロセスを定義します。

サービス名、ファイル名、または完全パス名を定義できます。たとえば、「services.exe」、「¥system32¥services.exe」、「c:¥windows¥system32¥services.exe」のように定義します。

タイプ: REG_MULTI_SZ

注: このレジストリ エントリの値が 1 つのみの場合、REG_SZ も有効なタイプです。

デフォルト: w3wp.exe sqlcmd.exe

CommunicationWaitTimeout

プラグインがトランザクションを送受信するときに待機する最大時間を秒単位で定義します。

タイプ: REG_DWORD

デフォルト: 15

EnvironmentVariables

特権ユーザ パスワード管理 エージェントへ転送される環境変数を指定します。

タイプ: REG_MULTI_SZ

デフォルト: TNS_ADMIN ORACLE_HOME

注: ユーザ自身がこのレジストリ エントリの値を変更しすることはお勧めできません。 詳細については、当社テクニカル サポート（http://www.ca.com/jp/support/）にお問い合わせください。

ExcludeProcess

プラグインが適用されないプロセスを定義します。

注: このエントリは、ApplyOnProcess が設定されていない場合にのみ有効です。

タイプ: REG_MULTI_SZ

デフォルトでは、このトークンは空白です。

OperationMode

メモリにプラグインをロードする(1)かどうかを指定します。

タイプ: REG_DWORD

デフォルト: 0

PluginName

プラグインのダイナミック リンク ライブラリ(DLL)の名前を定義します。

タイプ: REG_SZ

デフォルト: *ACInstallDir*¥bin¥OLEDBPlg.dll

SerializationWaitTimeout

loadlibrary と DllGetClassObject クラスの内部同期を定義します。

タイプ: REG_DWORD

デフォルト: 0xa(10 進数字で 10)

注: ユーザ自身がこのレジストリ エントリの値を変更しすることはお勧めできません。 詳細については、当社テクニカル サポート(http://www.ca.com/jp/support/)にお問い合わせください。

TraceDbgEnable

cainstrm モジュールのステータス フラグをトレースするかどうか、つまり、DbgView または Kernel Debugger へのトレースを有効にするかどうかを指定します。

タイプ: RED_DWORD

制限: 0 - false。1 - true

デフォルト: 0

TraceFileEnable

ファイルへのトレースを有効にします。

タイプ: REG_DWORD

デフォルト: 0(無効)

TraceFileIsCyclic

トレース ファイルのタイプを指定します。

タイプ: REG_DWORD

制限: 0 - トレース ファイルは循環しません。1 - トレース ファイルは循環します。

デフォルト: 0

TraceFileSizeLimit

トレース ファイルの最大サイズをバイト単位で定義します。この値が 0 の場合、トレース ファイルに対して最大サイズの制限が適用されません。

タイプ: REG_DWORD

デフォルト: 0

TraceFilteringMask

各プラグインのフィルタリング マスクを定義します。このレジストリ値の有効値は、対象となるソフトウェア コンポーネントのステータスによって異なります。定義済みの値は次の 2 つです。0 - すべての情報がフィルタされます(情報は何も表示されません)。0x0fffffff - どの情報もフィルタされません(すべての情報が表示されます)。

タイプ: REG_DWORD

デフォルト: 0

注: ユーザ自身がこのレジストリ エントリの値を変更しすることはお勧めできません。 詳細については、当社テクニカル サポート (http://www.ca.com/jp/support/) にお問い合わせください。

TraceFolderPath

トレース ファイルへの完全パス名を定義します。

タイプ: REG_SZ

デフォルト: 空白

TraceOutputMask

トレース出力チャネル（デバッグ ストリーム、ファイル、または ETW）のフィルタリング マスクを指定します。トレースの出力先として、ファイル、DbgView デバッグ チャネル、または WinDbg デバッグ チャネルを指定できます。この値が 0 の場合、出力は無効になります。

タイプ: REG_DWORD

デフォルト: 0

注: ユーザ自身がこのレジストリ エントリの値を変更しすることはお勧めできません。 詳細については、当社テクニカル サポート（http://www.ca.com/jp/support/）にお問い合わせください。

TraceReadParamsSec

トレース パラメータを更新する時間間隔を定義します。WinServicePlg.dll は、TraceReadParamsSec ごとにトレース パラメータの更新を読み込みます。

タイプ: REG_DWORD

デフォルト: 60

UpgradeWaitTimeOutMaxTries

プラグインを更新する再試行の試行の数を指定します。

タイプ: REG_DWORD

デフォルト: 3

注: ユーザ自身がこのレジストリ エントリの値を変更しすることはお勧めできません。 詳細については、当社テクニカル サポート（http://www.ca.com/jp/support/）にお問い合わせください。

UpgradeWaitTimeOutMilliseconds

アップグレードの失敗を宣言するまでのタイムアウト期間をミリ秒単位で指定します。

タイプ: REG_DWORD

デフォルト: 0x1ffff（131071）

注: ユーザ自身がこのレジストリ エントリの値を変更しすることはお勧めできません。 詳細については、当社テクニカル サポート（http://www.ca.com/jp/support/）にお問い合わせください。

プロバイダ

CA Access Control は OLEDB プラグインがサポートするプロバイダの設定を以下のキーに保持します。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Instrumentation¥PlugIns¥
OLEDBPlg¥Providers
```

Instrumentation¥PlugIns¥OLEDBPlg¥Providers レジストリ キーには、レジストリ エントリは含まれていません。このキーには、OLEDB プラグインがサポートするすべてのプロバイダのためのレジストリ サブキーが含まれています。

注: OLEDB プラグインがサポートするいくつかのプロバイダは CA Access Control でサポートされていません。

汎用

CA Access Control は OLEDB プラグインがサポートする汎用プロバイダの設定を以下のキーに保持します。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Instrumentation¥PlugIns¥
OLEDBPlg¥Providers¥Generic
```

Instrumentation¥PlugIns¥OLEDBPlg¥Providers¥Generic レジストリ キーには、レジストリ エントリは含まれていません。このキーには、OLEDB プラグインがサポートする汎用プロバイダのためのレジストリ サブキーが含まれています。

CLSID

CA Access Control は OLEDB プラグインがサポートする汎用プロバイダの CLSID (クラス識別子) 設定を以下のキーに保持します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Instrumentation¥PlugIns¥
OLEDBPlg¥Providers¥Generic¥CLSID

デフォルトでは、Instrumentation¥PlugIns¥OLEDBPlg¥Providers¥Generic¥CLSID レジストリ キーには、レジストリ エントリは含まれていません。このサブキー内に作成するエントリは以下の形式である必要があります。

CLSID

プロバイダのクラス識別子を定義します。

タイプ: REG_SZ

制限: 「1」はプロバイダのサポートを有効にします。「0」はプロバイダのサポートを無効にします。

Name

CA Access Control は OLEDB プラグインがサポートする汎用プロバイダの設定を以下のキーに保持します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Instrumentation¥PlugIns¥
OLEDBPlg¥Providers¥Generic¥Name

Instrumentation¥PlugIns¥OLEDBPlg¥Providers¥Generic¥Name レジストリ キーには、以下のレジストリ エントリが含まれています。

Microsoft OLE DB Provider for ODBC Drivers

OLEDB プラグインが Microsoft OLE DB Provider for ODBC Drivers をサポートすることを指定します。

タイプ: REG_DWORD

制限: 「1」はサポートを有効にします。「0」はサポートを無効にします。

デフォルト: 1

Jet

CA Access Control は OLEDB プラグインがサポートする Microsoft Jet ベースのプロバイダの設定を以下のキーに保持します。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Instrumentation¥PlugIns¥
OLEDBPlg¥Providers¥Jet
```

Instrumentation¥PlugIns¥OLEDBPlg¥Providers¥Jet レジストリ キーには、レジストリ エントリは含まれていません。このキーには、OLEDB プラグインがサポートする Microsoft Jet ベースのプロバイダのためのレジストリ サブキーが含まれています。

注: CA Access Control は現在 Microsoft Jet ベースのプロバイダをサポートしません。

CLSID

CA Access Control は OLEDB プラグインがサポートする Microsoft Jet ベースのプロバイダの CLSID(クラス識別子)設定を以下のキーに保持します。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Instrumentation¥PlugIns¥
OLEDBPlg¥Providers¥Jet¥CLSID
```

注: CA Access Control は現在 Microsoft Jet ベースのプロバイダをサポートしません。

デフォルトでは、Instrumentation¥PlugIns¥OLEDBPlg¥Providers¥Jet¥CLSID レジストリ キーには、レジストリ エントリは含まれていません。このサブキー内に作成するエントリは以下の形式である必要があります。

CLSID

プロバイダのクラス識別子を定義します。

タイプ: REG_SZ

制限: 「1」はプロバイダのサポートを有効にします。「0」はプロバイダのサポートを無効にします。

Name

CA Access Control は OLEDB プラグインがサポートする Microsoft Jet ベースのプロバイダの設定を以下のキーに保持します。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Instrumentation¥PlugIns¥
OLEDBPlg¥Providers¥Jet¥Name
```

注: CA Access Control は現在 Microsoft Jet ベースのプロバイダをサポートしません。

Instrumentation¥PlugIns¥OLEDBPlg¥Providers¥Jet¥Name レジストリ キーには、以下のレジストリ エントリが含まれています。

Microsoft Jet 4.0 OLE DB Provider

OLEDB プラグインが Microsoft Jet 4.0 OLE DB Provider をサポートすることを指定します。

タイプ: REG_DWORD

制限: 「1」はサポートを有効にします。「0」はサポートを無効にします。

デフォルト: 1

Microsoft Office 12.0 Access Database Engine OLE DB Provider

OLEDB プラグインが Microsoft Office 12.0 Access Database Engine OLE DB Provider をサポートすることを指定します。

タイプ: REG_DWORD

制限: 「1」はサポートを有効にします。「0」はサポートを無効にします。

デフォルト: 1

MSSQL

CA Access Control は OLEDB プラグインがサポートする Microsoft SQL Server ベースのプロバイダの設定を以下のキーに保持します。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Instrumentation¥PlugIns¥
OLEDBPlg¥Providers¥MSSQL
```

Instrumentation¥PlugIns¥OLEDBPlg¥Providers¥MSSQL レジストリ キーには、レジストリ エントリは含まれていません。このキーには、OLEDB プラグインがサポートする Microsoft SQL Server ベースのプロバイダのためのレジストリ サブキーが含まれています。

CLSID

CA Access Control は OLEDB プラグインがサポートする Microsoft SQL Server ベースのプロバイダの CLSID（クラス識別子）設定を以下のキーに保持します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Instrumentation¥PlugIns¥
OLEDBPlg¥Providers¥MSSQL¥CLSID

デフォルトでは、Instrumentation¥PlugIns¥OLEDBPlg¥Providers¥MSSQL¥CLSID レジストリ キーには、レジストリ エントリは含まれていません。このサブキー内に作成するエントリは以下の形式である必要があります。

CLSID

プロバイダのクラス識別子を定義します。

タイプ： REG_SZ

制限：「1」はプロバイダのサポートを有効にします。「0」はプロバイダのサポートを無効にします。

Name

CA Access Control は OLEDB プラグインがサポートする Microsoft SQL Server ベースのプロバイダの設定を以下のキーに保持します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Instrumentation¥PlugIns¥
OLEDBPlg¥Providers¥MSSQL¥Name

Instrumentation¥PlugIns¥OLEDBPlg¥Providers¥MSSQL¥Name レジストリ キーには、以下のレジストリ エントリが含まれています。

Microsoft OLE DB Provider for SQL Server

OLEDB プラグインが Microsoft OLE DB Provider for SQL Server をサポートすることを指定します。

タイプ： REG_DWORD

制限：「1」はサポートを有効にします。「0」はサポートを無効にします。

デフォルト： 1

SQL Native Client

OLEDB プラグインが SQL Native Client プロバイダをサポートすることを指定します。

タイプ: REG_DWORD

制限: 「1」はサポートを有効にします。「0」はサポートを無効にします。

デフォルト: 1

SQL Server Native Client 10.0

OLEDB プラグインが SQL Server Native Client 10.0 プロバイダをサポートすることを指定します。

タイプ: REG_DWORD

制限: 「1」はサポートを有効にします。「0」はサポートを無効にします。

デフォルト: 1

MySQL

CA Access Control は OLEDB プラグインがサポートする MySQL ベースのプロバイダの設定を以下のキーに保持します。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Instrumentation¥PlugIns¥
OLEDBPlg¥Providers¥MySQL
```

Instrumentation¥PlugIns¥OLEDBPlg¥Providers¥MySQL レジストリ キーには、レジストリ エントリは含まれていません。このキーには、OLEDB プラグインがサポートする MySQL ベースのプロバイダのためのレジストリ サブキーが含まれています。

注: CA Access Control は現在 MySQL ベースのプロバイダをサポートしません。

CLSID

CA Access Control は OLEDB プラグインがサポートする MySQL ベースのプロバイダの CLSID（クラス識別子）設定を以下のキーに保持します。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Instrumentation¥PlugIns¥
OLEDBPlg¥Providers¥MySQL¥CLSID
```

注: CA Access Control は現在 MySQL ベースのプロバイダをサポートしません。

デフォルトでは、Instrumentation¥PlugIns¥OLEDBPlg¥Providers¥MySQL¥CLSID レジストリ キーには、レジストリ エントリは含まれていません。このサブキー内に作成するエントリは以下の形式である必要があります。

CLSID

プロバイダのクラス識別子を定義します。

タイプ: REG_SZ

制限: 「1」はプロバイダのサポートを有効にします。「0」はプロバイダのサポートを無効にします。

Name

CA Access Control は OLEDB プラグインがサポートする MySQL ベースのプロバイダの設定を以下のキーに保持します。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Instrumentation¥PlugIns¥
OLEDBPlg¥Providers¥MySQL¥Name
```

注: CA Access Control は現在 MySQL ベースのプロバイダをサポートしません。

Instrumentation¥PlugIns¥OLEDBPlg¥Providers¥MySQL¥Name レジストリ キーには、以下のレジストリ エントリが含まれています。

MySQL **プロバイダ**

OLEDB プラグインが MySQL プロバイダをサポートすることを指定します。

タイプ: REG_DWORD

制限: 「1」はサポートを有効にします。「0」はサポートを無効にします。

デフォルト: 1

MySQL.OLEDB Provider

OLEDB プラグインが MySQL.OLEDB Provider をサポートすることを指定します。

タイプ: REG_DWORD

制限: 「1」はサポートを有効にします。「0」はサポートを無効にします。

デフォルト: 1

Oracle

CA Access Control は OLEDB プラグインがサポートする Oracle ベースのプロバイダの設定を以下のキーに保持します。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Instrumentation¥PlugIns¥
OLEDBPlg¥Providers¥Oracle
```

Instrumentation¥PlugIns¥OLEDBPlg¥Providers¥Oracle レジストリ キーには、レジストリ エントリは含まれていません。このキーには、OLEDB プラグインがサポートする Oracle ベースのプロバイダのためのレジストリ サブキーが含まれています。

CLSID

CA Access Control は OLEDB プラグインがサポートする Oracle ベースのプロバイダの CLSID(クラス識別子)設定を以下のキーに保持します。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Instrumentation¥PlugIns¥
OLEDBPlg¥Providers¥Oracle¥CLSID
```

デフォルトでは、Instrumentation¥PlugIns¥OLEDBPlg¥Providers¥Oracle¥CLSID レジストリ キーには、レジストリ エントリは含まれていません。このサブキー内に作成するエントリは以下の形式である必要があります。

CLSID

プロバイダのクラス識別子を定義します。

タイプ: REG_SZ

制限: 「1」はプロバイダのサポートを有効にします。「0」はプロバイダのサポートを無効にします。

Name

CA Access Control は OLEDB プラグインがサポートする Oracle ベースのプロバイダの設定を以下のキーに保持します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Instrumentation¥PlugIns¥
OLEDBPlg¥Providers¥Oracle¥Name

Instrumentation¥PlugIns¥OLEDBPlg¥Providers¥Oracle¥Name レジストリ キーには、以下のレジストリ エントリが含まれています。

Microsoft OLE DB Provider for Oracle

OLEDB プラグインが Microsoft OLE DB Provider for Oracle をサポートすることを指定します。

タイプ: REG_DWORD

制限: 「1」はサポートを有効にします。「0」はサポートを無効にします。

デフォルト: 1

Oracle Provider for OLE DB

DB プラグインが Oracle Provider for OLE DB をサポートすることを指定します。

タイプ: REG_DWORD

制限: 「1」はサポートを有効にします。「0」はサポートを無効にします。

デフォルト: 1

RunAsPlg

CA Access Control は、使用する RunAs プラグイン設定を以下のキーの下で保守します。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Instrumentation¥PlugIns¥RunAsPlg
```

Instrumentation¥PlugIns¥RunAsPlg レジストリ キーには、以下のレジストリ エントリが含まれています。

Altitude

プラグインのロード順序を定義します。

制限: 1 ～ 1000（これらの制限を上回る値および下回る値は、内部的使用のために予約されています）

タイプ: REG_DWORD

デフォルト: 5

ApplyOnDLL

現在のプラグインが適用される DLL 名（モジュール）を定義します。

タイプ: REG_MULTI_SZ

デフォルト: advapi32.dll

ApplyOnProcess

現在のプラグインが適用されるプロセスを定義します。

サービス名、ファイル名、または完全パス名を定義できます。たとえば、「services.exe」、「¥system32¥services.exe」、「c:¥windows¥system32¥services.exe」のように定義します。

タイプ: REG_MULTI_SZ

注: このレジストリ エントリの値が 1 つのみの場合、REG_SZ も有効なタイプです。

デフォルト: runas.exe explorer.exe consent.exe

注: consent.exe 値は Windows Server 2008 コンピュータのみに適用されます。

CommunicationWaitTimeout

プラグインがトランザクションを送受信するときに待機する最大時間を秒単位で定義します。

タイプ: REG_DWORD

デフォルト: 15

ExcludeProcess

プラグインが適用されないプロセスを定義します。

注: このエントリは、ApplyOnProcess が設定されていない場合にのみ有効です。

タイプ: REG_MULTI_SZ

デフォルトでは、このトークンは空白です。

OperationMode

メモリにプラグインをロードする(1)かどうかを指定します。

タイプ: REG_DWORD

デフォルト: 1

PluginName

プラグインのダイナミック リンク ライブラリ(DLL)の名前を定義します。

タイプ: REG_SZ

デフォルト: *ACInstallDir*¥bin¥RunAsPlg.dll

ServiceTimeOut

seosd のトランザクションを待つ最大間隔(ミリ秒単位)を定義します。

注: タイムアウトの値を超えると、要求が許可されます。

タイプ: REG_DWORD

デフォルト: 0x00000bb8(10 進数字で 3000)

TraceDbgEnable

cainstrm モジュールのステータス フラグをトレースするかどうか、つまり、DbgView または Kernel Debugger へのトレースを有効にするかどうかを指定します。

タイプ: RED_DWORD

制限: 0 - false。1 - true

デフォルト: 0

TraceFileEnable

ファイルへのトレースを有効にします。

タイプ: REG_DWORD

デフォルト: 0(無効)

TraceFileIsCyclic

トレース ファイルのタイプを指定します。

タイプ: REG_DWORD

制限: 0 - トレース ファイルは循環しません。1 - トレース ファイルは循環します。

デフォルト: 0

TraceFileSizeLimit

トレース ファイルの最大サイズをバイト単位で定義します。この値が 0 の場合、トレース ファイルに対して最大サイズの制限が適用されません。

タイプ: REG_DWORD

デフォルト: 0

TraceFilteringMask

各プラグインのフィルタリング マスクを定義します。このレジストリ値の有効値は、対象となるソフトウェア コンポーネントのステータスによって異なります。定義済みの値は次の 2 つです。0 - すべての情報がフィルタされます（情報は何も表示されません）。0x0fffffff - どの情報もフィルタされません（すべての情報が表示されます）。

タイプ: REG_DWORD

デフォルト: 0

注: ユーザ自身がこのレジストリ エントリの値を変更しすることはお勧めできません。 詳細については、当社テクニカル サポート（http://www.ca.com/jp/support/）にお問い合わせください。

TraceFolderPath

トレース ファイルへの完全パス名を定義します。

タイプ: REG_SZ

デフォルト: 空白

TraceOutputMask

トレース出力チャネル（デバッグ ストリーム、ファイル、または ETW）のフィルタリング マスクを指定します。トレースの出力先として、ファイル、DbgView デバッグ チャネル、または WinDbg デバッグ チャネルを指定できます。この値が 0 の場合、出力は無効になります。

タイプ: REG_DWORD

デフォルト: 0

注: ユーザ自身がこのレジストリ エントリの値を変更しすることはお勧めできません。 詳細については、当社テクニカル サポート（http://www.ca.com/jp/support/）にお問い合わせください。

TraceReadParamsSec

トレース パラメータを更新する時間間隔を定義します。WinServicePlg.dll は、TraceReadParamsSec ごとにトレース パラメータの更新を読み込みます。

タイプ: REG_DWORD

デフォルト: 60

StopPlg

CA Access Control は、使用するスタック オーバーフロー防止機能（STOP）プラグイン設定を以下のキーの下で保守します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Instrumentation¥PlugIns¥StopPlg

Instrumentation¥PlugIns¥StopPlg レジストリ キーには、以下のレジストリ エントリが含まれています。

Altitude

プラグインのロード順序を定義します。

制限： 1 ～ 1000（これらの制限を上回る値および下回る値は、内部的使用のために予約されています）

タイプ： REG_DWORD

デフォルト： 5

ApplyOnDLL

現在のプラグインが適用される DLL 名（モジュール）を定義します。

タイプ： REG_MULTI_SZ

デフォルト： Kernel32.dll

ApplyOnProcess

現在のプラグインが適用されるプロセスを定義します。

サービス名、ファイル名、または完全パス名を定義できます。たとえば、「services.exe」、「¥system32¥services.exe」、「c:¥windows¥system32¥services.exe」のように定義します。

タイプ： REG_MULTI_SZ

注：このレジストリ エントリの値が 1 つのみの場合、REG_SZ も有効なタイプです。

デフォルトでは、このトークンは設定されていません（プラグインはどのプロセスにも適用されます）。

ExcludeProcess

プラグインが適用されないプロセスを定義します。

注: このエントリは、ApplyOnProcess が設定されていない場合にのみ有効です。

タイプ: REG_MULTI_SZ

デフォルト(Windows 2008): slsvc.exe

デフォルト(他のすべての Windows バージョン): 空白(トークンは設定されません)

OperationMode

メモリにプラグインをロードする(1)かどうかを指定します。

タイプ: REG_DWORD

デフォルト: 0

PluginName

プラグインのダイナミック リンク ライブラリ(DLL)の名前を定義します。

タイプ: REG_SZ

デフォルト: *ACInstallDir*¥bin¥StopPlg.dll

STOPClientTraceEnabled

STOP クライアント モジュールのトレース ロギングを有効にするかどうかを指定します。

タイプ: REG_DWORD

デフォルト: 0(無効)

STOPClientTraceModulePath

STOP クライアント モジュールのトレース ロギング モジュールの完全パス名を定義します。

タイプ: REG_SZ

デフォルト: *ACInstallDir*¥bin¥STOPClientTrace.dll

STOPSEHHandlingModeDisabled

SEH ベースの攻撃に対して STOP による広範なチェックを有効にするかどうかを指定します。

タイプ: REG_DWORD

デフォルト: 1(無効)

TraceDbgEnable

cainstrm モジュールのステータス フラグをトレースするかどうか、つまり、DbgView または Kernel Debugger へのトレースを有効にするかどうかを指定します。

タイプ: RED_DWORD

制限: 0 - false。1 - true

デフォルト: 0

TraceFileIsCyclic

トレース ファイルのタイプを指定します。

タイプ: REG_DWORD

制限: 0 - トレース ファイルは循環しません。1 - トレース ファイルは循環します。

デフォルト: 0

TraceFileSizeLimit

トレース ファイルの最大サイズをバイト単位で定義します。この値が 0 の場合、トレース ファイルに対して最大サイズの制限が適用されません。

タイプ: REG_DWORD

デフォルト: 0

TraceFilteringMask

各プラグインのフィルタリング マスクを定義します。このレジストリ値の有効値は、対象となるソフトウェア コンポーネントのステータスによって異なります。定義済みの値は次の 2 つです。0 - すべての情報がフィルタされます(情報は何も表示されません)。0x0fffffff - どの情報もフィルタされません(すべての情報が表示されます)。

タイプ: REG_DWORD

デフォルト: 0

注: ユーザ自身がこのレジストリ エントリの値を変更しすることはお勧めできません。 詳細については、当社テクニカル サポート(http://www.ca.com/jp/support/)にお問い合わせください。

TraceFolderPath

トレース ファイルへの完全パス名を定義します。

タイプ: REG_SZ

デフォルト: 空白

TraceOutputMask

トレース出力チャネル(デバッグ ストリーム、ファイル、または ETW)のフィルタリング マスクを指定します。トレースの出力先として、ファイル、DbgView デバッグ チャネル、または WinDbg デバッグ チャネルを指定できます。この値が 0 の場合、出力は無効になります。

タイプ: REG_DWORD

デフォルト: 0

注: ユーザ自身がこのレジストリ エントリの値を変更しすることはお勧めできません。 詳細については、当社テクニカル サポート (http://www.ca.com/jp/support/) にお問い合わせください。

WinServicePlg

CA Access Control は、使用する Windows サービス保護プラグイン設定を以下のキーの下で保守します。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Instrumentation¥
PlugIns¥WinServicePlg
```

Instrumentation¥PlugIns¥WinServicePlg レジストリ キーには、以下のレジストリ エントリが含まれています。

Altitude

プラグインのロード順序を定義します。

制限: 1 ～ 1000(これらの制限を上回る値および下回る値は、内部的使用のために予約されています)

タイプ: REG_DWORD

デフォルト: 5

ApplyOnDLL

現在のプラグインが適用される DLL 名 (モジュール)を定義します。

タイプ: REG_MULTI_SZ

デフォルト: Rpcrt4.dll

ApplyOnProcess

現在のプラグインが適用されるプロセスを定義します。

サービス名、ファイル名、または完全パス名を定義できます。たとえば、「services.exe」、「¥system32¥services.exe」、「c:¥windows¥system32¥services.exe」のように定義します。

タイプ: REG_MULTI_SZ

注: このレジストリ エントリの値が 1 つのみの場合、REG_SZ も有効なタイプです。

デフォルト: Services.exe

ExcludeProcess

プラグインが適用されないプロセスを定義します。

注: このエントリは、ApplyOnProcess が設定されていない場合にのみ有効です。

タイプ: REG_MULTI_SZ

デフォルトでは、このトークンは空白です。

OperationMode

メモリにプラグインをロードする(1)かどうかを指定します。

タイプ: REG_DWORD

デフォルト: 1

PluginName

プラグインのダイナミック リンク ライブラリ(DLL)の名前を定義します。

タイプ: REG_SZ

デフォルト: *ACInstallDir*¥bin¥WinServicePlg.dll

ServiceTimeOut

seosd のトランザクションを待つ最大間隔(ミリ秒単位)を定義します。

注: タイムアウトの値を超えると、要求が許可されます。

タイプ: REG_DWORD

デフォルト: 0x00000bb8(10 進数字で 3000)

TraceDbgEnable

cainstrm モジュールのステータス フラグをトレースするかどうか、つまり、DbgView または Kernel Debugger へのトレースを有効にするかどうかを指定します。

タイプ: RED_DWORD

制限: 0 - false。1 - true

デフォルト: 0

TraceFileEnable

ファイルへのトレースを有効にします。

タイプ: REG_DWORD

デフォルト: 0(無効)

TraceFileIsCyclic

トレース ファイルのタイプを指定します。

タイプ: REG_DWORD

制限: 0 - トレース ファイルは循環しません。1 - トレース ファイルは循環します。

デフォルト: 0

TraceFileSizeLimit

トレース ファイルの最大サイズをバイト単位で定義します。この値が 0 の場合、トレース ファイルに対して最大サイズの制限が適用されません。

タイプ: REG_DWORD

デフォルト: 0

TraceFilteringMask

各プラグインのフィルタリング マスクを定義します。このレジストリ値の有効値は、対象となるソフトウェア コンポーネントのステータスによって異なります。定義済みの値は次の 2 つです。0 - すべての情報がフィルタされます（情報は何も表示されません）。0x0fffffff - どの情報もフィルタされません（すべての情報が表示されます）。

タイプ： REG_DWORD

デフォルト： 0

注：ユーザ自身がこのレジストリ エントリの値を変更しすることはお勧めできません。 詳細については、当社テクニカル サポート（http://www.ca.com/jp/support/）にお問い合わせください。

TraceFolderPath

トレース ファイルへの完全パス名を定義します。

タイプ： REG_SZ

デフォルト：空白

TraceOutputMask

トレース出力チャネル（デバッグ ストリーム、ファイル、または ETW）のフィルタリング マスクを指定します。トレースの出力先として、ファイル、DbgView デバッグ チャネル、または WinDbg デバッグ チャネルを指定できます。この値が 0 の場合、出力は無効になります。

タイプ： REG_DWORD

デフォルト： 0

注：ユーザ自身がこのレジストリ エントリの値を変更しすることはお勧めできません。 詳細については、当社テクニカル サポート（http://www.ca.com/jp/support/）にお問い合わせください。

TraceReadParamsSec

トレース パラメータを更新する時間間隔を定義します。WinServicePlg.dll は、TraceReadParamsSec ごとにトレース パラメータの更新を読み込みます。

タイプ： REG_DWORD

デフォルト：0x0000003c（10 進数字で 60）

lang

CA Access Control は、使用する管理言語（selang）設定を以下のキーの下で保守します。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥lang
```

lang レジストリ キーには、以下のレジストリ エントリが含まれています。

HandleHomeDir

ネイティブ ユーザ アカウントのプロパティ HOME_DIR が更新されてホーム ディレクトリが作成されるかどうかを判別する値。

値が 0 に設定されている場合、ユーザのプロパティ HOME_DIR の更新のみが行われます。値が 1 に設定されている場合、ユーザのプロパティが更新され、ファイル システムにホーム ディレクトリが物理的に作成されます。

デフォルト: 1

help_path

lang ヘルプ ファイルがインストールされているディレクトリ。

デフォルト: *ACInstallDir*¥data¥help

ModifiableClassFlags

CA Access Control 管理者が以下の selang コマンドを使用して変更できるフラグを指定します: setoptions class *className* flags{+ | -} (*flag*)

値: W — 特定のクラスの警告モードを設定します。I — 特定のクラスのリソースの大文字小文字を変更します。WI — 特定のクラスのリソースの警告モードを設定し、大文字小文字を変更します

デフォルト: W

query_size

データベースへの問い合わせで一覧表示されるレコードの最大数。

デフォルト: 100

SetBlockRun

Trusted プログラムの確認を行うかどうか、および Untrusted プログラムの実行をブロックするかどうかを指定します。

有効な値は以下のとおりです。

yes - viapgm アクセス権限ルールで定義されたすべてのプログラムでは、blockrun プロパティが yes に設定されます。

no - viapgm アクセス権限ルールで定義されたすべてのプログラムでは、blockrun プロパティが no に設定されます。

デフォルト: yes

SpaceReplace

内部的使用のみ。このキーは、常に空であることが必要です。

デフォルト: ""

use_old_commands

ACF2™ と互換性のある古いコマンド（ag、lg、rg、lu、au など）を無効にするかどうかを指定します。

制限: 0 — 古いコマンドをサポートしない、1— 古いコマンドをサポートする

デフォルト: 1（古いコマンドをサポートす）

logmgr キー - レジストリの設定

CA Access Control は、使用するロギング設定を以下のキーの下で保守します。

`HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥logmgr`

logmgr レジストリ キーには、以下のレジストリ エントリが含まれています。

audit_back

CA Access Control の監査バックアップ ファイルの名前。このファイルに対する書き込みを実行できるのは CA Access Control のみです。

デフォルト: *ACInstallDir*¥log¥seos.audit.bak

audit_group

監査ログに対する読み取り権限を持つグループ。

デフォルト: ComputerAssociates

audit_log

CA Access Control の監査ログ ファイルの名前。このファイルが audit_size で指定されたサイズに達すると、CA Access Control はファイルを閉じて、このファイルの名前を audit_back で指定された名前に変更した後、新しい監査ログを作成します。このファイルに対する書き込みを実行できるのは CA Access Control のみです。

デフォルト: *ACInstallDir*¥log¥seos.audit

audit_max_files

CA Access Control が日付によるバックアップを実行するときに蓄積する監査ログ バックアップ ファイルの最大数を定義します。BackUp_Date の設定が［*なし*］以外の任意の値に設定されている場合は、CA Access Control は引き続き日付によるバックアップ ファイルを蓄積します。この設定を使用すると、CA Access Control が監査ログのバックアップに使用するディスク領域を削減することができます。監査ログのバックアップ ファイル数が設定された制限に達すると、CA Access Control は最新のファイルを作成するときに最も古いバックアップ ファイルを削除します。

値は以下のとおりです。

- **0** - すべての監査ログ バックアップ ファイルを保持します。
- *n* - 0 を超える 正の整数。

注: CA Access Control は重複監査ログ バックアップ ファイルを自動的に保護するため、それらを手動で削除することはできません。さらに、監査レポートが有効な場合、レポート エージェントが処理を完了するまで、CA Access Control はバックアップ ファイルを削除しません。

デフォルト: 50

audit_size

CA Access Control の監査ログ ファイルの最大サイズ（KB 単位）。50 KB 以上のサイズを指定してください。

デフォルト: 10240

注: 監査ファイルのサイズが 2GB を超える場合、CA Access Control は、監査ファイルへの監査レコードの書き込みを停止します。

AuditFiltersFile

CA Access Control の監査フィルタ ファイルの名前。

デフォルト: *ACInstallDir*¥data¥audit.cfg

BackUp_Date

CA Access Control が監査ログ ファイルをバックアップする条件、および CA Access Control がタイムスタンプをバックアップ ファイル名に追加するかどうかを指定します。

audit_size 設定で指定されたサイズに達すると、CA Access Control は*常に*監査ログ ファイルをバックアップします。

値: none、yes、daily、weekly、monthly

- yes -- audit_size で指定されたサイズに達すると、CA Access Control は監査ログ ファイルをバックアップしし、タイム スタンプをバックアップ ファイル名に追加します。
- none -- audit_size で指定されたサイズに達すると、CA Access Control は監査ログ ファイルをバックアップしますが、タイム スタンプをバックアップ ファイル名に追加しません。
- daily、weekly、monthly -- 指定された時間間隔が経過し、かつ audit_size で指定されたサイズに達すると、CA Access Control は監査ログ ファイルをバックアップし、タイムスタンプをバックアップ ファイル名に追加します。ただし、指定された時間間隔内に監査イベントが監査ログ ファイルに書き込まれない場合、間隔が経過しても、CA Access Control はファイルをバックアップしません。

  注: CA Access Control は、最初の監査ログ ファイルを作成した時間から指定された間隔を数え、適切な日の午前零時にファイルをバックアップします。

例: 設定には週単位の値があり、CA Access Control は 4 月 1 日午前 9 時に監査ログ ファイルを作成します。多くの監査イベントが今週発生し、監査ログ ファイルは 4 月 4 日月曜日上に audit_size 設定で指定された値を超過します。CA Access Control は 4 月 4 日に監査ログ ファイルをバックアップし、タイム スタンプをバックアップ ファイル名に追加します。監査ログ ファイルが最初に作成された一週間後の 4 月 8 日金曜日の午前零時に、CA Access Control は再度監査ログ ファイルをバックアップし、タイムスタンプをバックアップ ファイル名に追加します。

制限: 値は、すべて大文字またはすべて小文字で指定する必要があります。

デフォルト: yes

error_back

CA Access Control のエラー バックアップ ファイルの名前。

デフォルト: *ACInstallDir*¥log¥seos.error.bak

error_group

エラー ログ ファイルに対する読み取り権限を持つグループ。

この値が none に設定されている場合は、Administrators グループのみがファイルを読み取れます。

デフォルト: none

error_log

CA Access Control のエラー ログ ファイルの名前。このファイルが error_size で指定されたサイズに達すると、CA Access Control はファイルを閉じ、このファイルの名前を error_back に指定された名前に変更し、新しいエラー ログを作成します。このファイルに対する書き込みを実行できるのは CA Access Control のみです。

デフォルト: *ACInstallDir*¥log¥seos.error

error_size

CA Access Control のエラー ログ ファイルの最大サイズ(KB 単位)。

デフォルト: 50

irecorder_audit

IR API ライブラリが、ローカル セキュリティ サービスの監査イベントだけでなく、既存の PMD の監査イベントも送るかどうかを指定します。

all - ローカル セキュリティ サービスの監査イベントだけでなく、Policy Model の監査イベントも送ります。

localhost - ローカル セキュリティ サービスの監査イベントのみを送ります。

デフォルト: all

SendAuditToNativeChannel

(Windows 2008 のみ) seosd が監査イベントを CA Access Control の Windows 2008 イベント ログ チャネルに送信するかどうかを指定します(1)。

デフォルト: 0(設定しない)

SendAuditToNativeLog

seosd が監査イベントを Windows イベント ログに送信するかどうかを指定します(1)。

デフォルト: 0(設定しない)

message

CA Access Control は、使用するメッセージ設定を以下のキーの下で保守します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥message

message レジストリ キーには、以下のレジストリ エントリが含まれています。

filename

CA Access Control のコマンドに応答して表示される大部分のメッセージを提供するファイルの名前。

デフォルト: *ACInstallDir*¥Data¥SeOS.msg

MessagesDirectory

CA Access Control メッセージ ファイルの場所を指定します。

デフォルト: *ACInstallDir*¥Data¥Messages

OS_user

CA Access Control は、使用するエンタープライズ ユーザ設定を以下のキーの下で保守します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥OS_user

OS_user レジストリ キーには、以下のレジストリ エントリが含まれています。

create_user_in_db

CA Access Control に定義されていないユーザがログインしたときに、そのユーザの XUSER レコードを CA Access Control が作成するかどうかを指定します。

注: この設定は、エンタープライズ ユーザを使用する (osuser_enabled が 1 に設定されている) 場合にのみ適用されます。

有効な値は以下のとおりです。

0 - CA Access Control は XUSER レコードを自動的に作成しません。

1 - CA Access Control は XUSER レコードを自動的に作成します。

デフォルト: 1

osuser_enabled

エンタープライズ ユーザおよびエンタープライズ グループを有効にするかどうかを指定します。

有効な値は以下のとおりです。

0 - エンタープライズ ユーザおよびエンタープライズ グループの使用が無効になっています。

1 - エンタープライズ ユーザおよびエンタープライズ グループの使用が有効になっています。

デフォルト: 1

passwd

CA Access Control は、使用するパスワード設定を以下のキーの下で保守します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥passwd

passwd レジストリ キーには、以下のレジストリ エントリが含まれています。

DefaultPgroup

内部的使用のみ。

デフォルト: other

ディクショナリ

パスワードとして使用 *できない* 語が格納されているファイルの完全パス名を定義します。

注: このファイルを使用するには、*ファイル*に辞書形式パスワード ルール (use_dbdict)を設定し、UseDict 設定を *yes* に設定する必要があります。辞書形式が *db* に設定された場合、使用できないパスワードは CA Access Control データベースから取得され、この設定は無視されます。

デフォルト: *ACInstallDir*¥data¥words

EnforceViaEtrust

CA Access Control のみを使用して、ユーザのパスワードの更新または作成を行うかどうかを指定します。

デフォルト: 0 (CA Access Control を使用する必要なし)

PasswordTimeOut

CA Access Control のパスワード フィルタが認証レスポンスを待つ最大ミリ秒数を定義します。

デフォルト: 4000

PasswordTimeOutAnswer

指定したタイムアウト期間内に認証プロセスが応答しない場合に、LSA に返信する回答を指定します。

これを 0 に設定した場合は、パスワードの変更が拒否されます。これを 1 に設定した場合は、パスワードの変更が承認されます。

デフォルト: 0

UseDict

パスワードの確認時に、(Dictionary 設定で指定された)辞書ファイルを使用するかどうかを指定します。

注: 辞書ファイルを使用するには、*ファイル*に辞書形式パスワード ルール(use_dbdict)を設定する必要があります。辞書形式が *db* に設定された場合、使用できないパスワードは CA Access Control データベースから取得され、この設定は無視されます。

デフォルト: no

Pmd

CA Access Control は、使用する汎用の Policy Model 設定を以下のキーの下で保守します。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Pmd
```

Pmd レジストリ キーには、以下のレジストリ エントリが含まれています。

__pmd_backup_directory__

CA Access Control が Policy Model のバックアップを格納するために使用するディレクトリを定義します。CA Access Control は各 PMD バックアップを *pmd_name* という名前のサブディレクトリに格納します。

デフォルト: *ACInstallDir*¥Data¥policies_backup

_Pmd_directory_

PMDB データベース ファイルが格納されているディレクトリを定義します。

デフォルト: *ACInstallDir*¥Data

ClientOperationTimeout

このコンピュータの Policy Model クライアントが、Policy Model から応答があるまで待つ時間を秒単位で定義します。Policy Model が指定された時間内に応答しない場合、Policy Model クライアントは Policy Model を応答していないものと見なします。

デフォルト: 60

MaximumPolicyModels

作成できる Policy Model の最大数を定義します。

デフォルト: 16

SendAuditToNativeLog

CA Access Control が Policy Model の監査イベントを Windows イベント ログに送信するかどうかを指定します。

値: 0 — 監査イベントを Windows イベントログに送信しません。1 — 監査イベントを Windows イベント ログに送信します。

デフォルト: 0

ShutdownWaitingTimeout

このコンピュータの Policy Model が、そのコンポーネントが安全に停止するまで待つ時間をミリ秒単位で定義します。指定された時間内に Policy Model のコンポーネントが安全に停止しない場合、Policy Model によって強制的に停止されます。

デフォルト: 60000（1 分）

TCPReceiveTimeout

このコンピュータの Policy Model が、そのサブスクライバから応答があるまで待つ時間を秒単位で定義します。指定された時間内に Policy Model のサブスクライバが応答しない場合は、Policy Model によってサブスクライバとの接続が解除されます。

デフォルト: 60

<PMDB_Name>

CA Access Control は、使用する特定の Policy Model 設定を以下のキーの下で保守します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Pmd¥*PMDB_Name*

それぞれの Pmd¥*PMDB_Name* レジストリ キーには、以下のレジストリ エントリが含まれています。

_Min_Retries

サブスクライバが利用不能と判断する前に、Policy Model が行う失敗したサブスクライバ接続の回数を定義します。

デフォルト: 4

_Retry_Timeout

_Min_Retries で指定された最少試行回数の実行後、利用不能なサブスクライバに更新を再送する前に、Policy Model が待機する時間を分単位で指定します。

デフォルト: 30

_Shutoff_Time_

使用されなくなりました。

Active_Policy

Policy Model 名を定義します。

Always_Propagate

エラーがあるときに Policy Model がコマンドを伝達するかどうかを指定します。デフォルトでは、Policy Model は常に、コマンドを送信して伝達します。これを *no* に設定した場合は、エラーがあるときに Policy Model はコマンドを送信しなくなります。

デフォルト: yes

Auto_Truncate

自動またはオフセットのいずれかを指定せずに sepmd -t を実行する場合、sepmd が更新ファイルを切り捨てるかどうかを指定します。

値: Yes — sepmd -t パラメータが指定されていない場合、sepmd は自動的に更新ファイルを切り捨てる、No — sepmd -t パラメータが指定されていない場合、sepmd は更新ファイルを切り捨てない

デフォルト: yes

フィルタ

更新ファイルのフィルタ ファイルの完全パス名を定義します。

デフォルト値なし

force_auto_truncate

Policy Model のサブスクライバが存在しない場合でも、CA Access Control が更新ファイルを切り捨てるかどうかを指定します。

更新ファイルは（sepmd -t を使用して）手動で切り捨てることができます。また、CA Access Control は、自動切り捨てをトリガするイベントを定義した別の環境設定（trigger_auto_truncate）に基づいて、ファイルを自動的に切り捨てます。

注: Policy Model のサブスクライバがすべて「非同期」の場合、Policy Model には実質的にサブスクライバがありません。

デフォルト: yes

Parent_Pmd

この Policy Model が更新を受け取る親 PMDB の名前を定義します。

デフォルト値なし

trigger_auto_truncate

Policy Model 更新ファイルの自動切り捨てをトリガするサイズ（メガバイト単位）を定義します。

このエントリを 0 に設定すると、CA Access Control はハードコードされたデフォルト値（100MB）を使用します。上限より大きな値を使用した場合は、上限の値が使用されます。

タイプ: REG_DWORD

制限: 1 ～ 2000 MB

デフォルト (DMS__ and DH__WRITER): 1024 MB

デフォルト（他のすべての PMDB）: 100 MB

UseEncryption

updates.dat ファイルに保存される更新情報を暗号化するかどうかを指定します。

値: 0 — updates.dat ファイルを暗号化しない、1 — updates.dat ファイルを暗号化する

デフォルト: 0

logmgr

CA Access Control は、使用する特定の Policy Model ログ設定を以下のキーの下で保守します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Pmd¥*PMDB_Name*¥logmgr

それぞれの Pmd¥*PMDB_Name*¥logmgr レジストリ キーには、以下のレジストリ エントリが含まれています。

audit_back

Policy Model の監査バックアップ ファイルの名前を定義します。このファイルに対する書き込みを実行できるのは CA Access Control のみです。

デフォルト: pmd_audit.bak

audit_group

監査ログに対する読み取り権限を持つグループを定義します。

デフォルト: Computer Associates

audit_log

Policy Model の監査ログ ファイルの名前を定義します。このファイルが audit_size で指定されたサイズに達すると、CA Access Control はファイルを閉じて、このファイルの名前を audit_back で設定された名前に変更した後、新しい監査ログを作成します。このファイルに対する書き込みを実行できるのは CA Access Control のみです。

デフォルト: pmd.audit

audit_size

Policy Model の監査ログ ファイルの最大サイズ(KB 単位)を定義します。50 KB 以上の値を指定してください。

デフォルト: 1024

error_back

Policy Model のエラー バックアップ ファイルの名前を定義します。

デフォルト: pmd_error.back

error_group

エラー ログ ファイルに対する読み取り権限を持つグループを定義します。

この値が *none* に設定されている場合は、Administrators グループのみがファイルを読み取れます。

デフォルト: none

error_log

Policy Model のエラー ログ ファイルの名前を指定します。このファイルが error_size で指定されたサイズに達すると、CA Access Control はファイルを閉じ、このファイルの名前を error_back に指定された名前に変更し、新しいエラー ログを作成します。このファイルに対する書き込みを実行できるのは CA Access Control のみです。

デフォルト: pmd.error

error_size

CA Access Control のエラー ログ ファイルの最大サイズ(KB 単位)を定義します。

デフォルト: 1024

<DMS_Name>

CA Access Control は、使用する特定の DMS 設定を以下のキーに保持します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Pmd¥*DMS_Name*

Pmd¥*DMS_Name* レジストリ キーには、以下のレジストリ エントリが含まれています。

_Min_Retries

サブスクライバが利用不能と判断する前に、Policy Model が行う失敗したサブスクライバ接続の回数を定義します。

デフォルト: 4

_Retry_Timeout

_Min_Retries で指定された最少試行回数の実行後、利用不能なサブスクライバに更新を再送する前に、Policy Model が待機する時間を分単位で指定します。

デフォルト: 30

_Shutoff_Time_

使用されなくなりました。

Active_Policy

Policy Model 名を定義します。

Always_Propagate

エラーがあるときに Policy Model がコマンドを伝達するかどうかを指定します。デフォルトでは、Policy Model は常に、コマンドを送信して伝達します。これを *no* に設定した場合は、エラーがあるときに Policy Model はコマンドを送信しなくなります。

デフォルト: yes

Auto_Truncate

自動またはオフセットのいずれかを指定せずに sepmd -t を実行する場合、sepmd が更新ファイルを切り捨てるかどうかを指定します。

値: Yes — sepmd -t パラメータが指定されていない場合、sepmd は自動的に更新ファイルを切り捨てる、No — sepmd -t パラメータが指定されていない場合、sepmd は更新ファイルを切り捨てない

デフォルト: yes

フィルタ

更新ファイルのフィルタ ファイルの完全パス名を定義します。

デフォルト値なし

force_auto_truncate

Policy Model のサブスクライバが存在しない場合でも、CA Access Control が更新ファイルを切り捨てるかどうかを指定します。

更新ファイルは（sepmd -t を使用して）手動で切り捨てることができます。また、CA Access Control は、自動切り捨てをトリガするイベントを定義した別の環境設定（trigger_auto_truncate）に基づいて、ファイルを自動的に切り捨てます。

注: Policy Model のサブスクライバがすべて「非同期」の場合、Policy Model には実質的にサブスクライバがありません。

デフォルト: yes

Parent_Pmd

この Policy Model が更新を受け取る親 PMDB の名前を定義します。

デフォルト値なし

trigger_auto_truncate

Policy Model 更新ファイルの自動切り捨てをトリガするサイズ（メガバイト単位）を定義します。

このエントリを 0 に設定すると、CA Access Control はハードコードされたデフォルト値（100MB）を使用します。上限より大きな値を使用した場合は、上限の値が使用されます。

タイプ： REG_DWORD

制限： 1 ～ 2000 MB

デフォルト (DMS__ and DH__WRITER)： 1024 MB

デフォルト（他のすべての PMDB）： 100 MB

UseEncryption

updates.dat ファイルに保存される更新情報を暗号化するかどうかを指定します。

値： 0 — updates.dat ファイルを暗号化しない、1 — updates.dat ファイルを暗号化する

デフォルト： 0

endpoint_management

CA Access Control は、使用する特定の DMS エンドポイント管理設定を以下のキーに保持します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Pmd¥*DMS_NAME*¥endpoint_management

dmsmgr は、DMS を作成するときにこのキーにレジストリ値を定義します。DMS がホストに存在しない場合、このキーは定義されません。

Pmd¥*DMS_Name*¥endpoint_management レジストリ キーには、以下のレジストリ エントリが含まれています。

commands_to_exec_before_sleep

DMS がスリープ前にループ中で実行するエンドポイント コマンドの数を指定します。

デフォルト: 10

debug_mode

CA Access Control が DMS ディレクトリ(1)内の endpoint_management.log ファイルにデバッグ メッセージを書き込むかどうかを指定します。

制限: 0,1

デフォルト: 0 (デバッグは無効になります)

注: ログ ファイルは、*DMSInstallDirectory*¥endpoint_management.log にあります。

operation_mode

CA Access Control メッセージ キューによる一元(DMS)エンドポイント管理を有効にするかどうかを指定します。

制限: 0、1

デフォルト: 1 (有効)

sleep_between_exec_commands

DMS のスリープ期間をミリ秒単位で指定します。DMS は、スリープから復帰したときに commands_to_exec_before_sleep レジストリ値で指定された数のエンドポイント コマンドを実行します。

デフォルト: 100

policyfetcher

CA Access Control は、使用する policyfetcher サービス設定を以下のキーの下で保守します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥policyfetcher

policyfetcher レジストリ キーには、以下のレジストリ エントリが含まれています。

check_deployment_tasks

分散ホスト上で新規のデプロイ タスク(DEPLOYMENT リソース)を policyfetcher がチェックする頻度(秒単位)を定義します。

デフォルト: 600(10 分ごと)

deploy_timeout

デプロイ タスクまたはデプロイ解除タスクがエンドポイントで完了するのを policyfetcher が待つ秒数を定義します。

デフォルト: 900

devcalc_command

policyfetcher で偏差計算の実行に使用する selang コマンドを定義します。

デフォルト: start DEVCALC params(-nonotify)

例: start DEVCALC params(-nonotify -precise)

dh_command_retry_interval

DH 通知コマンドの試行間隔を秒数で定義します。

デフォルト: 30

endpoint_heartbeat

policyfetcher が分散ホスト(DH)にハートビートを送信する頻度を定義します。この頻度は check_deployment_task 設定の要因であり、policyfetcher がハートビートを送信する前にデプロイ タスクをチェックする回数を決定します。たとえば、check_deployment_task がデフォルトの 600 秒(10 分)に設定されているときに 6 に設定すると、policyfetcher は 3600 秒(1 時間)ごとにハートビートを送信します。

ハートビートの送信後、policyfetcher はさらに偏差計算を実行(devcalc コマンドを開始)し、偏差計算が完了するのを 60 秒待ちます。60 秒後、policyfetcher は、ローカル エンドポイント情報が DH 情報と同一であることを確認します。

デフォルト: 10

max_dh_command_retry

policyfetcher が DH から更新通知の取得を再試行する最大回数を定義します。この回数を超えても取得されない場合は、再試行されなくなります。

デフォルト: 3

max_dh_retry_cycles

policyfetcher が本番の DH から更新通知の取得を再試行する最大サイクル数を定義します。このサイクル数を超えても取得されない場合、惨事復旧用の DH に移行します。

デフォルト: 3

policy_verification

policyfetcher がバックアップ CA Access Control データベース上で新しいデプロイ タスクを実行する前にそれらを検証するかどうかを指定します。

有効な値は以下のとおりです。

1 - ポリシー検証を実行する

0 - ポリシー検証を無効にする

デフォルト: 0

policyfetcher_enabled

policyfetcher サービスを実行するかどうかを指定します。

有効な値は以下のとおりです。

1 - policyfetcher を実行する

0 - policyfetcher を無効にする

デフォルト: 0

PUPMAgent

CA Access Control は、使用する特権ユーザ パスワード管理エージェント設定を以下のキーの下で保守します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥PUPMAgent

特権ユーザ パスワード管理 エージェント レジストリ キーには、以下のレジストリ エントリが含まれています。

EnableLogonIntegration

端末統合が有効であると指定します。

制限: 0 - 端末統合は無効です。1 - 端末統合は有効です。

デフォルト: 1

EnableRunAsInterface

特権ユーザ パスワード管理 エージェントがターゲット ユーザのパスワードでプロンプト表示されるかどうかを指定します。

制限: 0 -- 特権ユーザ パスワード管理 エージェントはインストールされていません。1 -- 特権ユーザ パスワード管理 はインストールされています。

デフォルト: 1

interfaceName

リクエスト処理のために、特権ユーザ パスワード管理 エージェントが使用するインターフェース名を定義します。

デフォルト: PUPMAgentInterface

OperationMode

特権ユーザ パスワード管理 エージェントの動作モードを指定します。

制限: 0 - 特権ユーザ パスワード管理 エージェントは無効です。実行されていません。1 - 特権ユーザ パスワード管理 エージェントは有効で、実行されています。しかし、トレース ファイルにデータを記録していません。2 - 特権ユーザ パスワード管理 エージェントは有効で、実行されています。また、トレース ファイルにデータを記録中です。

デフォルト: 0

ProcessArgumentsReplacement

特権ユーザ パスワード管理エージェントが Process Arguments Replacement をサポートするかどうか指定します。

制限: 0、1

デフォルト: 0

注: Process Arguments Replacement をサポートすることを選択した場合(このレジストリ エントリの値を 1 に設定した場合)、CMD Plugin も有効にする必要があります。CMD Plugin を有効にするには、以下のレジストリ エントリを 1 に設定します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Instrumentation¥plugins¥CMDPlg¥OperationMode

Report

CA Access Control は、使用する sereport 設定を以下のキーの下で保守します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Reports

Reports レジストリ キーには、レジストリ エントリが含まれていません。含まれているのは、sereport が生成するすべてのレポートのレジストリ サブキーです。

注: sereport が生成するレポートそれぞれのレジストリ エントリの詳細については、「sereport ユーティリティ (P. 243)」を参照してください。

colors

CA Access Control は、使用する sereport スタイル設定を以下のキーの下で保守します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Reports¥colors

Reports¥colors レジストリ キーには、以下のレジストリ エントリが含まれています。

background

内部的使用のみ。

このキーは変更しないでください。

class_title

レポートの class_title の色を定義します。

デフォルト: green

logo

ロゴ ファイルへの完全パス名を定義します。

デフォルト: *ACInstallDir*¥data¥logo.jpg

title

レポートのタイトルの色を定義します。

デフォルト: midnightblue

ReportAgent キー - レジストリの設定

CA Access Control は、使用するレポート エージェント設定を以下のキーの下で保守します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥ReportAgent

ReportAgent レジストリ キーには、以下のレジストリ エントリが含まれています。

audit_enabled

エンドポイント監査データを配布サーバに送信するかどうかを指定します。

値: 0 - いいえ、**1** - はい

デフォルト: 0

audit_filter

レポート エージェントが外部ソース(CA Enterprise Log Manager など)に経路指定する監査レコードのフィルタリング ルールが含まれているファイルへのフル パス名を定義します。このファイルは、レポート エージェントが経路指定するレコードを特定します。

デフォルト: *ACInstallDir*¥Data¥AuditRouteFlt.cfg

audit_queue

レポート エージェントがエンドポイント監査データを送信するキューの名前を定義します。

デフォルト: キュー/監査

audit_read_chunk

レポート エージェントが監査ファイルの単一の読み取りで収集を試みる最大監査レコードを定義します。

制限: 正の整数を入力します。

デフォルト: 300

audit_send_chunk

レポート エージェントが各接続で配布サーバに送信する監査レコードの最大数を定義します。レポート エージェントは、収集する監査レコードがこの数に達すると、それらを配布サーバに送信します。

制限: 正の整数を入力します。

デフォルト: 1800

audit_sleep

レポート エージェントが監査レポートを生成する間のスリープする時間の長さを定義します。

制限: 秒数を表す正の整数。

デフォルト: 10

audit_timeout

レポート エージェントがエンドポイント監査データを配布サーバに送信する周期を定義します。最後の送信からこの時間が経過すると、収集したレコード数が audit_send_chunk 値よりも少ない場合であっても、レポート エージェントは監査データを配布サーバに送信します。

制限: 秒数を表す正の整数。

デフォルト: 300

間隔

CA Access Control がレポートを作成して配布サーバに送信する間隔(秒)を定義します。

[*スケジュール*]設定では、間隔の開始時間および実行する曜日を定義します。レポート エージェントが予定されているオカレンスよりも遅く開始した場合は、スケジュールから計算した次の間隔でレポートを送信し、その後は予定された曜日の定義された間隔で送信します。

例: 「schedule=8:30@Mon,Tue,Wed」および「interval=5 」に設定されている場合は、レポート エージェントは火曜日の 8:47 am にロードして、レポートを 8:50 am に作成して送信します。これは、5 分間隔を使用して予定されている開始時刻から計算された最早の周期です。

値: **0** - 間隔なし(予定されているオカレンスのみを使用); *正の整数* - 間隔として使用する分数

デフォルト: 0

reportagent_enabled

ローカル コンピュータでレポートが有効(1)になっているかどうかを指定します。

デフォルト: 0

schedule

レポートを生成し、配布サーバに送信する日時を定義します。

この設定は、次の形式で指定します。time@day[,day2][...]

たとえば、「19:22@Sun,Mon」と指定すると、レポートは毎週土曜日と日曜日の 7:22 pm に生成されます。

デフォルト: 00:00@Sun,Mon,Tue,Wed,Thu,Fri,Sat

send_queue

レポート エージェントがローカル データベースおよび任意の PMDB のスナップショットを送信する配布サーバのレポート キューの名前を定義します。

デフォルト: queue/snapshots

詳細情報:

auditrouteflt.cfg ファイル - 監査レコード ルーティングのフィルタリング (P. 469)

SeOSD キー - レジストリの設定

CA Access Control は、使用する汎用設定を以下のキーの下で保守します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥SeOSD

SeOSD レジストリ キーには、以下のレジストリ エントリが含まれています。

AuditCollectorInterfaceName

パイプ名を定義します。パイプ名は、監査コレクタ コンポーネント(seosd 内)と監査コレクタの異なるクライアント(カーネル)との間の監査インターフェースとして機能します。

デフォルト: AuditCollector

AuditServerCacheSize

監査キャッシュのサイズを、エントリ数で定義します。

デフォルト: 1024

CreateNewClasses

seclassadm ユーティリティを使用して作成した新しいクラスを CA Access Control データベースに追加できるかどうかを指定します。

デフォルト: yes

CreateNewProps

sepropadm ユーティリティを使用して作成した新しいプロパティを CA Access Control データベースに追加できるかどうかを指定します。

デフォルト: yes

dbdir

CA Access Control データベースが格納されているディレクトリ。

デフォルト: *ACInstallDir*¥data¥seosdb

DefLookupThreads

SID をアカウント名に解決するために、CA Access Control が使用できるスレッド数を定義します。

デフォルト: 5

DefLookupTimeout

CA Access Control が SID のアカウント名への解決を停止するまでの、タイムアウトをミリ秒単位で定義します。

デフォルト: 2000

domain_names

照合に使用される名前のサフィックスのリスト。

長い完全修飾ホスト名を作成するために、CA Access Control がこれらのサフィックスを短いホスト名に追加します。関連する HOST クラス、CONNECT クラス、または TERMINAL クラスで、これらの名前を承認できます。完全名を識別するために、CA Access Control は短い名前に domain_names リストのドメイン名を追加して承認に使用します。HOSTNP クラスの場合、CA Access Control は、実際の IP アドレスに解決されるパターンと(このレジストリで列挙された)すべてのドメイン名を照合します。

デフォルト値なし

EnablePolicyCache

この値は、認証エンジンがキャッシュされたレコードを使用するか、またはデータベースのレコードを直接使用するかを制御します。

有効な値は以下のとおりです。

no - 認証エンジンはデータベースのレコードを使用します。

yes - 認証エンジンはキャッシュされたレコードを使用します。

デフォルト: no

EnvVarResolvingMode

埋め込み環境変数を解決する方法（FILE クラス、SECFILE クラス、PROGRAM クラス、PROCESS クラス、SPECIALPGM クラス、TERMINAL クラス、または USER クラスのオブジェクトの場合）。以下に例を示します。

newfile %SystemRoot%¥temp.txt.

0 が選択されている場合、CA Access Control はすべての環境変数の解決を試み、エラー メッセージがユーザに発行され、オブジェクトは作成されません。

1 が選択されている場合、CA Access Control はすべての環境変数の解決を試み、警告メッセージがユーザに発行され、オブジェクトが作成されます。

2 が選択されている場合、CA Access Control はすべての環境変数の解決を試み、メッセージが表示されずに、オブジェクトが作成されます。

3 が選択されている場合、CA Access Control は環境変数の解決を試みません。

注: PMDB では、環境変数が存在しないことを前提とするため、解決が試みられることはありません。

デフォルト: 2

GeneralInterceptionMode

Full Enforcement モード（0）と Audit Only モード（1）のいずれを使用するかを指定します。

デフォルト: 0

GraceCountForMessage

猶予ログインの残り回数を定義します。この回数に達すると、[パスワードを変更します]ダイアログ ボックスが表示されます。

デフォルト: 0

HostResolutionMode

ホスト名を解決する際に CA Access Control が使用するメソッドを指定します。

値は以下のとおりです。

0 - HOST 解決は同期です（現行の動作）

1 - HOST 解決は非同期です（「イベント ログ」レポート付き）

この設定の効果は、以下のとおりです。

- 制御は直ちに selang に返されます。
- HOST レコードが解決できない場合、selang メッセージは表示されません（0 と同様）。
- 通知メッセージは、「イベント ログ」に書き込まれます。

2 - HOST 解決は非同期です（「イベント ログ」レポートなし）

通知メッセージがどこにも書き込まれ*ない*ことを除いては、「1」と同様です。

デフォルト: 0

HostResolutionRenewal

内部キャッシュの更新時間。ネットワーク インターセプトの認証イベントはレジストリ値を使用します。

デフォルト: 30000

HostResolutionTimeout

ネットワーク インターセプトのイベント発生時に、認証エンジンが IP の逆引きルックアップ要求を待つ時間。

デフォルト: 2000

LogonTimeOut

CA Access Control がサブ認証 DLL（eACSubAuth.dll）によるトランザクションを待機する時間（ミリ秒単位）を定義します。この時間を過ぎると待機を止めます。この時間を過ぎると、CA Access Control は LogonTimeOutAnswer に設定された値を返信します。

デフォルト: 4000

LogonTimeOutAnswer

CA Access Control からの回答がないうちに LogonTimeOut 設定が経過した場合の、オペレーティング システムに対するログオン回答を定義します。

デフォルト: 1(true)

MaximumDiscreteFILELimit

CA Access Control データベースに作成できる個別 FILE レコードの数。

最小値はデフォルトの値です。ユーザがこの値をデフォルトよりも小さい値に設定した場合、CA Access Control は最小値が設定されたかのように動作します。

デフォルト: 4096

MaximumGenericFILELimit

CA Access Control データベースに作成できる包括 FILE レコード(名前パターン ベースのレコード)の数。

最小値はデフォルトの値です。ユーザがこの値をデフォルトよりも小さい値に設定した場合、CA Access Control は最小値が設定されたかのように動作します。

デフォルト: 512

ProcessCreationNotificationMode

カーネルまたはインストルメンテーション モードを使用して、プロセス作成をインターセプトし、seosd に通知するかどうかを指定します。

タイプ: REG_DWORD

値:

0 -- プロセス作成はカーネル モジュールを使用して実行されます。

1 -- プロセス作成はインストルメンテーション モジュールを使用して実行されます。

デフォルト: 0

注: キーを 1 に設定した場合、CA Access Control は Windows API のみを通じてプロセス作成をインターセプトします。

RebuildSuspiciousDatabase

前回のセッションでデータベースが正しく閉じられなかった場合のみ、この値が適用されます。

この値が 0 に設定されている場合、起動時に、データベースの正当性がヒューリスティックな手順で検証されます。このチェックでデータベースに問題が検出された場合は、データベースが再構築されます。

この値が 1 に設定されている場合は、ヒューリスティックな手順によるチェック機能は省略されます。データベースはデータベース完全性チェックに従って再構築されます。

デフォルト: 1

RefreshIPInterval

自動 IP 更新要求の間隔(分単位)。

値が 0 に設定されている場合、IP 更新は自動的に実行されません。1 ～ 30 の値を使用した場合、CA Access Control は、設定可能な最小間隔である 30 分を値として使用します。

注: 更新要求には時間がかかる場合があります。詳細については、secons ユーティリティの -refIP オプションを参照してください。

デフォルト: 0

ResponseFile

eACOexist.exe ユーティリティで使用する response.ini が格納されている場所。

デフォルト: *ACInstallDir*¥data¥response.ini

sim_login_timeout

アクセサ エレメント エントリ テーブル(ACEE)から、未使用の仮想ログイン ユーザ エントリを CA Access Control が削除するまでのタイムアウト(分単位)を定義します。

CA Access Control は、ACEE に格納されている情報にアクセスする必要があるときに、仮想ログインを実行して ACEE エントリを作成します。

デフォルト: 60

SurrogateInterceptionMode

SURROGATE クラスインターセプト モードを指定します。

タイプ: REG_DWORD

制限: 0 - ユーザ モード インターセプト。CA Access Control は RunAs ユーティリティから発生した偽装リクエストだけをインターセプトします。1 - カーネル モード インターセプト。CA Access Control はすべての偽装リクエストをインターセプトします。

デフォルト: 0

SusrauthReadParamsSec

トレース パラメータの更新頻度を定義します。

デフォルト: 30

SusrauthTraceDbgEnable

DbgView または Kernel Debugger へのトレースが有効(1)になっているかどうかを指定します。

デフォルト: 0

SusrauthTraceFileEnable

トレース ファイル(SusrauthTraceFileName)へのトレースが有効(1)になっているかどうかを指定します。

デフォルト: 0

SusrauthTraceFileName

トレース ファイルへの完全パス名を定義します。

デフォルト値なし

TerminalSearchOrder

認証プロセス中にどの TERMINAL レコードを検証するかを認証エンジンが判定する方法を指定します。

値は以下のとおりです。

name - 認証エンジンは最初に、名前で TERMINAL レコードを探し、その名前のレコードが見つからなかった場合は、IP アドレスの一致を探します。

nameonly - 認証エンジンは、名前で TERMINAL レコードを探し、その名前のレコードが見つからなかった場合は、検索を停止します。IP アドレス形式の TERMINAL レコードは無視されます。

IP - 認証エンジンは最初に、IP アドレスで TERMINAL レコードを探し、そのアドレスのレコードが見つからなかった場合は、名前の一致を探します。

注: TERMINAL クラスは、ワイルドカードで定義された包括的なルールをサポートしています(IP アドレスまたはホスト名のパターンの一致)。汎用ルールは、常に、特定(フルネーム)のルールの後に検証されます。たとえば、これを IP に設定した場合、IP アドレスの完全一致、ホスト名の完全一致、IP アドレスのパターン一致、ホスト名のパターン一致の順で seosd は TERMINAL リソースを探します。

デフォルト: nameonly

TermSrvTimeout

端末サービス接続時に、認証エンジンが 2 回目の連続ログインを待機するタイムアウト(ミリ秒単位)を指定します。

デフォルト: 2000

注: ユーザがローカル アカウントを使用してログインする場合、CA Access Control は 2 つのログイン試行通知を受信します。1 つ目はローカル端末から、2 つ目は端末サーバからです。ユーザが猶予ログイン回数を割り当てられている場合、2 つのログイン試行がログ記録され、また猶予回数から引かれます。このため、ログイン試行が指定されたタイムアウト期間内に発生した場合、CA Access Control は、2 番目のログインで猶予回数を更新しません。

trace_file

トレース メッセージが要求される場合の、トレース メッセージの送信先ファイルの名前。

デフォルト: *ACInstallDir*¥log¥seosd.trace

trace_file_type

トレース ファイルのタイプ。

既存のトレース ファイルのこの値を変更すると、既存のトレース ファイルは名前に拡張子「.backup」を付けて保存され、新しいトレース ファイルが指定したフォーマットで開始されます。

デフォルト: text

trace_filter

トレース メッセージのフィルタ処理に使用される、フィルタ データを保存するファイルの名前。ファイルの完全パスを指定する必要があります。

デフォルト: *ACInstallDir*¥log¥trcfilter.ini

trace_space_saver

ファイル システムに確保する空き容量(KB 単位)。空き容量がこの数値を下回ると、CA Access Control ではトレースは無効になります。

注: 使用可能な容量が後で増えた場合でも、トレースは自動的には有効になりません。

デフォルト: 5120

trace_to

トレース メッセージの送信先。none、file、または file,stop を設定します。

none を選択すると、CA Access Control はトレース メッセージを生成しません。

file を選択すると、CA Access Control はトレース メッセージを生成し、CA Access Control がアクティブになると、ただちに trace_file レジストリで指定されたファイルにそのトレース メッセージを送信します。

file,stop を選択すると、CA Access Control はサービスの初期化時にトレース メッセージを生成します。サービスが初期化された後は、トレース メッセージは生成されません。

デフォルト: file,stop

SeOSWD

CA Access Control は、使用する Watchdog の設定を以下のキーの下で保守します。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥SeOSWD
```

SeOSWD レジストリ キーには、以下のレジストリ エントリが含まれています。

PgmRest

最後のイベントの後からプログラムの再チェックの前までの期間を秒単位で指定します。チェック プログラムは、システムの過負荷を防止するために休止します。

デフォルト: 10

PgmTestInterval

プログラムの再スキャンを実行する間隔(秒単位)。

デフォルト: 18000

SecFileRest

最後のイベントの後からセキュリティで保護されたファイルの再チェックまでの期間を秒単位で指定します。チェック プログラムは、システムの過負荷を防止するために休止します。

デフォルト: 10

SecFileTestInterval

セキュリティで保護されたファイルの再スキャンを実行する間隔(秒単位)。

デフォルト: 36000

STOP

CA Access Control は、使用するスタック オーバーフロー防止機能（STOP）設定を以下のキーの下で保守します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥STOP

STOP レジストリ キーには、以下のレジストリ エントリが含まれています。

STOPIniFileName

STOP 初期化ファイルの完全パスおよび名前を定義します。このファイルには、STOP が有効になっている機能のリストが含まれています。

デフォルト: *ACInstallDir*¥Data¥stop.ini

STOPLearningModeEnabled

特殊なラーニング モードで STOP が実行されるかどうかを指定します。このモードでは、インシデントはログに記録されますが、常に許可されます。つまり、拒否インシデントはその旨がログに記録されますが、続行が許可されます。

デフォルト: 0（無効）

STOPLogFileName

スタック オーバーフロー防止機能（STOP）で使用する動的インシデント データベースの完全パスおよび名前を定義します。

デフォルト: *ACInstallDir*¥Log¥STOPRTEvents.dat

STOPServerTraceEnabled

STOP サーバ モジュールのトレース ロギングを有効にするかどうかを指定します。

デフォルト: 0（無効）

STOPSignatureBrokerName

コンピュータのホスト名を定義します。（定義した場合）このコンピュータは、STOP シグネチャ データベースの取得元として使用されます。

デフォルト値なし

STOPSignatureFileName

STOP シグネチャ ファイル（trusted インシデント データベース）の完全パスおよび名前を定義します。

デフォルト: *ACInstallDir*¥Data¥stopsignature.dat

STOPUpdateInterval

STOP シグネチャ データベースの更新を試みる間隔(分単位)を定義します。

デフォルト: 60

STOPZeroSnapshotBypassEnabled

コード スナップショットのサイズがゼロのインシデントを STOP で許可するかどうかを指定します。

デフォルト: 0(許可されていません)

Tracer

CA Access Control は、使用するモジュールのトレース設定を以下のキーの下で保守します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Tracer

Tracer レジストリ キーには、以下のレジストリ エントリが含まれています。

TraceCfgFile

CA Access Control モジュールのトレースの初期環境設定が格納されているファイルの完全パスを定義します。

デフォルト: *ACInstallDir*¥Data¥tracer.ini

TraceEnabled

トレース メカニズムを有効にするかどうかを指定します。

デフォルト: 0(無効)

UCTNG

CA Access Control は、使用する Unicenter 統合設定を以下のキーの下で保守します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥UCTNG

UCTNG レジストリ キーには、以下のレジストリ エントリが含まれています。

EvtManagerServer

Unicenter TNG ホストの名前を定義します。

Integration

Unicenter TNG との統合を有効にし、監査データを送信するかどうかを指定します。

デフォルト: 0 (統合を有効にしない)

uxauth Key - レジストリの設定

UNIX 認証ブローカ では、使用する Active Directory スキーマ設定を以下のキーで管理します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥uxauth

CA Access Control UNIX Attributes プラグインを Active Directory サーバにインストールするときに、UNIX 認証ブローカ はこのレジストリ キーをインストールします。このレジストリ キーは CA Access Control の一部としてはインストールされません。

注: デフォルトの属性は Active Directory 2003 R2 スキーマ用です。

uxauth レジストリ キーには、以下のレジストリ エントリが含まれています。

group_gid_attr_name

移行された UNIX グループの GID を UNIX 認証ブローカ がマップする先の Active Directory 属性を指定します。

デフォルト: gidNumber

Trace_Enabled

CA Access Control UNIX 属性プラグインで追跡が有効かどうかを指定します。

値: 0 — 追跡は無効。1 — 追跡は有効

デフォルト: 0

user_gecos_attr_name

移行された UNIX ユーザの gecos プロパティを UNIX 認証ブローカ がマップする先の Active Directory 属性を指定します。

デフォルト: gecos

user_gid_attr_name

移行された UNIX ユーザの GID を UNIX 認証ブローカ がマップする先の Active Directory 属性を指定します。

デフォルト: gidNumber

user_homedir_attr_name

移行された UNIX ユーザのホーム ディレクトリ プロパティを UNIX 認証ブローカ がマップする先の Active Directory 属性を指定します。

デフォルト: unixHomeDirectory

user_loginshell_attr_name

移行された UNIX ユーザのログイン シェル プロパティを UNIX 認証ブローカ がマップする先の Active Directory 属性を指定します。

デフォルト: loginShell

user_uid_attr_name

移行された UNIX ユーザの UID を UNIX 認証ブローカ がマップする先の Active Directory 属性を指定します。

デフォルト: uidNumber

WebService

CA Access Control は、使用する Web サービス設定を以下のキーの下で保守します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥WebService

注: WebService レジストリ キーおよび関連するエントリが、CA Access Control エンドポイント管理 のインストールの一部として追加されます。

WebService レジストリ キーには、以下のレジストリ エントリが含まれています。

auditFileCheckInterval

監査ファイルのサイズが定義済みの制限に達した場合に、CA Access Control Web サービスがチェックする頻度(秒単位)を定義します。

デフォルト: 60

auditFileMaxSize

CA Access Control Web サービスの監査ログ ファイルの最大サイズ(KB 単位)を定義します。

ファイルがこのサイズに達すると、Web サービスはこのファイルの名前を「*Backup_of_logFileName*」に変更後、新しい監査ログ ファイルを作成します。

デフォルト: 20000

backLog

CA Access Control Web サービスが保守する要求のキューの最大サイズを定義します。

デフォルト: 101

logFileName

CA Access Control Web サービスの監査ログ ファイルの名前を定義します。

この値を空の文字列("")のままにすると、-debug オプションを使用して Web サービスを実行したときに、Web サービスは端末にログ メッセージを送信します。

デフォルト: *ACServerInstallDir*¥WebService¥log¥WebService.log

machineName

CA Access Control Web サービスがインストールされているコンピュータの名前を定義します。

デフォルト: 127.0.0.1

maxRequestsQueue

ソケットのグローバルな要求のキューのサイズを定義します。

デフォルト: 1001

maxThreads

CA Access Control Web サービスで使用されるスレッドの数を定義します。

デフォルト: 7

portNumber

CA Access Control Web サービスで通信に使用されるポートを定義します。

デフォルト: 5248

sessionTimeOut

操作がないときに CA Access Control Web サービスがセッションを終了するまでの秒数を定義します。

デフォルト: 601

StandAloneService

CA Access Control Web Service がスタンド アロンのサービスとして機能するかどうかを指定します。

CA Access Control Web Service がスタンドアロン サービスとして機能している場合、CA Access Control サービスを secons を使用して停止するか、seosd を使用して開始すると、サービスは停止または開始されません。代わりに、Windows のネイティブ ツールを使用して、CA Access Control Web Service を開始および停止します。

CA Access Control Web Service がスタンドアロン サービスとして機能していない場合、CA Access Control サービスを secons を使用して停止するか、seosd を使用して開始すると、サービスは停止または開始されます。Windows のネイティブ ツールを使用して、CA Access Control Web Service を開始および停止します。ただし、CA Access Control Web Service を開始するために seosd -start を使用するには、CA Access Control Web Service を AccessControl¥AccessControlServices レジストリ エントリに定義する必要があります。

値: 1 — スタンドアロン サービスとして機能します。0 — スタンドアロン サービスとして機能しません

デフォルト: 1

TraceEnabled

CA Access Control Web Service コンポーネントで追跡が有効化どうかを指定します。

値: 0 — 追跡は無効。1 — 追跡は有効

デフォルト: 0

追加レジストリ キー

CA Access Control の実行方法を変更するために、以下のキーと値を追加または変更することもできます。

レジストリ エントリ	Type	Description
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥drveng¥Parameters¥DisableFileInterception	REG_DWORD	ファイル インターセプト フックが無効かどうかを定義します(関連する関数は、ブート時に初期化されません)。 **値:** 1(無効) **注**: このレジストリ エントリが存在しない場合(デフォルトの状態)、または 1 以外の値に設定されている場合、ファイル インターセプトはブート時に初期化されます。
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥drveng¥Parameters¥DisableNetworkInterception	REG_DWORD	ネットワーク インターセプト フックが無効かどうかを定義します(関連する機能は、ブート時に初期化されません)。 **値:** 1(無効) **注**: このレジストリ エントリが存在しない場合(デフォルトの状態)、または 1 以外の値に設定されている場合、ネットワーク インターセプトはブート時に初期化されます。
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥drveng¥Parameters¥DisableProcessInterception	REG_DWORD	プロセス インターセプト フックが無効かどうかを定義します(関連する機能は、ブート時に初期化されません)。 **値:** 1(無効) **注**: このレジストリ エントリが存在しない場合(デフォルトの状態)、または 1 以外の値に設定されている場合、プロセス インターセプトはブート時に初期化されます。

レジストリ エントリ	Type	Description
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥drveng¥Parameters¥DisableRegistryInterception	REG_DWORD	レジストリ インターセプト フックが無効かどうかを定義します(関連する機能は、ブート時に初期化されません)。 **値:** 1(無効) **注**: このレジストリ エントリが存在しない場合(デフォルトの状態)、または 1 以外の値に設定されている場合、レジストリ インターセプトはブート時に初期化されます。
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥SeosDrv¥Parameters¥KernelBuffersSize	REG_DWORD	CA Access Control カーネル ドライバ(seosdrv.sys)が起動するときに、デフォルトで、以下の式に従って内部で使用するメモリが割り当てられます。 number_of_buffers = amount_of_RAM たとえば、256 個のバッファを 256 MB の RAM に割り当てるとします。各バッファの長さは 4096 バイトになります。 seos.drv によって割り当てられるバッファ数を制御する場合は、このレジストリ キーを作成し、割り当てるバッファの数を設定します。 **注**: バッファ数の最小値は 32 です。
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥Eventlog¥System¥SeosDrv¥EventMessageFile	REG_EXPAND_SZ	seosdrv.sys ドライバのパス名を定義します。 **デフォルト:** %SystemRoot%¥System32¥drivers¥seosdrv.sys
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥Eventlog¥System¥SeosDrv¥TypesSupported	REG_DWORD	サポート対象のイベント タイプのビットマスクを定義する、標準的な Windows エントリです。 **デフォルト:** 7
HKEY_LOCAL_MACHINE¥System¥CurrentControlSet¥Services¥cainstrm¥parameters¥DllScanList	REG_SZ	cainstrm.sys によってインジェクションをトリガする、カンマ区切り DLL のリスト(名前別)を定義します。 **デフォルト:** デフォルトなし
HKEY_LOCAL_MACHINE¥System¥CurrentControlSet¥Services¥cainstrm¥parameters¥DllScanListRefreshPeriod	REG_DWORD	cainstrm レジストリ エントリをスキャンする間隔を秒単位で定義します。 **デフォルト:** 600

レジストリ エントリ	Type	Description
HKEY_LOCAL_MACHINE¥System¥CCS¥Services¥Cainstrm¥parameters¥ExcludeProcess	REG_MULTI_SZ	ドライバによってネイティブ計装から除外される、名前によるプロセスを指定します。 デフォルト: none

付録 A: 監査ログ レコード

このセクションには、以下のトピックが含まれています。

監査レコード

監査ログの各レコードには、列で構成されたデータが含まれています。2 つの列(日付およびタイムスタンプ)はすべてのタイプのレコードに共通です。残りの列とそこに含まれるデータは、監査レコードの作成をトリガしたイベントのタイプにより異なります。

注: 監査ログ レコードに表示される順序、番号、および列の内容は、監査ログを表示するのに選択した方法によって異なります。フィールドによっては、CA Access Control エンドポイント管理、seaudit 出力、または詳細な seaudit 出力に表示されないものがあります。また、seaudit ユーティリティを使用する場合は、指定するオプションが列の番号、順序、および内容も特定します。

監査レコードのイベント タイプを識別する方法

監査レコードのコンテンツを理解するには、最初に監査レコードのイベント タイプを識別する必要があります。これは、レコードに含まれるデータが監査レコードの作成をトリガしたイベントのタイプによって異なるためです。

注: 監査ログ レコードに表示される順序、番号、および列の内容は、監査ログを表示するのに選択した方法によって異なります。フィールドによっては、CA Access Control エンドポイント管理、seaudit 出力、または詳細な seaudit 出力に表示されないものがあります。また、seaudit ユーティリティを使用する場合は、指定するオプションが列の番号、順序、および内容も特定します。

監査レコードのイベント タイプを識別する方法

- CA Access Control エンドポイント管理 で監査レコードを表示している場合は、監査レコードが属しているイベント タイプが[監査レコード検索結果]ペインの最初の列に表示されます。

  監査レコードの詳細を表示するには、最初の列の監査イベント タイプのリンクをクリックします。

- seaudit 出力で監査レコードを表示している場合は、詳細な出力(-detail オプション)を表示してイベント タイプを表示する必要があります。

イベント タイプを識別したら、次に残りのメッセージの詳細を解釈することができます。

例: CA Access Control エンドポイント管理 の監査レコード

以下のイメージでは、CA Access Control エンドポイント管理 が監査イベントを表示する方法を示します。


監査レコード検索結果 更新

次のフィルタによる監査レコード: '今日のレコード'。最終更新日時:09/06/12 11:04

表示: 10 イベント/ページ 1 - 10/75

イベント	日付	ステータス	クラス	ユーザ名	オブジェクト/リソース	端末	プログラム
ログイン イベント	2009/06/12 11:02:26 KST	許可		_dms		dhaas01-kor	_dh_module_
ログイン イベント	2009/06/12 10:52:26 KST	許可		_dms		dhaas01-kor	_dh_module_
ログイン イベント	2009/06/12 10:42:26 KST	許可		_dms		dhaas01-kor	_dh_module_
ログイン イベント	2009/06/12 10:32:25 KST	許可		_dms		dhaas01-kor	_dh_module_
ログイン イベント	2009/06/12 10:22:25 KST	許可		_dms		dhaas01-kor	_dh_module_
セキュリティ データベース管理	2009/06/12 10:22:20 KST	成功	HNODE	_dms	dhaas01-kor	DMS__@dhaas01-kor	
ログイン イベント	2009/06/12 10:12:20 KST	許可		_dms		dhaas01-kor	_dh_module_
ログイン イベント	2009/06/12 10:02:20 KST	許可		_dms		dhaas01-kor	_dh_module_
ログイン イベント	2009/06/12 9:52:20 KST	許可		_dms		dhaas01-kor	_dh_module_
ログイン イベント	2009/06/12 9:42:20 KST	許可		_dms		dhaas01-kor	_dh_module_

1 - 10/75

例:デフォルトの seaudit 出力の監査レコード

seaudit ユーティリティでデフォルトで示される監査イベントは、以下の seaudit 出力(抜粋)のようになります。

```
19 Dec 2008 16:46:47 P WINSERVICE  TM123VM-AC¥Administrator Read    1059  2 VMTools
C:¥WINDOWS¥system32¥services.exe TM123VM-AC
19 Dec 2008 16:46:52 P WINSERVICE  TM123VM-AC¥Administrator Read    1059  2 VMTools
C:¥WINDOWS¥system32¥services.exe TM123VM-AC
19 Dec 2008 16:46:53 P LOGIN        TM123VM-AC¥Administrator   55  2 TM123VM-AC
C:¥WINDOWS¥system32¥lsass.exe
19 Dec 2008 16:46:57 P WINSERVICE  TM123VM-AC¥Administrator Read    1059  2 VMTools
C:¥WINDOWS¥system32¥services.exe TM123VM-AC
19 Dec 2008 16:47:02 P WINSERVICE  TM123VM-AC¥Administrator Read    1059  2 VMTools
C:¥WINDOWS¥system32¥services.exe TM123VM-AC
19 Dec 2008 16:47:07 P WINSERVICE  TM123VM-AC¥Administrator Read    1059  2 VMTools
C:¥WINDOWS¥system32¥services.exe TM123VM-AC
19 Dec 2008 16:47:12 P WINSERVICE  TM123VM-AC¥Administrator Read    1059  2 VMTools
C:¥WINDOWS¥system32¥services.exe TM123VM-AC
19 Dec 2008 16:47:16 S UPDATE      GROUP     TM123VM-AC¥Administrator  336  0 test
TM123VM-AC egtest audit-
19 Dec 2008 18:28:18 P LOGIN        TM123VM-AC¥Administrator   55 10 TM123VM-AC
selang
19 Dec 2008 18:28:18 S UPDATE       TERMINAL   TM123VM-AC¥Administrator  305  0
TM123VM-AC-SC1.ca.com TM123VM-AC er terminal TM123VM-AC-SC1.ca.com
```

上記のメッセージのうち、最初の seaudit 出力について、詳細を以下に示します。

```
19 Dec 2008 16:46:47 P WINSERVICE  TW852VM-AC¥Administrator Read    1059  2 VMTools
C:¥WINDOWS¥system32¥services.exe TM123VM-AC
Event type: Resource access
Status: Permitted
Class: WINSERVICE
Resource: VMTools
Access: Read
User name: TM123VM-AC¥Administrator
User Logon Session ID: 00000000:05647d29
Terminal: TM123VM-AC
Program: C:¥WINDOWS¥system32¥services.exe
Date: 19 Dec 2008
Time: 16:46
Details: Default record universal access check
Audit flags: AC database user
```

監査イベント タイプ

CA Access Control が監査ログに保存する情報は、監査するイベントのタイプによって決定されます。

CA Access Control では、以下のイベント タイプの監査レコードを記録します。

ログイン イベント

ログイン イベントは、CA Access Control または CA Access Control の保護されたホストへのログイン試行を示します。

このイベントの監査レコードは、以下の形式になります。

Date Time Status Event UserName SessionID Details Reason Terminal Program AuditFlags

Date

イベントが発生した日付を識別します。

形式: DD MMM YYYY

注: CA Access Control エンドポイント管理 は日付の表示をコンピュータの設定に従って整形します。

Time

イベントが発生した時間を識別します。

形式: HH:MM:SS

注: CA Access Control エンドポイント管理 は時間の表示をコンピュータの設定に従って整形します。

ステータス

イベントのリターン コードを示します。

値: 以下のいずれかです。

- D（拒否）- 権限が不十分なためイベントが拒否されました。
- P（許可）- イベントが許可されました。
- W（警告）- アクセス要求はアクセス ルールに違反していますが警告モードが設定されたためイベントが許可されました。

イベント タイプ

このレコードが属するイベントのタイプを識別します。

注: CA Access Control エンドポイント管理 はこのフィールドを単にイベントとして参照します。

ユーザ名

このイベントをトリガしたアクションを実行したアクセス元の名前を識別します。

User Logon Session ID

アクセス元のセッション ID を識別します。

注: デフォルトでは、このフィールドは seaudit の詳細でない出力には表示されません。seaudit の詳細でない出力でこのフィールドを表示するには、seaudit コマンドに -sessionid オプションを指定します。

詳細

CA Access Control がこのイベントに対して実行するアクションを決定したステージを示します。

注: seaudit の詳細でない出力では、監査レコードのこのフィールドに数字が表示されます。この数字は承認 stage code といいます。詳細な出力または CA Access Control エンドポイント管理 では、監査レコードに承認 stage code に関連するメッセージが表示されます。すべての stage code を一覧表示するには、seaudit -t を実行します。

Reason

CA Access Control が監査レコードを書き込んだ理由を示します。

注: このフィールドは seaudit の詳細な出力または CA Access Control エンドポイント管理 には表示されません。seaudit の詳細でない出力では、監査レコードのこのフィールドに数字が表示されます。この数字は理由コードといいます。すべての理由コードを一覧表示するには、seaudit -t を実行します。

Terminal

アクセス元がホストに接続するのに使用した端末名を識別します。

Program

イベントをトリガしたプログラム名を識別します。これは、ログイン試行にアクセサが使用したプログラムです。CA Access Control 管理ログインでは、ログインした CA Access Control モジュールを指します（selang、Web サービスなど）。

監査フラグ

アクセス元が内部ユーザ（CA Access Control データベース ユーザ）であるかまたはエンタープライズ ユーザであるかを示します。

注: アクセス元がエンタープライズ ユーザである場合、seaudit の詳細でない出力では、監査レコードのこのフィールドに「(OS user)」の文字列が表示されます。エンタープライズ ユーザではない場合、このフィールドは空白です。

例:ログイン イベント メッセージ

以下の監査レコードは、seaudit の詳細出力から取得したものです。

```
28 Oct 2008 12:15:01 P LOGIN  root  49047159:0000034b  59  2  _CRONJOB_  SBIN_CRON
Event type: Login event
Status: Permitted
User name: root
Terminal: _CRONJOB_
Program: SBIN_CRON
Date: 28 Oct 2008
Time: 12:15
Details: Resource UACC check
User Logon Session ID: 49047159:0000034b
Audit flags: AC database user
```

この監査レコードは、2008 年 10 月 28 日、12 時 15 分 01 秒に、保護されたホストに root ユーザが _CRONJOB_ 端末からログインし、SBIN_CRON プログラムを実行したことを示しています。リソースのデフォルトのアクセス許可で、このアクションが許可されているため、CA Access Control は操作を許可しました(承認 stage code 59 - リソース UACC のチェック)。アクセサの監査モードでこのイベントをログに記録することが指定されているため、CA Access Control はこのイベントをログに記録しました(reason code 2 - ユーザ監査モードは、ログ記録を必要とします)。

詳細情報:

ログインおよびログアウト イベントの承認 stage code (P. 687)
レコードを作成した理由を示す理由コード (P. 725)

ログアウト イベント

UNIX に該当

ログアウト イベントは CA Access Control または CA Access Control で保護されるホストからのログアウト試行を示しています。

注: ログアウト イベントは UNIX でのみサポートされます。CA Access Control は実際にログアウトをインターセプトするわけではありません。その代わりに、セッションの最後のプロセスが終了するときにログアウトが発生すると想定します。

このイベントの監査レコードは、以下の形式になります。

Date Time Status Event UserName SessionID Details Reason Terminal AuditFlags

Date

イベントが発生した日付を識別します。

形式: DD MMM YYYY

注: CA Access Control エンドポイント管理 は日付の表示をコンピュータの設定に従って整形します。

Time

イベントが発生した時間を識別します。

形式: HH:MM:SS

注: CA Access Control エンドポイント管理 は時間の表示をコンピュータの設定に従って整形します。

ステータス

ユーザ ログアウトが発生したことを示します。

値: O (ログアウト)

イベント タイプ

このレコードが属するイベントのタイプを識別します。

注: CA Access Control エンドポイント管理 はこのフィールドを単にイベントとして参照します。

ユーザ名

このイベントをトリガしたアクションを実行したアクセス元の名前を識別します。

User Logon Session ID

アクセス元のセッション ID を識別します。

注: デフォルトでは、このフィールドは seaudit の詳細でない出力には表示されません。seaudit の詳細でない出力でこのフィールドを表示するには、seaudit コマンドに -sessionid オプションを指定します。

詳細

ログアウトの検出方法を示します。

詳細

CA Access Control がこのイベントに対して実行するアクションを決定したステージを示します。

注: seaudit の詳細でない出力では、監査レコードのこのフィールドに数字が表示されます。この数字は承認 stage code といいます。詳細な出力または CA Access Control エンドポイント管理 では、監査レコードに承認 stage code に関連するメッセージが表示されます。すべての stage code を一覧表示するには、seaudit -t を実行します。

Reason

CA Access Control が監査レコードを書き込んだ理由を示します。

注: このフィールドは seaudit の詳細な出力または CA Access Control エンドポイント管理 には表示されません。seaudit の詳細でない出力では、監査レコードのこのフィールドに数字が表示されます。この数字は理由コードといいます。すべての理由コードを一覧表示するには、seaudit -t を実行します。

Terminal

アクセス元がホストに接続するのに使用した端末名を識別します。

監査フラグ

アクセス元が内部ユーザ（CA Access Control データベース ユーザ）であるかまたはエンタープライズ ユーザであるかを示します。

注: アクセス元がエンタープライズ ユーザである場合、seaudit の詳細でない出力では、監査レコードのこのフィールドに「(OS user)」の文字列が表示されます。エンタープライズ ユーザではない場合、このフィールドは空白です。

例: ログアウト イベント メッセージ

以下の監査レコードは、seaudit の詳細出力から取得したものです。

```
29 Jan 2009 17:23:33 0 LOGOUT       root                  49  2 computer.com
Event type: Logout
Status: Logout
User name: root
Terminal: computer.com
Date: 29 Jan 2009
Time: 17:23
Details: Logout detected after last process terminated
Audit flags: AC database user
```

この監査レコードは、2009 年 1 月 29 日に、CA Access Control がリモート端末 computer.com で作業中のユーザ root の最後のセッション プロセスが終了したことを検知し、それによりユーザがシステムからログアウトしたと想定したことを示します(承認 stage code 49 - 最後のプロセスの終了後にログアウトを検知しました)。

詳細情報:

ログインおよびログアウト イベントの承認 stage code (P. 687)
レコードを作成した理由を示す理由コード (P. 725)

ログイン アカウントの有効化イベント

UNIX で該当

ログイン アカウントの有効化イベントは、serevu がユーザのログインを有効化するイベントを示しています。

このイベントの監査レコードは、以下の形式になります。

Date Time Status Event UserName Details Reason Terminal Program AuditFlags

Date

イベントが発生した日付を識別します。

形式: DD MMM YYYY

注: CA Access Control エンドポイント管理 は日付の表示をコンピュータの設定に従って整形します。

Time

イベントが発生した時間を識別します。

形式: HH:MM:SS

注: CA Access Control エンドポイント管理 は時間の表示をコンピュータの設定に従って整形します。

ステータス

serevu がユーザのログインを有効化したことを示します。

値: E (ログインが有効になりました)

イベント タイプ

このレコードが属するイベントのタイプを識別します。

注: CA Access Control エンドポイント管理 はこのフィールドを単にイベントとして参照します。

ユーザ名

このイベントをトリガしたアクションを実行したアクセス元の名前を識別します。

詳細

CA Access Control がこのイベントに対して実行するアクションを決定したステージを示します。

注: seaudit の詳細でない出力では、監査レコードのこのフィールドに数字が表示されます。この数字は承認 stage code といいます。詳細な出力または CA Access Control エンドポイント管理 では、監査レコードに承認 stage code に関連するメッセージが表示されます。すべての stage code を一覧表示するには、seaudit -t を実行します。

Reason

CA Access Control が監査レコードを書き込んだ理由を示します。

注: このフィールドは seaudit の詳細な出力または CA Access Control エンドポイント管理 には表示されません。seaudit の詳細でない出力では、監査レコードのこのフィールドに数字が表示されます。この数字は理由コードといいます。すべての理由コードを一覧表示するには、seaudit -t を実行します。

Terminal

アクセス元がホストに接続するのに使用した端末名を識別します。

Program

イベントをトリガしたプログラム名を識別します。

監査フラグ

アクセス元が内部ユーザ（CA Access Control データベース ユーザ）であるかまたはエンタープライズ ユーザであるかを示します。

注: アクセス元がエンタープライズ ユーザである場合、seaudit の詳細でない出力では、監査レコードのこのフィールドに「(OS user)」の文字列が表示されます。エンタープライズ ユーザではない場合、このフィールドは空白です。

例: ログイン アカウントの有効化イベント メッセージ

以下の監査レコードは、seaudit の詳細出力から取得したものです。

```
13 Jan 2009 17:05:00 E LOGINENABLE  test1          0  5 computer.com      serevu
Event type: Login account enabled
Status: Login enabled
User name: test1
Details: Stage code 0
Terminal: computer.com
```

```
Date: 13 Jan 2009
Time: 17:05
Program: serevu
Audit flags: AC database userLogin account disable –
```

この監査レコードは、2009 年 1 月 13 日に serevu デーモンがユーザ test1 の端末 computer.com からのログインを有効化したことを示します。serevu デーモンが監査を要求したので、CA Access Control はこのイベントをログに記録しました（理由コード 5 - CA Access Control serevu ユーティリティが監査を要求しました）。

詳細情報:

ログインおよびログアウト イベントの承認 stage code (P. 687)
レコードを作成した理由を示す理由コード (P. 725)

ログイン アカウントの無効化イベント

UNIX で該当

ログイン アカウントの無効化イベントは、serevu がユーザのログインを無効化するイベントを示しています。

このイベントの監査レコードは、以下の形式になります。

Date Time Status Event UserName Details Reason Terminal Program AuditFlags

Date

イベントが発生した日付を識別します。

形式: DD MMM YYYY

注: CA Access Control エンドポイント管理 は日付の表示をコンピュータの設定に従って整形します。

Time

イベントが発生した時間を識別します。

形式: HH:MM:SS

注: CA Access Control エンドポイント管理 は時間の表示をコンピュータの設定に従って整形します。

ステータス

serevu がユーザのログインを無効化したことを示します。

値: I (ログインが無効になりました)

イベント タイプ

このレコードが属するイベントのタイプを識別します。

注: CA Access Control エンドポイント管理 はこのフィールドを単にイベントとして参照します。

ユーザ名

このイベントをトリガしたアクションを実行したアクセス元の名前を識別します。

User Logon Session ID

アクセス元のセッション ID を識別します。

注: デフォルトでは、このフィールドは seaudit の詳細でない出力には表示されません。seaudit の詳細でない出力でこのフィールドを表示するには、seaudit コマンドに -sessionid オプションを指定します。

詳細

CA Access Control がこのイベントに対して実行するアクションを決定したステージを示します。

注: seaudit の詳細でない出力では、監査レコードのこのフィールドに数字が表示されます。この数字は承認 stage code といいます。詳細な出力または CA Access Control エンドポイント管理 では、監査レコードに承認 stage code に関連するメッセージが表示されます。すべての stage code を一覧表示するには、seaudit -t を実行します。

Reason

CA Access Control が監査レコードを書き込んだ理由を示します。

注: このフィールドは seaudit の詳細な出力または CA Access Control エンドポイント管理 には表示されません。seaudit の詳細でない出力では、監査レコードのこのフィールドに数字が表示されます。この数字は理由コードといいます。すべての理由コードを一覧表示するには、seaudit -t を実行します。

Terminal

アクセス元がホストに接続するのに使用した端末名を識別します。

Program

イベントをトリガしたプログラム名を識別します。

監査フラグ

アクセス元が内部ユーザ(CA Access Control データベース ユーザ)であるかまたはエンタープライズ ユーザであるかを示します。

注: アクセス元がエンタープライズ ユーザである場合、seaudit の詳細でない出力では、監査レコードのこのフィールドに「(OS user)」の文字列が表示されます。エンタープライズ ユーザではない場合、このフィールドは空白です。

例: ログイン アカウントの無効化イベント メッセージ

以下の監査レコードは、seaudit の詳細出力から取得したものです。

```
13 Jan 2009 16:53:26 I LOGINDISABLE test1                    0  5
computer.com      serevu
Event type: Login account disable
Status: Login disabled
User name: test1
Terminal: computer.com
Date: 13 Jan 2009
Time: 16:53
Program: serevu
Details: Stage code 0
User Logon Session ID: 496b629c:00000003
Audit flags: AC database user
```

この監査レコードは、2009 年 1 月 13 日に serevu デーモンがユーザ test1 の端末 computer.com からのログインを禁止したことを示します。serevu デーモンが監査を要求したので、CA Access Control はこのイベントをログに記録しました(理由コード 5 - CA Access Control serevu ユーティリティが監査を要求しました)。

詳細情報:

ログインおよびログアウト イベントの承認 stage code (P. 687)
レコードを作成した理由を示す理由コード (P. 725)

パスワード試行イベント

UNIX で該当

パスワード試行イベントはアクセス元が不正なパスワードでログインしようとしたことを示しています。

このイベントの監査レコードは、以下の形式になります。

Date Time Status Event UserName Details Reason Terminal Program AuditFlags

Date

イベントが発生した日付を識別します。

形式: DD MMM YYYY

注: CA Access Control エンドポイント管理 は日付の表示をコンピュータの設定に従って整形します。

Time

イベントが発生した時間を識別します。

形式: HH:MM:SS

注: CA Access Control エンドポイント管理 は時間の表示をコンピュータの設定に従って整形します。

ステータス

不正なパスワード試行を示します。

値: A (パスワード試行)

イベント タイプ

このレコードが属するイベントのタイプを識別します。

注: CA Access Control エンドポイント管理 はこのフィールドを単にイベントとして参照します。

ユーザ名

このイベントをトリガしたアクションを実行したアクセス元の名前を識別します。

詳細

CA Access Control がこのイベントに対して実行するアクションを決定したステージを示します。

注: seaudit の詳細でない出力では、監査レコードのこのフィールドに数字が表示されます。この数字は承認 stage code といいます。詳細な出力または CA Access Control エンドポイント管理 では、監査レコードに承認 stage code に関連するメッセージが表示されます。すべての stage code を一覧表示するには、seaudit -t を実行します。

Reason

CA Access Control が監査レコードを書き込んだ理由を示します。

注: このフィールドは seaudit の詳細な出力または CA Access Control エンドポイント管理 には表示されません。seaudit の詳細でない出力では、監査レコードのこのフィールドに数字が表示されます。この数字は理由コードといいます。すべての理由コードを一覧表示するには、seaudit -t を実行します。

Terminal

アクセス元がホストに接続するのに使用した端末名を識別します。

Program

イベントをトリガしたプログラム名を識別します。

監査フラグ

アクセス元が内部ユーザ（CA Access Control データベース ユーザ）であるかまたはエンタープライズ ユーザであるかを示します。

注: アクセス元がエンタープライズ ユーザである場合、seaudit の詳細でない出力では、監査レコードのこのフィールドに「(OS user)」の文字列が表示されます。エンタープライズ ユーザではない場合、このフィールドは空白です。

例: パスワード試行イベント メッセージ

以下の監査レコードは、seaudit の詳細出力から取得したものです。

```
13 Jan 2009 16:21:12 A LOGIN        admin                 17  8
localhost.localdomain login
Event type: Password attempt
Status: Password attempt
User name: admin
Terminal: localhost.localdomain
Date: 13 Jan 2009
```

```
Time: 16:21
Program: login
Details: Attempt rejected by the native environment
Audit flags: AC database user
```

この監査レコードは、2009 年 1 月 13 日にユーザ admin がアカウントのパスワードを変更しようとしたことを示します。この試行はログイン エラーのためネイティブ環境により拒否されました(承認 stage code 17 - 試行はネイティブ環境により拒否されました)。pam _seos モジュールがこのイベントをログに記録しました(理由コード 8 - CA Access Control pam サポート UNIX がログインに失敗しました)。

詳細情報:

ログインおよびログアウト イベントの承認 stage code (P. 687)
レコードを作成した理由を示す理由コード (P. 725)

リソース アクセス イベント

リソース アクセス イベントは FILE、TERMINAL、PROGRAM などのリソースへのアクセス試行を示しています。このイベントの監査レコードのデータは、アクセス元が TERMINAL リソースへのアクセスを試行するときに、LOGIN イベントなどのほかのレコードにも表示させることができます。この場合のイベント レコードは LOGIN タイプですが、レコードに表示される監査レコードのデータは、リソース アクセス イベント メッセージのうちのいずれかです。

このイベントの監査レコードは、以下の形式になります。

Date Time Status Class UserName SessionID Access Details Reason Resource Program Terminal EffectiveUserName AuditFlags

Date

イベントが発生した日付を識別します。

形式: DD MMM YYYY

注: CA Access Control エンドポイント管理 は日付の表示をコンピュータの設定に従って整形します。

Time

イベントが発生した時間を識別します。

形式: HH:MM:SS

注: CA Access Control エンドポイント管理 は時間の表示をコンピュータの設定に従って整形します。

ステータス

イベントのリターン コードを示します。

値: 以下のいずれかです。

- D（拒否）- 権限が不十分なためイベントが拒否されました。
- P（許可）- イベントが許可されました。
- W（警告）- アクセス要求はアクセス ルールに違反していますが警告モードが設定されたためイベントが許可されました。

クラス

アクセスされているリソースが属するクラスを識別します。

ユーザ名

このイベントをトリガしたアクションを実行したアクセス元の名前を識別します。

User Logon Session ID

アクセス元のセッション ID を識別します。

注: デフォルトでは、このフィールドは seaudit の詳細でない出力には表示されません。seaudit の詳細でない出力でこのフィールドを表示するには、seaudit コマンドに -sessionid オプションを指定します。

アクセス

このイベントをトリガしたアクセス試行のタイプを識別します。

例: 読み取り

注: アクセスの値は、インターセプトされたリソースが属するクラスによって異なります。各クラスに対するアクセス権限の詳細については、「selang リファレンス ガイド」*を参照してください*。

詳細

CA Access Control がこのイベントに対して実行するアクションを決定したステージを示します。

注: seaudit の詳細でない出力では、監査レコードのこのフィールドに数字が表示されます。この数字は承認 stage code といいます。詳細な出力または CA Access Control エンドポイント管理 では、監査レコードに承認 stage code に関連するメッセージが表示されます。すべての stage code を一覧表示するには、seaudit -t を実行します。

Reason

CA Access Control が監査レコードを書き込んだ理由を示します。

注: このフィールドは seaudit の詳細な出力または CA Access Control エンドポイント管理 には表示されません。seaudit の詳細でない出力では、監査レコードのこのフィールドに数字が表示されます。この数字は理由コードといいます。すべての理由コードを一覧表示するには、seaudit -t を実行します。

Resource

アクセスまたは更新されている実際のリソースの名前を識別します。

Program

イベントをトリガしたプログラム名を識別します。これは、アクセス元がリソースへのアクセス試行に使用するプログラムです

Terminal

アクセス元がホストに接続するのに使用した端末名を識別します。(UNIX のみ)。

有効なユーザ名

(UNIX のみ)このイベントをトリガしたネイティブな OS の有効なユーザ名を識別します。ユーザが別のユーザを代行する(代理になる)または setuid プログラムを実行する場合、この名前はユーザ名とは異なります。

注: このフィールドは KBL 監査出力には表示されません。

監査フラグ

アクセス元が内部ユーザ(CA Access Control データベース ユーザ)であるかまたはエンタープライズ ユーザであるかを示します。

注: アクセス元がエンタープライズ ユーザである場合、seaudit の詳細でない出力では、監査レコードのこのフィールドに「(OS user)」の文字列が表示されます。エンタープライズ ユーザではない場合、このフィールドは空白です。

例: リソース アクセス イベント メッセージ

以下の監査レコードは、seaudit の詳細出力から取得したものです。

```
18 Nov 2008 15:23:56 D FILE       admabc  4922ae61:00000132 Read      69  3 /tmp/one
/usr/local/bin/tcsh  localhost      admabc
Event type: Resource access
Status: Denied
Class: FILE
Resource: /tmp/one
Access: Read
User name: admabc
Terminal: localhost
Program: /usr/local/bin/tcsh
Date: 18 Nov 2008
Time: 15:23
Details: No Step that allowed access
User Logon Session ID: 4922ae61:00000132
Audit flags: AC database user
Effective user name: admabc
```

この監査レコードは 2008 年 11 月 18 日 15:23:56 に、ユーザ admabc がローカル コンピュータから UNIX tcsh シェル プログラムを使用して、保護された /tmp/one ファイル リソースを読み取ろうとしたことを示します。このタイプのアクセスを許可するルールがデータベースに存在しないため、CA Access Control は操作を拒否しました(承認 stage code 69 - アクセスを許可したステップがありません)。リソースの監査モードでこのイベントはログに記録する必要があると指定しているため、CA Access Control はこのイベントをログに記録しました(理由コード 3 - リソース監査モードはログへの記録を要求しました)。

詳細情報:

リソース アクセス イベントの承認 stage code (P. 690)
レコードを作成した理由を示す理由コード (P. 725)

アントラスト メッセージ イベント

アントラスト イベントは CA Access Control Watchdog がイベントのたびに生成する警告メッセージを示します。

このイベントの監査レコードは、以下の形式になります。

Date Time Status Class Module Details MessageID/errno File

Date

イベントが発生した日付を識別します。

形式: DD MMM YYYY

注: CA Access Control エンドポイント管理 は日付の表示をコンピュータの設定に従って整形します。

Time

イベントが発生した時間を識別します。

形式: HH:MM:SS

注: CA Access Control エンドポイント管理 は時間の表示をコンピュータの設定に従って整形します。

ステータス

アントラストが発生したことを示します。

値: U (アントラスト)

クラス

watchdog メッセージをトリガしたリソースが属する CA Access Control クラスを識別します。

値: PROGRAM または SECFILE

Module Name

CA Access Control Watchdog の名前が表示されます。

値: seoswd

詳細

アントラスト イベントが発生した理由を示します。

注: seaudit の詳細でない出力では、監査レコードのこのフィールドに数字が表示されます。この数字はアントラスト理由コードといいます。詳細な出力または CA Access Control エンドポイント管理 では、監査レコードにアントラスト理由コードに関連するメッセージが表示されます。すべてのパスワード品質コードを一覧表示するには、seaudit -t を実行します。

メッセージ ID

(UNIX のみ) CA Access Control が PROGRAM または SECFILE を信頼できない理由を示します。

注: seaudit の詳細でない出力では、監査レコードのこのフィールドに数字が表示されます。この数字はステータス コードといい、詳細な出力または CA Access Control エンドポイント管理 では表示されません。ステータス コードの意味を知るには、seaudit -Stat *untrust_code* を実行します。このフィールドは承認 stage code が 1 の場合にのみ表示されます。そのほかの場合は、代わりにエラー番号フィールドが表示されます。

errno

errno 変数（エラー状態に対するエラー コード）の戻り値を示します。

値: 以下のいずれかです。

0 - エラーはありません。この値は承認 stage code が 1 の場合にのみ返されます。この場合、エラー番号フィールドは表示されず、代わりにメッセージ ID フィールドが表示されます。

errno - エラーであるゼロ以外の整数です。

注: UNIX でエラーの意味を調べるには、ローカル コンピュータの /usr/include/errno.h ファイルまたは /usr/include/sys/errno.h ファイルを参照してください。Windows では、ローカル コンピュータで次のコマンドを入力します。net helpmsg *errno*

ファイル

Watchdog メッセージをトリガした保護されたリソースのフル パス名を識別します。

例: アントラスト メッセージ イベント メッセージ

以下の監査レコードは、seaudit の詳細出力から取得したものです。

```
18 Nov 2008 14:01:18 U PROGRAM      seoswd                  1 11776 /tmp/testsuid
Event type: Untrust message
Class: PROGRAM
Module name: seoswd
Message ID: 11776
Date: 18 Nov 2008
Time: 14:01
File: /tmp/testsuid
Details: Stat information changed on file system
Audit flags: AC database user
```

この監査レコードは、2008 年 11 月 15 日に Watchdog によって、プログラム /tmp/testsuid が untrusted（U）としてマークされたことを示します。このプログラムはステータス情報が変更されているために信頼できませんでした（アントラスト理由コード 1 - ファイル情報がファイルシステムで変更されました）。

例：seaudit -Stat を使用してプログラムが信頼できなかった理由を表示（UNIX）

以下の seaudit -Stat 出力には、監査レコードが記述する Watchdog メッセージ ID に関するより詳細な情報を取得する方法が示されます。

```
# seaudit -Stat 11776
CA Access Control seaudit v12.01.00.45 - Audit log lister
Copyright (c) 2008 CA. All rights reserved.

The MODE of the file was changed
The INODE of the file was changed
The SIZE of the file was changed
The MTIME of the file was changed
```

メッセージ ID を指定して seaduit -Stat コマンドを実行すると、ファイルに対する変更が一覧表示されます。この例では、ファイルの MODE、INODE、SIZE、および MTIME が変更されています。結果として、CA Access Control はこのファイルを untrusted ファイルとしてマークしました。

詳細情報:

アントラスト メッセージ イベントの承認 stage code (P. 701)
レコードを作成した理由を示す理由コード (P. 725)

受信ネットワーク接続イベント

受信ネットワーク接続イベントは、保護されたホストへの受信トラフィックを示します。受信ネットワーク イベントは 2 つの形式で監査されます（ローカル データベースのクラスのアクティブ化に従う）。どちらの監査イベント タイプにも同じ情報が含まれますが表示方法が異なります。たとえば、片方の監査イベントには HOST がクラス名として含まれますが、もう一方には TCP がクラス名として表示されます。

このイベントの監査レコードは、以下の形式になります。

Date Time Status Event Service Details Reason Host Program

Date

イベントが発生した日付を識別します。

形式: DD MMM YYYY

注: CA Access Control エンドポイント管理 は日付の表示をコンピュータの設定に従って整形します。

Time

イベントが発生した時間を識別します。

形式: HH:MM:SS

注: CA Access Control エンドポイント管理 は時間の表示をコンピュータの設定に従って整形します。

ステータス

イベントのリターン コードを示します。

値: 以下のいずれかです。

- D（拒否）- 権限が不十分なためイベントが拒否されました。
- P（許可）- イベントが許可されました。
- W（警告）- アクセス要求はアクセス ルールに違反していますが警告モードが設定されたためイベントが許可されました。

イベント タイプ

このレコードが属するイベントのタイプを識別します。

注: CA Access Control エンドポイント管理 はこのフィールドを単にイベントとして参照します。

サービス

接続が使用されるサービスの名前を識別します。

詳細

CA Access Control がこのイベントに対して実行するアクションを決定したステージを示します。

注: seaudit の詳細でない出力では、監査レコードのこのフィールドに数字が表示されます。この数字は承認 stage code といいます。詳細な出力または CA Access Control エンドポイント管理 では、監査レコードに承認 stage code に関連するメッセージが表示されます。すべての stage code を一覧表示するには、seaudit -t を実行します。

Reason

CA Access Control が監査レコードを書き込んだ理由を示します。

注: このフィールドは seaudit の詳細な出力または CA Access Control エンドポイント管理 には表示されません。seaudit の詳細でない出力では、監査レコードのこのフィールドに数字が表示されます。この数字は理由コードといいます。すべての理由コードを一覧表示するには、seaudit -t を実行します。

ホスト名

ネットワークトラフィックの送信元のホスト名を示します。

Program

(UNIX のみ)アクセサが実行しようとしているプログラム名を示します。

例: 受信ネットワーク接続イベントのメッセージ

以下の監査レコードは、seaudit の詳細出力から取得したものです。

```
17 Nov 2008 12:22:04 D HOST         telnet              173  3 computer.org.com
/usr/sbin/inetd
Event type: Inbound network connection
Status: Denied
Host name: computer.org.com
Service: telnet
Program: /usr/sbin/inetd/
Date: 17 Nov 2008
Time: 12:22
Details: HOST entry day & time restrictions
Audit flags: AC database user
```

この監査レコードは、2008 年 11 月 17 日に、telnet サービスを使用してホスト computer.org.com にアクセスして inetd プログラムを実行しようとしたアクセサが、保護されたホストに適用される日時の制限のために拒否されたことを示します（承認 stage code 173 - HOST エントリの日時の制限）。リソースの監査モードでこのイベントはログに記録する必要があると指定しているため、CA Access Control はこのイベントをログに記録しました（理由コード 3 - リソース監査モードはログへの記録を要求しました）。

詳細情報:

受信ネットワーク接続イベントの承認 stage code (P. 703)
レコードを作成した理由を示す理由コード (P. 725)

送信ネットワーク接続イベント

送信ネットワーク接続イベントは、保護されたホストへの送信トラフィックを示します。送信ネットワーク イベントはローカル データベースでのクラスのアクティブ化により 2 つの形式で監査されます。どちらの監査イベント タイプにも同じ情報が含まれますが表示方法が異なります。たとえば、片方の監査イベントには HOST がクラス名として含まれますが、もう一方には TCP がクラス名として表示されます。

このイベントの監査レコードは、以下の形式になります。

Date Time Status Class Service UserName Details Reason Host Program Terminal AuditFlags

Date

イベントが発生した日付を識別します。

形式: DD MMM YYYY

注: CA Access Control エンドポイント管理 は日付の表示をコンピュータの設定に従って整形します。

Time

イベントが発生した時間を識別します。

形式: HH:MM:SS

注: CA Access Control エンドポイント管理 は時間の表示をコンピュータの設定に従って整形します。

ステータス

イベントのリターン コードを示します。

値: 以下のいずれかです。

- D（拒否）- 権限が不十分なためイベントが拒否されました。
- P（許可）- イベントが許可されました。
- W（警告）- アクセス要求はアクセス ルールに違反していますが警告モードが設定されたためイベントが許可されました。

クラス

クラスの名前を識別します。

サービス

接続が使用されるサービスの名前を識別します。

ユーザ名

このイベントをトリガしたアクションを実行したアクセス元の名前を識別します。

詳細

CA Access Control がこのイベントに対して実行するアクションを決定したステージを示します。

注: seaudit の詳細でない出力では、監査レコードのこのフィールドに数字が表示されます。この数字は承認 stage code といいます。詳細な出力または CA Access Control エンドポイント管理 では、監査レコードに承認 stage code に関連するメッセージが表示されます。すべての stage code を一覧表示するには、seaudit -t を実行します。

Reason

CA Access Control が監査レコードを書き込んだ理由を示します。

注: このフィールドは seaudit の詳細な出力または CA Access Control エンドポイント管理 には表示されません。seaudit の詳細でない出力では、監査レコードのこのフィールドに数字が表示されます。この数字は理由コードといいます。すべての理由コードを一覧表示するには、seaudit -t を実行します。

ホスト名

ターゲット ホストの名前を識別します。

Program

イベントをトリガしたプログラム名を識別します。

Terminal

アクセス元がホストに接続するのに使用した端末名を識別します。

User Logon Session ID

アクセス元のセッション ID を識別します。

注: デフォルトでは、このフィールドは seaudit の詳細でない出力には表示されません。seaudit の詳細でない出力でこのフィールドを表示するには、seaudit コマンドに -sessionid オプションを指定します。ユーザ ログオン セッション ID フィールドは、TCP または CONNECT クラス定義の結果として生成されたイベントに対してのみ追加されます。

監査フラグ

アクセス元が内部ユーザ(CA Access Control データベース ユーザ)であるかまたはエンタープライズ ユーザであるかを示します。

注: アクセス元がエンタープライズ ユーザである場合、seaudit の詳細でない出力では、監査レコードのこのフィールドに「(OS user)」の文字列が表示されます。エンタープライズ ユーザではない場合、このフィールドは空白です。

例: 送信ネットワーク接続イベント メッセージ

以下の監査レコードは、seaudit の詳細出力から取得したものです。

```
21 Jan 2009 15:37:43 D TCP      telnet    root    408  2 computer.org /usr/bin/telnet
computer.com
Event type: Outbound network connection
Status: Denied
Host name: computer.org
Service: telnet
Program: /usr/bin/telnet
User name: Administrator
Terminal: computer.com
User name: root
Date: 21 Jan 2009
Time: 15:37:43
Details: Default access of TCP service
User Logon Session ID: 4977248c:0000012a5248
Audit flags: AC database user
```

この監査レコードは、2009 年 1 月 21 日に管理者が端末 computer.org からコンピュータ computer.com に telnet サービス経由で外部接続を開いたことを示します。CA Access Control はこの操作を TCP レコードの defaccess プロパティにより拒否しました。(承認 stage code 408 - TCP サービスのデフォルト) CA Access Control はアクセス元の AUDIT_MODE プロパティがレコードの結果と一致したために、このイベントをログに記録しました。(理由コード 2 - ユーザ監査モードはログへの記録を要求します)

詳細情報:

送信ネットワーク接続イベントの承認 stage code (P. 708)
レコードを作成した理由を示す理由コード (P. 725)

セキュリティ データベース管理イベント

セキュリティ データベース管理イベントは、適切な権限を持つ CA Access Control 管理者またはサブ管理者が実行し、CA Access Control がインターセプトしたアクションを示します。

このイベントの監査レコードは、以下の形式になります。

Date Time Status Event Class Admin Details Reason Object Terminal Command AuditFlags

Date

イベントが発生した日付を識別します。

形式: DD MMM YYYY

注: CA Access Control エンドポイント管理 は日付の表示をコンピュータの設定に従って整形します。

Time

イベントが発生した時間を識別します。

形式: HH:MM:SS

注: CA Access Control エンドポイント管理 は時間の表示をコンピュータの設定に従って整形します。

ステータス

イベントのリターン コードを示します。

値: 以下のいずれかです。

- D（拒否）- 権限が不十分なためイベントが拒否されました。
- S（成功）- イベントが許可されました。
- F（失敗）- イベントが失敗しました。

イベント タイプ

このレコードが属するイベントのタイプを識別します。

注: CA Access Control エンドポイント管理 はこのフィールドを単にイベントとして参照します。

クラス

管理対象のリソースが属するクラスを特定します。

管理者

selang コマンドを実行した管理者ユーザの名前を特定します。

詳細

CA Access Control がこのイベントに対して実行するアクションを決定したステージを示します。

注: seaudit の詳細でない出力では、監査レコードのこのフィールドに数字が表示されます。この数字は承認 stage code といいます。詳細な出力または CA Access Control エンドポイント管理 では、監査レコードに承認 stage code に関連するメッセージが表示されます。すべての stage code を一覧表示するには、seaudit -t を実行します。

Reason

CA Access Control が監査レコードを書き込んだ理由を示します。

注: このフィールドは seaudit の詳細な出力または CA Access Control エンドポイント管理 には表示されません。seaudit の詳細でない出力では、監査レコードのこのフィールドに数字が表示されます。この数字は理由コードといいます。すべての理由コードを一覧表示するには、seaudit -t を実行します。

オブジェクト

管理されているリソースの名前を示します。

Terminal

アクセス元がホストに接続するのに使用した端末名を識別します。

注: コマンドが親ポリシー モデルから引き継がれている場合、このフィールドには PMD の完全修飾名が表示されます。

コマンド

ユーザが実行した selang コマンドが表示されます。

監査フラグ

アクセス元が内部ユーザ(CA Access Control データベース ユーザ)であるかまたはエンタープライズ ユーザであるかを示します。

注: アクセス元がエンタープライズ ユーザである場合、seaudit の詳細でない出力では、監査レコードのこのフィールドに「(OS user)」の文字列が表示されます。エンタープライズ ユーザではない場合、このフィールドは空白です。

コマンド タイプ

このイベントが示すデータベース管理コマンドのタイプを識別します。

値は以下のいずれかです。

- **ユーザの追加** - newusr コマンド用
- **グループの追加** - newgrp コマンド用
- **リソースの追加** - newres または newfile コマンド用
- **ユーザの変更** - chusr コマンド用
- **グループの変更** - chgrp コマンド用
- **グループ メンバシップの変更** - join コマンド用
- **リソースの変更** - chres コマンド用
- **リソース アクセスの変更** - authorize コマンド用
- **ユーザの削除** - rmusr コマンド用
- **グループの削除** - rmgrp コマンド用
- **リソースの削除** - rmres または rmfile コマンド用
- **オプションの設定** - setoptions コマンド用
- **ユーザの追加/変更** - editusr コマンド用
- **グループの追加/変更** - editgrp コマンド用

- **リソースの追加/変更** - editres または editfile コマンド用
- **管理コマンド** - そのほかのコマンド用

例: セキュリティデータベース管理イベントのメッセージ

以下の監査レコードは、seaudit の詳細出力から取得したものです。

```
05 Nov 2008 15:45:12 S UPDATE       FILE       DOMAIN_NAME¥computer 305  0 dfdok
computer.com cr file dfdok defacc(r)
Event type: Security database administration
Command type: Modify resource
Status: Successful
Administrator: DOMAIN_NAME¥computer
Class: FILE
Object: dfdok
Terminal: computer.com
Date: 05 Nov 2008
Time: 15:45
Details: Command successful for ADMIN user.
Command: cr file dfdok defacc(r)
Audit flags: AC database user
```

この監査レコードは、2008 年 11 月 5 日、端末 computer.com からログインして、保護されたホスト上でコマンド cr file dfdok defacc(r) を実行してファイルを更新しようとした管理者からのアクセスを、CA Access Control が拒否したことを示します(承認 stage code 305 - コマンドが管理者ユーザに許可されました)。

詳細情報:

セキュリティ データベース管理イベントの承認 stage code (P. 712)
レコードを作成した理由を示す理由コード (P. 725)

スタートアップ イベント

CA Access Control スタートアップ イベントは、CA Access Control のサービス（Windows）またはデーモン（UNIX）のスタートアップ シーケンスを示します。

このイベントの監査レコードは、以下の形式になります。

Date Time M *Event Service*

Date

イベントが発生した日付を識別します。

形式： DD MMM YYYY

注： CA Access Control エンドポイント管理 は日付の表示をコンピュータの設定に従って整形します。

Time

イベントが発生した時間を識別します。

形式： HH:MM:SS

注： CA Access Control エンドポイント管理 は時間の表示をコンピュータの設定に従って整形します。

イベント タイプ

このレコードが属するイベントのタイプを識別します。

注： CA Access Control エンドポイント管理 はこのフィールドを単にイベントとして参照します。

サービス

seosd - CA Access Control のメイン デーモンまたはサービス。seosd デーモンまたはサービスは、CA Access Control のスタートアップおよびシャットダウン シーケンスを制御します。

例：デーモンの起動イベントのメッセージ（UNIX）

以下の監査レコードは、seaudit の詳細出力から取得したものです。

```
02 Nov 2008 15:41:06 M START                                    seoswd
Event type: Daemon start
Daemon: seoswd
Date: 02 Nov 2008
```

```
Time: 15:41
Audit flags: AC database user
```

この監査レコードは seoswd Watchdog が 2008 年 11 月 2 日に起動されたことを示します。

例: エンジン サービス開始イベント メッセージ(Windows)

以下の監査レコードは、seaudit の詳細出力から取得したものです。

```
02 Nov 2008 15:34:48 M START                                    seosd
Event type: Engine service start
Engine service: seosd
Date: 02 Nov 2008
Time: 15:34
Audit flags: AC database user
```

この監査レコードは 2008 年 11 月 2 日に CA Access Control の開始を担当する seosd サービス エンジンが起動されたことを示します。

シャットダウン イベント

CA Access Control のシャットダウン イベントは、システムをシャットダウンする権限を持つ管理者またはサブ管理者ユーザが実行したプロセスを示します。

このイベントの監査レコードは、以下の形式になります。

Date Time M *Event UserName SessionID Details Service AuditFlags*

Date

イベントが発生した日付を識別します。

形式: DD MMM YYYY

注: CA Access Control エンドポイント管理 は日付の表示をコンピュータの設定に従って整形します。

Time

イベントが発生した時間を識別します。

形式: HH:MM:SS

注: CA Access Control エンドポイント管理 は時間の表示をコンピュータの設定に従って整形します。

イベント タイプ

このレコードが属するイベントのタイプを識別します。

注: CA Access Control エンドポイント管理 はこのフィールドを単にイベントとして参照します。

ユーザ名

このイベントをトリガしたアクションを実行したアクセス元の名前を識別します。

User Logon Session ID

アクセス元のセッション ID を識別します。

注: デフォルトでは、このフィールドは seaudit の詳細でない出力には表示されません。seaudit の詳細でない出力でこのフィールドを表示するには、seaudit コマンドに -sessionid オプションを指定します。

詳細

CA Access Control がこのイベントに対して実行するアクションを決定したステージを示します。

注: seaudit の詳細でない出力では、監査レコードのこのフィールドに数字が表示されます。この数字は承認 stage code といいます。詳細な出力または CA Access Control エンドポイント管理 では、監査レコードに承認 stage code に関連するメッセージが表示されます。すべての stage code を一覧表示するには、seaudit -t を実行します。

デーモン（UNIX）/エンジン サービス（Windows）

シャットダウンされた CA Access Control デーモン（UNIX）またはサービス（Windows）の名前を識別します。

値: seosd（CA Access Control エンジン）

監査フラグ

アクセス元が内部ユーザ（CA Access Control データベース ユーザ）であるかまたはエンタープライズ ユーザであるかを示します。

注: アクセス元がエンタープライズ ユーザである場合、seaudit の詳細でない出力では、監査レコードのこのフィールドに「(OS user)」の文字列が表示されます。エンタープライズ ユーザではない場合、このフィールドは空白です。

例: UNIX のシャットダウン イベント メッセージ

以下の監査レコードは、seaudit の詳細出力から取得したものです。

```
24 Sep 2008 15:40:46 M SHUTDOWN     root    452 seosd
Event type: Daemon shutdown
User name: root
Daemon: seosd
Date: 24 Sep 2008
Time: 15:40:46
Details: User is ADMIN or SPECIAL
User Logon Session ID: 48da26ce:00000142
Audit flags: CA Access Control database user
```

この監査レコードは、2008 年 9 月 24 日、CA Access Control をシャットダウンしようとしたユーザ root が、ADMIN 属性を持っているため、シャットダウンを許可されたことを示します(承認 stage code 452 - ユーザは ADMIN または SPECIAL です)。

例: Windows のシャットダウン イベント メッセージ

以下の監査レコードは、seaudit の詳細出力から取得したものです。

```
23 Dec 2008 12:56:20 D SHUTDOWN     tst002                  460 seosd
Event type: Engine service shutdown
User name: tst002
Engine service: seosd
Date: 10 Feb 2009
Time: 12:56
Details: User is not allowed to shutdown CA Access Control

User Logon Session ID: 00000000:04c240d5
Audit flags: AC database user
```

この監査レコードは、2008 年 12 月 23 日、ユーザ tst002 が CA Access Control のシャットダウンを許可されていないため、CA Access Control のシャットダウンが拒否されたことを示します(承認 stage code 460 - ユーザは CA Access Control をシャットダウンする権限がありません)。

詳細情報:

シャットダウン イベントの承認 stage code (P. 719)

パスワード確認イベント

パスワード確認イベント タイプ メッセージはユーザがアカウントのパスワードの変更に失敗したことを示します。

このイベントの監査レコードは、以下の形式になります。

Date Time Status Event UserName Details Reason AuditFlags

Date

イベントが発生した日付を識別します。

形式: DD MMM YYYY

注: CA Access Control エンドポイント管理 は日付の表示をコンピュータの設定に従って整形します。

Time

イベントが発生した時間を識別します。

形式: HH:MM:SS

注: CA Access Control エンドポイント管理 は時間の表示をコンピュータの設定に従って整形します。

ステータス

イベントのリターン コードを示します。

値: F (Failed) - アカウント パスワードの変更に失敗しました。

イベント タイプ

このレコードが属するイベントのタイプを識別します。

注: CA Access Control エンドポイント管理 はこのフィールドを単にイベントとして参照します。

ユーザ名

パスワード試行が適用されたユーザ名を識別します。

詳細

パスワード変更の試行が失敗した理由を示します。

注: seaudit の詳細でない出力では、監査レコードのこのフィールドに数字が表示されます。この数字はパスワード品質コードといいます。詳細な出力または CA Access Control エンドポイント管理 では、監査レコードにパスワード品質コードに関連するメッセージが表示されます。すべてのパスワード品質コードを一覧表示するには、seaudit -t を実行します。

Reason

CA Access Control が監査レコードを書き込んだ理由を示します。

注: このフィールドは seaudit の詳細な出力または CA Access Control エンドポイント管理 には表示されません。seaudit の詳細でない出力では、監査レコードのこのフィールドに数字が表示されます。この数字は理由コードといいます。すべての理由コードを一覧表示するには、seaudit -t を実行します。

監査フラグ

アクセス元が内部ユーザ(CA Access Control データベース ユーザ)であるかまたはエンタープライズ ユーザであるかを示します。

注: アクセス元がエンタープライズ ユーザである場合、seaudit の詳細でない出力では、監査レコードのこのフィールドに「(OS user)」の文字列が表示されます。エンタープライズ ユーザではない場合、このフィールドは空白です。

例: パスワード確認イベント メッセージ

以下の監査レコードは、seaudit の詳細出力から取得したものです。

```
02 Dec 2008 10:23:47 F PASSWORD     test1         1 10
Event type: Password verification
Status: Failed
User name: test1
Details: Password too short
Audit flags: AC database user
```

この監査レコードは、2008 年 12 月 2 日にユーザがアカウントのパスワードを変更しようとして、パスワード ポリシーに定義された必要最低文字数を満たしていなかったために拒否されたことを示します(承認 stage code 1 - パスワードが短すぎます)。CA Access Control は明示的な要求に従ってこのイベント メッセージをログに記録しました(理由コード 10 - 操作をログに記録する明示的な要求を受け取りました)。

詳細情報:

パスワード確認イベントの承認 Stage Code (P. 720)
レコードを作成した理由を示す理由コード (P. 725)

ユーザのトレース メッセージ

ユーザ イベントのトレース メッセージは、保護されたリソースを開く、実行する、または使用する試行を示しています。

Windows の場合、このイベントの監査レコードは、以下の形式になります。

Date Time Status Event UserName SessionID RealUID RealUsername Class Resource Details Trace AuditFlags

UNIX の場合、このイベントの監査レコードは、以下の形式になります。

Date Time Status Event UserName SessionID RealUsername EffectiveUsername Class Resource Details Trace AuditFlags

Date

イベントが発生した日付を識別します。

形式: DD MMM YYYY

注: CA Access Control エンドポイント管理 は日付の表示をコンピュータの設定に従って整形します。

Time

イベントが発生した時間を識別します。

形式: HH:MM:SS

注: CA Access Control エンドポイント管理 は時間の表示をコンピュータの設定に従って整形します。

ステータス

イベントのリターン コードを示します。

値: 以下のいずれかです。

- D（拒否）- 権限が不十分なためイベントが拒否されました。
- P（許可）- イベントが許可されました。
- W（警告）- アクセス要求はアクセス ルールに違反していますが警告モードが設定されたためイベントが許可されました。

注: seaudit の詳細な出力ではこのフィールドはトレース情報を示します。

イベント タイプ

このレコードが属するイベントのタイプを識別します。

注: CA Access Control エンドポイント管理 はこのフィールドを単にイベントとして参照します。

ユーザ名

このイベントをトリガしたアクションを実行したアクセス元の名前を識別します。

User Logon Session ID

アクセス元のセッション ID を識別します。

Real User ID

プロセスを実行したユーザのユーザ ID を識別します。

注: (UNIX) このフィールドは seaudit の詳細でない出力には表示されません。

Real user name

トレースされたアクションを実行しているユーザ名を識別します。

有効なユーザ ID

(UNIX のみ) ネイティブな OS の有効なユーザ ID の ID を識別します。

注: このフィールドは seaudit の詳細でない出力には表示されません。

有効なユーザ名

(UNIX のみ) このイベントをトリガしたネイティブな OS の有効なユーザ名を識別します。ユーザが別のユーザを代行する (代理になる) または setuid プログラムを実行する場合、この名前はユーザ名とは異なります。

注: このフィールドは KBL 監査出力には表示されません。

クラス

アクセスされているリソースが属するクラスを識別します。

Resource

アクセスまたは更新されている実際のリソースの名前を識別します。

詳細

CA Access Control がこのイベントに対して実行するアクションを決定したステージを示します。

注: seaudit の詳細でない出力では、監査レコードのこのフィールドに数字が表示されます。この数字は承認 stage code といいます。詳細な出力または CA Access Control エンドポイント管理 では、監査レコードに承認 stage code に関連するメッセージが表示されます。すべての stage code を一覧表示するには、seaudit -t を実行します。

Trace information

クラス、リソース、およびそのリソースで実行されたアクションまたはそのアクションの結果を含む、詳細なトレース情報を表示します。

監査フラグ

アクセス元が内部ユーザ（CA Access Control データベース ユーザ）であるかまたはエンタープライズ ユーザであるかを示します。

注: アクセス元がエンタープライズ ユーザである場合、seaudit の詳細でない出力では、監査レコードのこのフィールドに「(OS user)」の文字列が表示されます。エンタープライズ ユーザではない場合、このフィールドは空白です。

例: UNIX 上のユーザ イベント メッセージのトレース メッセージ

以下の監査レコードは、seaudit の詳細出力から取得したものです。

```
03 Nov 2008 10:38:47 P TRACE       root        490daddd:00000140 john        root
FILE       /home/jon/file.txt   55  FILE    > Result: 'P' [stage=55 gstag=55 ACEEH=8
rv=0(/home/john/file.txt
Event type: Trace message on a user
Date: 03 Nov 2008
Time: 10:38
Details: Resource ACL check
Trace information: FILE    > Result: 'P' [stage=55 gstag=55 ACEEH=8
rv=0(/home/john/file.txt
Class: FILE
Resource: /home/admin/file.txt
User name: root
Real user ID: 108
Real user name: john
Effective user ID: 108
Effective user name: root
User Logon Session ID: 490daddd:00000140
Audit flags: AC database user
```

この監査レコードは、2008 年 11 月 3 日に管理者が FILE クラスに属するリソースにアクセスしようとしたことにより、トレース メッセージがログに記録されたことを示します。アクセスされたリソースの ACL に従って、管理者はアクセスが許可されました(承認 stage code 55 - リソースの ACL チェック)。

例: Windows 上のユーザ イベント メッセージのトレース メッセージ

以下の監査レコードは、seaudit の詳細出力から取得したものです。

```
10 Nov 2008 10:14:53 P TRACE     MACHINE¥Administrator 00000000:172ef9ef MACHINE¥john
MACHINE¥john WINSERVICE   _default     1059  WINSERVICE >
(C:¥WINDOWS¥system32¥services.exe) Result: 'P' [stage=1059 gstag=1059 ACEEH=6
rv=0x0 (WebClient)]                    Why?  Default record universal access check
Event type: Trace message on a user
Date: 10 Nov 2008
Time: 10:14
Details: Default record universal access check
Trace information: WINSERVICE > (C:¥WINDOWS¥system32¥services.exe) Result: 'P'
[stage=1059 gstag=1059 ACEEH=6   rv=0x0 (WebClient)]                 Why? Default
record universal access check
Class: WINSERVICE
Resource: _default
User name: MACHINE¥Administrator
Real user name: MACHINE¥john
User Logon Session ID: 00000000:172ef9ef
Audit flags: AC database user
```

この監査レコードは、2008 年 11 月 10 日に管理者が WINSERVICE クラスに属するリソース _default にアクセスしようとしたことにより、トレース メッセージがトリガされたことを示します。レコード ユニバーサル アクセス チェックにより管理者はアクセスが許可されました(承認 stage code 1059 - デフォルト レコードユニバーサル アクセス チェック)。

詳細情報:

ユーザのトレース メッセージの承認 Stage Code (P. 724)
レコードを作成した理由を示す理由コード (P. 725)

ログインおよびログアウト イベントの承認 stage code

ログインおよびログアウト イベントの承認 stage code は、CA Access Control がログインおよびログアウト イベントに対して実行するアクションを決定するステージを示しています。

詳細情報:

ログイン イベント (P. 647)
ログアウト イベント (P. 650)
ログイン アカウントの有効化イベント (P. 653)
ログイン アカウントの無効化イベント (P. 655)
パスワード試行イベント (P. 658)

2 - ユーザ オブジェクトの取得

ユーザ モード、端末、ログイン プログラムなどのユーザ情報を CA Access Control がロードできなかったためにログイン試行が失敗したことを示します。データベースが破損している場合、または CA Access Control が正常に起動しなかった場合、CA Access Control がこのメッセージを監査ログに書き込みます。

3 - ログイン端末ソースの端末チェック

TERMINAL クラス ルールに従って、CA Access Control がログインを許可または拒否したことを示します。

5 - ユーザの一時停止のチェック

ユーザ アカウントが一時停止にされているため、CA Access Control がログインを拒否したことを示します。

6 - ユーザの有効期限のチェック

ユーザのプロファイルに定義されているユーザ アカウントの有効期限が切れているため、CA Access Control がログインを拒否したことを示します。

7 - ユーザの日時のチェック

ユーザが CA Access Control データベースで許可された日時以外にログインしようとしたため、CA Access Control がログインを拒否したことを示します。

8 - パスワード有効性のチェック

UNIX で該当

CA Access Control がユーザのパスワードをチェックして、パスワード ルールに従っているかどうかを確認したことを示します。ユーザのパスワードが CA Access Control データベースのパスワード ルールに従っていないためにログイン試行が失敗したときに、CA Access Control がこのメッセージを監査ログに書き込みます。

9 - ユーザの猶予ログインのチェック

ユーザ アカウントが猶予ログインの試行回数に達したため、CA Access Control がログインを拒否したことを示します。

10 - パスワードの期限が切れ、これ以上猶予ログインはできません

パスワードの期限が切れたため、CA Access Control がログインを拒否したことを示します。ユーザがパスワードの期限内にパスワードを変更せず、ユーザのプロファイル グループの定義または CA Access Control グローバル定義のいずれにも、パスワードの有効期限以降の猶予ログイン回数が設定されていません。

11 - ユーザ ACEE の作成

CA Access Control がユーザの ACEE を正常に生成したことを示します。

12 - ユーザの非アクティブな日数のチェック

非アクティブの許容期間を超過してユーザが非アクティブだったため、CA Access Control がログインを拒否したことを示します。非アクティブの許容期間は、ユーザのプロファイルまたは CA Access Control グローバル設定に定義されています。

13 - ユーザのログイン回数が多すぎます

最大許容回数を超えて、さまざまな端末からユーザが同時ログインを行ったため、CA Access Control がログインを拒否したことを示します。同時ログインの最大許容回数は、ユーザのプロファイルまたは CA Access Control グローバル設定の Maxlogins プロパティ値で定義されています。

14 - アクティブな HOLIDAY のチェック

制限された休日中にユーザがログインしようとしたため、CA Access Control たログインを拒否したことを示します。制限された休日は、HOLIDAY クラスに定義されています。

15 - ログイン アプリケーション（LOGINAPPL）のチェック

UNIX で該当

LOGINAPPL クラス ルールに従って CA Access Control がログインを拒否したことを示します。

16 - ユーザ グループの日時のチェック

ユーザまたはユーザのグループの 1 つに対して許可された日時以外にユーザがログインしようとしたため、CA Access Control がログインを拒否したことを示します。

17 - ネイティブ環境によって試行が拒否されました

UNIX で該当

ネイティブ環境の設定により、ログイン試行が失敗したことを示します。CA Access Control PAM モジュールがログに記録します。

18 - ドメイン制限のないユーザ

Windows で該当

ユーザがドメイン名を指定しなかったため、CA Access Control がログインを拒否しました。

19 - 拒否する理由がありません - ログインを許可

ログイン試行がすべてのチェック ステージを通過し、ログイン認証に TERMINAL オブジェクトが割り当てられているため、CA Access Control がログインを許可したことを示します。

注: このイベント ステージ メッセージが表示される場合、ログイン認証が端末名が指定されていない CA Access Control 許可 API によってトリガされたことを示します。

20 - 「論理」ユーザのチェック

CA Access Control が「論理」ユーザ(*logical* プロパティが設定されているユーザ)のログインを許可しないため、CA Access Control がログインを拒否したことを示します。

49 - 最後のプロセスの終了後、ログアウトが検出されました

UNIX で該当

最後のプロセスの終了後、CA Access Control はユーザ ログアウト イベントの発生を検出しました。

リソース アクセス イベントの承認 stage code

リソース アクセス イベントの承認 stage code は、CA Access Control がリソース アクセス イベントに対して実行するアクションを決定するステージを示しています。

詳細情報:

リソース アクセス イベント (P. 661)

50 - リソースのセキュリティ LABEL チェック

リソースにアクセスしようとしたユーザについて、以下のうち 1 つが当てはまるため、CA Access Control がリソースへのアクセスを拒否したことを示します。

- リソースのセキュリティ ラベルの方がユーザのセキュリティ ラベルよりもセキュリティ レベルが高い
- ユーザにセキュリティ ラベルがない

51 - リソースのセキュリティ LEVEL チェック

リソースにアクセスしようとしたユーザについて、以下のうち 1 つが当てはまるため、CA Access Control がリソースへのアクセスを拒否したことを示します。

- リソースのセキュリティ レベルがユーザよりも高い
- ユーザにセキュリティ レベルがない

52 - リソースのカテゴリのチェック

リソースに、ユーザに割り当てられていないセキュリティ カテゴリが割り当てられているため、CA Access Control がリソースへのアクセスを拒否したことを示します。

53 - リソースの DAYTIME のチェック

ユーザがリソースに許可されている日時以外にアクセスしようとしたため、CA Access Control がリソースへのアクセスを拒否したことを示します。

54 - リソースの OWNER のチェック

アクセスしているユーザがリソースを所有しているため、CA Access Control がリソースへのアクセスを許可したことを示します。

55 - リソースの ACL のチェック

リソースの ACL にユーザが含まれるため、CA Access Control がリソースへのアクセスを許可または拒否したことを示します。

56 - リソース グループの ACL のチェック

リソース グループの ACL リストにユーザが含まれるため、CA Access Control がリソースへのアクセスを許可または拒否したことを示します。

57 - リソース ACL のユーザ グループ

ユーザ グループ ACL に少なくとも 1 つのリソースが含まれるため、CA Access Control がリソースへのアクセスを許可または拒否したことを示します。

58 - リソース グループ ACL のユーザ グループ

リソース グループの ACL に少なくとも 1 つのユーザ グループが含まれるため、CA Access Control がリソースへのアクセスを許可または拒否したことを示します。

59 - リソースの UACC のチェック

リソースのデフォルト設定のため、CA Access Control がリソースへのアクセスを許可したことを示します。

61 - ユーザはリソースのオペレータ

ユーザに OPERATOR 属性があるため、CA Access Control がリソースへのアクセスを許可したことを示します。OPERATOR 属性により、ユーザは FILE リソースの読み取りおよび chdir アクセスの認証手順をバイパスできます。

注: UNIX では、CA Access Control はこのメッセージをトレース ファイルのみに書き込み、監査ログ ファイルには書き込みません。

62 - 保護されていないリソースのクラスの UACC チェック

CA Access Control が、リソース クラスの defaccess 値に従って、CA Access Control データベースにレコードを持たないリソースへのアクセスを許可または拒否したことを示します。

63 - プログラム条件付きアクセス

リソースの PACL にプログラムとユーザ、またはユーザ グループの 1 つが含まれるため、CA Access Control がリソースへのアクセスを許可または拒否したことを示します。

64 - リソース ACL のユーザ '*'

リソースの ACL にアスタリスク(*)が含まれるため、CA Access Control がリソースへのアクセスを許可または拒否したことを示します。

注: アスタリスクはすべての定義されたユーザを指定します。

65 - ユーザはリソースの AUDITOR

ユーザに AUDITOR 属性があるため、CA Access Control が監査ファイルへのアクセスを許可したことを示します。AUDITOR 属性により、ユーザは読み取りおよび chdir アクセス要求の認証手順をバイパスできます。

注: CA Access Control はこのメッセージをトレース ファイルにのみ書き込み、監査ログ ファイルには書き込みません。

69 - アクセスを許可したステップがありません

ユーザをリソースにアクセスさせるルールが見つからなかったため、CA Access Control はリソースへのアクセスを拒否しました。

70 - リソースのグループの OWNER チェック

リソースへのアクセスを試行しているユーザがいずれかのリソースのグループの所有者であるため、CA Access Control はリソースへのアクセスを許可しました。

75 - リソース グループ ACL のユーザ '*'

リソース グループの ACL にアスタリスク(*)が含まれるため、CA Access Control がリソースへのアクセスを許可または拒否したことを示します。

注: アスタリスクはすべての定義されたユーザを指定します。

76 - リソースが ACL チェックを拒否しました

リソースの NACL にユーザが含まれるため、CA Access Control がリソースへのアクセスを拒否したことを示します。

77 - リソース グループ内で ACL チェックを拒否しました

リソース グループの NACL にユーザが含まれるため、CA Access Control がリソースへのアクセスを拒否したことを示します。

78 - リソース内のユーザ グループが ACL を拒否しました

リソースの NACL に少なくとも 1 つのユーザ グループが含まれるため、CA Access Control がリソースへのアクセスを拒否したことを示します。

79 - リソース グループ内のユーザ グループが ACL を拒否しました

リソース グループの NACL に少なくとも 1 つのユーザ グループが含まれるため、CA Access Control がリソースへのアクセスを拒否したことを示します。

80 - リソース内のユーザ '*' が ACL を拒否しました

リソースの NACL にアスタリスク(*)が含まれるため、CA Access Control がリソースへのアクセスを拒否したことを示します。

注: アスタリスクはすべての定義されたユーザを指定します。

81 - リソース グループ内のユーザ '*' が ACL を拒否しました

リソース グループの NACL にアスタリスク(*)が含まれるため、CA Access Control がリソースへのアクセスを拒否したことを示します。

注: アスタリスクはすべての定義されたユーザを指定します。

82 - リソース DAYTIME のグループのチェック

ユーザがリソース グループに許可されている日時以外にリソースにアクセスしようとしたため、CA Access Control がリソースへのアクセスを拒否したことを示します。

86 - ユーザのリソース カレンダ ACL チェック

ユーザがリソースの CALACL によって許可または拒否される時間にリソースにアクセスしようとしたため、CA Access Control がリソースへのアクセスを許可または拒否したことを示します。

87 - ユーザのリソース グループ カレンダ ACL チェック

ユーザがリソース グループの CALACL によって許可または拒否される時間にリソースにアクセスしようとしたため、CA Access Control がリソースへのアクセスを許可または拒否したことを示します。

88 - ユーザ グループのリソース カレンダ ACL チェック

ユーザがリソースの CALACL に含まれるグループの 1 つのメンバであるために許可または拒否された時間にユーザがリソースにアクセスしようとしたため、CA Access Control がリソースへのアクセスを許可または拒否しました。

89 - ユーザ グループのリソース グループ カレンダ ACL チェック

ユーザがリソースの CALACL に含まれるグループの 1 つのメンバであるために許可または拒否された時間にユーザ グループがリソースにアクセスしようとしたため、CA Access Control がリソースへのアクセスを許可または拒否したことを示します。

90 - リソース カレンダ ACL のユーザ *

リソースの CALACL にアスタリスク(*)が含まれるため、CA Access Control がリソースへのアクセスを許可または拒否したことを示します。

注: アスタリスクはすべての定義されたユーザを指定します。

91 - リソース グループ カレンダ ACL のユーザ *

リソース グループの CALACL にアスタリスク(*)が含まれるため、CA Access Control がリソースへのアクセスを許可または拒否したことを示します。

注: アスタリスクはすべての定義されたユーザを指定します。

92 - 保護対象リソースのパスの名前変更を試行しました

Windows で該当

CA Access Control が保護されたファイルまたはレジストリ エントリの名前変更の要求を拒否したことを示します。

200 - クラス チェックが有効でありません

リソース クラスが非アクティブなため、CA Access Control がリソースへのアクセスを許可したことを示します。

注: リソース クラスが非アクティブな場合、setoptions list コマンドではクラス アクティビティが 'No' と表示されます。

201 - ユーザ情報をロードしています

ユーザの情報を取得できなかったため、CA Access Control が要求を承認できなかったことを示します。

202 - 警告モードのリソース

リソースが警告モードであるため、CA Access Control がリソースへのアクセスを許可したことを示します。

203 - リソースに対するアクセスは MAXIMUM_ALLOWED です

Windows で該当

許可される場合、CA Access Control がレジスト ハンドルに最大アクセス権を割り当てたことを示します。

拒否される場合、CA Access Control がレジストリ ハンドルへのアクセスをブロックしたことを示します。

204 - 警告モードのクラス

リソース クラスが警告モードであるため、CA Access Control がリソースへのアクセスを許可したことを示します。

210 - 特殊なカーネル モジュールのロード チェック

UNIX で該当

KMODULE クラス定義に基づき、CA Access Control がカーネル モジュールのロードまたはアンロードを許可または拒否したことを示します。

250 - untrusted プログラムの実行

CA Access Control が untrusted プログラムの実行の試行を拒否したことを示します。

251 - 拒否可能なパラメータの使用

コマンド構文に SUDO レコードで禁止と定義されているパラメータがあるため、CA Access Control が sesudo コマンド実行の試行を拒否したことを示します。

252 - _abspath ユーザが指定した相対パス

UNIX で該当

プログラム実行を試みるユーザが '_abspath' グループのメンバであるため、CA Access Control が相対パスで指定されたプログラム実行の試行を拒否したことを示します。

253 - 許可された sesudo ジョブ

CA Access Control が sesudo コマンド実行の試行を許可したことを示します。

254 - sesudo コマンドが失敗しました

UNIX で該当

sesudo がオペレーティング システムの実行に失敗したことを示します。

440 - 無効なカレンダが検出されました

カレンダ情報の取得エラー(メモリの問題、カレンダ テーブルの破損など)のため CA Access Control がアクセスを拒否したことを示します。

441 - カレンダへのアクセスが拒否されました

アクセスされたリソースと関連するカレンダ オブジェクトの定義に現時点でアクセスできないため、CA Access Control がアクセスを拒否したことを示します。

1050 - デフォルト レコードのセキュリティ ラベル チェック

リソースへのアクセスを試行したユーザに対し以下のいずれかが true のため、CA Access Control がデフォルト レコードへのアクセスを拒否したことを示します。

- リソースのセキュリティ ラベルの方がユーザのセキュリティ ラベルよりもセキュリティ レベルが高い
- ユーザにセキュリティ ラベルがない

1051 - デフォルト レコードのセキュリティ レベル チェック

リソースへのアクセスを試行したユーザに対し以下のいずれかが true のため、CA Access Control がデフォルトリソースへのアクセスを拒否したことを示します。

- リソースのセキュリティレベルがユーザよりも高い
- ユーザにセキュリティレベルがない

1052 - デフォルト レコードのカテゴリ チェック

ユーザに割り当てられていないセキュリティ カテゴリにリソースが割り当てられているため、CA Access Control がデフォルトリソースへのアクセスを拒否したことを示します。

1053 - デフォルト レコードの日付と時間チェック

ユーザがリソースに対し許可された日付と時間以外でアクセスしようとしたため、CA Access Control がデフォルトリソースへのアクセスを拒否したことを示します。

1054 - デフォルト レコードの OWNER のチェック

アクセス中のユーザがデフォルトリソースを所有しているため、CA Access Control がデフォルトリソースへのアクセスを許可したことを示します。

1055 - ユーザに対するデフォルト レコードの ACL のチェック

リソースの ACL がユーザを一覧表示する、またはしないため、CA Access Control がデフォルトリソースへのアクセスを許可または拒否したことを示します。

1056 - ユーザに対するデフォルト レコード グループの ACL のチェック

リソース グループの ACL がユーザを一覧表示する、またはしないため、CA Access Control がデフォルトリソースへのアクセスを許可または拒否したことを示します。

1057 - ユーザ グループに対するデフォルト レコードの ACL のチェック

CA Access Control がデフォルト リソースへの読み取りまたは chdir アクセスを許可したことを示します。

注: CA Access Control はこのメッセージをトレース ファイルにのみ書き込み、監査ログ ファイルには書き込みません。

1058 - ユーザ グループに対するデフォルト レコード グループの ACL のチェック

リソース グループの ACL がユーザ グループを一覧表示する、またはしないために、CA Access Control がデフォルト リソースへのアクセスを許可または拒否したことを示します。

1059 - デフォルト レコードのユニバーサル アクセス チェック

リソースのデフォルト設定により、CA Access Control がデフォルト リソースへのアクセスを許可したことを示します。

1061 - デフォルト レコードの OPERATOR 属性のチェック

ユーザが OPERATOR 属性を所有しているために、CA Access Control がデフォルト リソースへのアクセスを許可したことを示します。OPERATOR 属性により、ユーザは読み取りおよび chdir アクセス要求の認証手順をバイパスできます。

注: CA Access Control はこのメッセージをトレース ファイルにのみ書き込み、監査ログ ファイルには書き込みません。

1062 - デフォルト レコード クラスのグローバル ユニバーサル アクセス

リソース クラスの defaccess 値に基づき、CA Access Control が CA Access Control データベースにレコードを持たないデフォルト リソースへのアクセスを許可または拒否したことを示します。

1063 - デフォルト レコードのプログラム条件アクセス

リソースの PACL がリソースをアクセスしているプログラムを一覧表示する、またはしないため、CA Access Control がデフォルト リソースへのアクセスを許可または拒否したことを示します。

1064 - _default レコード ACL のユーザ「*」

リソースの ACL にアスタリスク (*) が含まれているため、CA Access Control がデフォルト リソースへのアクセスを許可または拒否したことを示します。

注: アスタリスクはすべての定義されたユーザを指定します。

1069 - デフォルト レコードへのアクセス許可のルールがありません

ユーザがリソースにアクセスできるルールを検出できなかったため、CA Access Control がデフォルト リソースへのアクセスを拒否したことを示します。

1202 - 警告モードでのデフォルト レコード

リソースが警告モードであるために、CA Access Control がデフォルト リソースへのアクセスを許可したことを示します。

1250 - デフォルト レコードがアントラストに設定されています

CA Access Control がデフォルトのアントラスト プログラムの実行の試行を拒否したことを示します。

アントラスト メッセージ イベントの承認 stage code

アントラスト メッセージ イベントの承認 stage code は、CA Access Control がアントラスト メッセージ イベントに対して実行するアクションを決定するステージを示します。

詳細情報:

アントラスト メッセージ イベント (P. 664)

0 - Watchdog によるファイル確認中に一般エラーが発生しました

CA Access Control がファイル情報の取得中にエラーが発生したことを示します。ファイルが信頼できない場合、CA Access Control はこのメッセージを監査ログに書き込みます。詳細はシステム ログを確認してください。

1 - PROGRAM または SECFILE の stat 情報が変更されました

PROGRAM または SECFILE クラスのレコードでデータが変更されたことを示します。CA Access Control がプログラムまたはファイルの改ざんの試行を検出した場合、このメッセージが監査ログに書き込まれます。監査イベント、システム ログ、プログラムまたはファイルのトレース レコードを確認してください。プログラムまたはファイルが管理者によって変更された場合は、変更されたプログラムまたはファイルを再度 Trusted 状態にすることを検討してください。

4 - 変更された PROGRAM または SECFILE の CRC チェック

PROGRAM または SECFILE クラスのレコードの CRC(Cyclic Redundancy Check)が変更されたことを示します。システム ログ、イベント ログ ファイル、プログラムまたはファイルのトレース レコードを確認してください。

5 - PROGRAM または SECFILE のファイルに対して Stat を実行できません

CA Access Control が指定されたファイルのファイル情報の取得に失敗したことを示します。以下のいずれかに該当する場合、CA Access Control はこのメッセージを監査ログに書き込みます。

- ファイル名またはディレクトリが変更された
- ファイル名またはディレクトリが存在しない
- ファイルのアクセス許可
- システムのメモリが不足している

エラーの考えられる原因を判定するため、システム ログ ファイルを確認します。

7 - PROGRAM または SECFILE の MD5 シグネチャが変更されました

PROGRAM または SECFILE クラスのレコードの MD5 シグネチャが変更されたことを示します。システム ログ ファイル、監査メッセージ、プログラムまたはファイルのトレース ログを確認してください。

8 - PROGRAM または SECFILE の SHA1 シグネチャが変更されました

PROGRAM または SECFILE クラスのレコードの SHA1 シグネチャが変更されたことを示します。システム ログ ファイル、監査メッセージ、プログラムまたはファイルのトレース ログを確認してください。

受信ネットワーク接続イベントの承認 stage code

受信ネットワーク接続イベントの承認 stage code は、CA Access Control が受信ネットワーク接続イベントに対して実行するアクションを決定するステージを示します。

詳細情報:

受信ネットワーク接続イベント (P. 668)

150 - クラス テーブルの確認

クラスが CA Access Control データベースで見つからなかったことを示します。CA Access Control データベースに問題がある場合、CA Access Control はこのメッセージを監査ログに書き込みます。この問題を解決するには、dbmgr ユーティリティを使用して CA Access Control データベースを再構築します。

重要: dbmgr ユーティリティは、問題を解決する際にサポート担当者の指示に従って使用する必要があります。 詳細については、当社テクニカル サポート (http://www.ca.com/jp/support/) にお問い合わせください。

詳細情報:

dbmgr ユーティリティ (P. 34)

153 - inetacl の HOST エントリのアスタリスク

ホスト INETACL にアスタリスク(*)が含まれるため、CA Access Control が保護されたホストからの接続を許可または拒否したことを示します。

注: アスタリスクはゼロまたはそれ以上の文字の連続を示すため、INETACL で使用されるとすべてのサービスと一致します。

156 - HOST エントリ inetacl

ホスト INETACL に接続サービスがあるため、CA Access Control が保護されたホストからの接続を許可または拒否したことを示します。

157 - HOST クラス UACC

ホスト UACC クラスに定義されたアクセス権限のデフォルト値のため、CA Access Control が保護されたホストからの接続を許可または拒否したことを示します。

159 - HOST エントリ サービス範囲 ACL

接続サービスがホスト INETACL の範囲内にあるため、CA Access Control が保護されたホストからの接続を許可または拒否したことを示します。

163 - サービスへのアクセスを許可するルールがありません

アクセスを許可するルールが見つからなかったため、CA Access Control がホストからの接続を拒否したことを示します。このホストの HOST クラス アクセス ルールを確認してください。

164 - HOST グループ inetacl

GHOST オブジェクトの INETCAL に接続サービスがあるため、CA Access Control が保護されたホストからの接続を許可または拒否したことを示します。

165 - HOST グループ サービス範囲 ACL

接続サービスがホスト グループの INETACL の範囲にあるため、GHOST ホスト グループ オブジェクトのメンバである保護されたホストからの接続を CA Access Control が許可または拒否したことを示します。

166 - inetacl の HOST グループのアスタリスク

ホスト グループの INETACL にアスタリスク(*)があるため、GHOST ホスト グループ オブジェクトのメンバである保護されたホストからの接続を CA Access Control が許可または拒否したことを示します。

注: アスタリスクはゼロまたはそれ以上の文字の連続を示すため、INETACL で使用されるとすべてのサービスと一致します。

167 - HOSTNET(ネットワークまたは IP マスク/一致)の inetacl

HOSTNET レコードの INETACL に接続サービスがあるため、CA Access Control が保護されたホストからの接続を許可または拒否したことを示します。

168 - HOSTNET(ネットワークまたは IP マスク/マッチ)のサービス範囲

接続サービスが HOSTNET レコードの INETACL の範囲内にあるため、CA Access Control が保護されたホストからの接続を許可または拒否したことを示します。

169 - HOSTNET(ネットワークまたは IP マスク/マッチ)の inetacl のアスタリスク

HOSTNET レコードの INETACL にアスタリスク(*)が含まれるため、CA Access Control が保護されたホストからの接続を許可または拒否したことを示します。

注: アスタリスクはゼロまたはそれ以上の文字の連続を示すため、INETACL で使用されるとすべてのサービスと一致します。

170 - HOSTNP(ホスト名パターン)の inetacl

HOSTNP レコードの INETACL に接続サービスがあるため、CA Access Control が保護されたホストからの接続を許可または拒否したことを示します。

171 - HOSTNP（ホスト名パターン）のサービス範囲

接続サービスが HOSTNP レコードの INETACL の範囲内にあるため、CA Access Control が保護されたホストからの接続を許可または拒否したことを示します。

172 - HOSTNP（ホスト名パターン）の inetacl のアスタリスク

HOSTNP レコードの INETACL にアスタリスク（*）が含まれるため、CA Access Control が保護されたホストからの接続を許可または拒否したことを示します。

注：アスタリスクはゼロまたはそれ以上の文字の連続を示すため、INETACL で使用されるとすべてのサービスと一致します。

173 - HOST エントリの日時の制限

試みたアクセスが HOST レコードの日時制限の範囲外だったため、CA Access Control が保護されたホストへのアクセスを拒否したことを示します。

174 - HOST グループの日時の制限

GHOST レコードの日時制限の範囲外だったため、CA Access Control が保護されたホスト グループへのアクセスを拒否したことを示します。

175 - HOSTNET（ネットワークまたは IP マスク/一致）の日時の制限

HOSTNET レコードの日時制限の範囲外だったため、CA Access Control が保護されたホストへのアクセスを拒否したことを示します。

176 - HOSTNP（ホスト名パターン）の日時の制限

HOSTNP レコードの日時制限の範囲外だったため、CA Access Control が保護されたホストへのアクセスを拒否したことを示します。

177 - HOST_default の日時の制限

HOST _default レコードの日時制限の範囲外だったため、CA Access Control が保護されたホストへのアクセスを拒否したことを示します。

178 - HOST_default inetacl

HOST _default INETACL の値のため、CA Access Control が保護されたホストへのアクセスを許可または拒否したことを示します。

179 - HOST_default のサービス範囲

接続サービスが HOST _default レコードの INETACL の範囲内にあるため、CA Access Control が保護されたホストへのアクセスを許可または拒否したことを示します。

180 - HOST_default のサービスのアスタリスク

HOST _default レコードの INETACL にアスタリスク(*)が含まれるため、CA Access Control が保護されたホストからのアクセスを許可または拒否したことを示します。

注: アスタリスクはゼロまたはそれ以上の文字の連続を示すため、INETACL で使用されるとすべてのサービスと一致します。

404 - TCP サービス ACL の HOST エントリ

TCP レコードの ACL に HOST が含まれるため、CA Access Control が HOST からのアクセスを許可または拒否したことを示します。

405 - TCP サービス ACL の GHOST エントリ

TCP レコードの ACL に HOST がメンバである GHOST が含まれているため、CA Access Control が HOST からのアクセスを許可または拒否したことを示します。

406 - TCP サービス ACL の HOSTNET エントリ

TCP レコードの ACL に HOST が属している HOSTNET ネットワークが含まれているため、CA Access Control が HOST からのアクセスを許可または拒否したことを示します。

407 - TCP サービス ACL の HOSTNP エントリ

TCP レコードの ACL に HOST が属している HOSTNP セットが含まれているため、CA Access Control が HOST からのアクセスを許可または拒否したことを示します。

送信ネットワーク接続イベントの承認 stage code

送信ネットワーク接続イベントの承認 stage code は、CA Access Control が送信ネットワーク接続イベントに対して実行するアクションを決定するステージを示します。

詳細情報:

送信ネットワーク接続イベント (P. 670)

400 - TCP クラスの _default サービス

TCP レコードのサービス接続のための _default オブジェクト アクセス権限により、CA Access Control が保護されたホストへのアクセスを許可または拒否したことを示します。

401 - TCP サービスの UACC クラス

UACC クラスの TCP オブジェクトの値により、CA Access Control が保護されたホストへのアクセスを許可または拒否したことを示します。

402 - TCP サービスの日時制限

TCP レコードの日時制限の範囲外だったため、CA Access Control が保護された TCP サービスへのアクセスを拒否したことを示します。

403 - ACL は TCP サービスのステージを読み込みます

TCP レコードの ACL 読み取りプロパティのため、CA Access Control が TCP サービスへのアクセスを許可または拒否したことを示します。データベースが破損している場合、CA Access Control はこのメッセージを監査ログに書き込みます。

408 - TCP サービスのデフォルト アクセス

TCP レコードの defaccess プロパティのため、CA Access Control が TCP クラス サービスへのアクセスを許可または拒否したことを示します。

注: このイベント メッセージも着信 TCP イベントに適用して HOST への受信接続を示します。

409 - CACL は TCP サービスのステージを読み込みます

TCP レコードの CACL 読み取りプロパティのため、CA Access Control が TCP サービスへのアクセスを拒否したことを示します。 データベースが破損している場合、CA Access Control はこのメッセージを監査ログに書き込みます。

410 - TCP サービス CACL 内の USER の HOST エントリ

CA Access Control が指定された USER または XUSER の HOST オブジェクトへのアクセスを許可または拒否したことを示します。CA Access Control は TCP サービスの CACL 内のアクセス ルールを使用して、アクセスを許可するか拒否するかを決定します。

411 - TCP サービス CACL 内の USER の GHOST エントリ

CA Access Control が指定された USER または XUSER オブジェクトの GHOST オブジェクトへのアクセスを許可または拒否したことを示します。CA Access Control は TCP サービスの CACL 内のアクセス ルールを使用して、アクセスを許可するか拒否するかを決定します。

412 - TCP サービス CACL 内の USER の HOSTNET エントリ

CA Access Control が指定された USER または XUSER オブジェクトの HOSTNET オブジェクトへのアクセスを許可または拒否したことを示します。CA Access Control は TCP サービスの CACL 内のアクセス ルールを使用して、アクセスを許可するか拒否するかを決定します。

413 - TCP サービス CACL 内の USER の HOSTNP エントリ

CA Access Control が指定された USER または XUSER オブジェクトの HOSTNP オブジェクトへのアクセスを許可または拒否したことを示します。CA Access Control は TCP サービスの CACL 内のアクセス ルールを使用して、アクセスを許可するか拒否するかを決定します。

414 - TCP サービス CACL 内の GROUP の HOST エントリ

CA Access Control が指定された GROUP または XGROUP オブジェクトの HOST オブジェクトへのアクセスを許可または拒否したことを示します。CA Access Control は TCP サービスの CACL 内のアクセス ルールを使用して、アクセスを許可するか拒否するかを決定します。

415 - TCP サービス CACL 内の GROUP の GHOST エントリ

CA Access Control が指定された GROUP または XGROUP オブジェクトの GHOST オブジェクトへのアクセスを許可または拒否したことを示します。CA Access Control は TCP サービスの CACL 内のアクセス ルールを使用して、アクセスを許可するか拒否するかを決定します。

416 - TCP サービス CACL 内の GROUP の HOSTNET エントリ

CA Access Control が指定された GROUP または XGROUP オブジェクトの HOSTNET オブジェクトへのアクセスを許可または拒否したことを示します。CA Access Control は TCP サービスの CACL 内のアクセス ルールを使用して、アクセスを許可するか拒否するかを決定します。

417 - TCP サービス CACL 内の GROUP の HOSTNP エントリ

CA Access Control が指定された GROUP または XGROUP オブジェクトの HOSTNP オブジェクトへのアクセスを許可または拒否したことを示します。CA Access Control は TCP サービスの CACL 内のアクセス ルールを使用して、アクセスを許可するか拒否するかを決定します。

418 - TCP サービス CACL 内のユーザ '*' の HOST エントリ

HOST レコードの CACL にアスタリスク(*)が含まれるため、CA Access Control がユーザの HOST へのアクセスを許可または拒否したことを示します。

注: アスタリスクはすべての定義されたユーザを指定します。

419 - TCP サービス CACL 内のユーザ '*' の GHOST エントリ

GHOST レコードの CACL にアスタリスク(*)が含まれるため、CA Access Control が GHOST クラスに属する HOST へのユーザのアクセスを許可または拒否したことを示します。

注: アスタリスクはすべての定義されたユーザを指定します。

420 - TCP サービス内のユーザ '*' の HOSTNET エントリ

HOSTNET レコードの CACL にアスタリスク(*)が含まれるため、CA Access Control がユーザの HOSTNET オブジェクトへのアクセスを許可または拒否したことを示します。

注: アスタリスクはすべての定義されたユーザを指定します。

421 - TCP サービス CACL 内のユーザ '*' の HOSTNP エントリ

HOSTNP レコードの CACL にアスタリスク(*)が含まれるため、CA Access Control がユーザの HOSTNET オブジェクトへのアクセスを許可または拒否したことを示します。

注: アスタリスクはすべての定義されたユーザを指定します。

セキュリティ データベース管理イベントの承認 stage code

セキュリティ データベース管理イベントの承認 stage code は、CA Access Control がセキュリティ データベース管理イベントに対して実行するアクションを決定するステージを示します。

詳細情報:

セキュリティ データベース管理イベント (P. 673)

300 - 未定義の CA Access Control ユーザ

アクセスしているユーザが CA Access Control データベースに見つからなかったため、CA Access Control がシステムへのアクセスを拒否したことを示します。ユーザ アカウント プロファイルを確認してください。

301 - 最後の ADMIN ユーザを削除する試行

CA Access Control が以下のいずれかを実行する要求を拒否したことを示します。

- 最後の ADMIN ユーザを CA Access Control データベースから削除する
- ADMIN 属性を割り当てられた唯一のユーザから ADMIN 属性を削除する

302 - ユーザのルート権限を削除する試行

UNIX で該当

CA Access Control がシステム ルート アカウントを削除する試行を拒否したことを示します。

303 - ユーザが自分のパスワードを変更しようとしています

ユーザが selang コマンドを使用して自分のパスワードを変更しようとしたことを CA Access Control が拒否したことを示します。UNIX では、ユーザは sepass ユーティリティを使用して自分のパスワードを変更できます。Windows では、ネイティブのパスワード管理ツールを使用してパスワードを変更できます。

304 - 監査担当者ではないユーザが監査モードを設定しようとしています

ユーザに AUDITOR 属性がないため、CA Access Control がレコードの監査モードの変更を拒否したことを示します。ユーザにレコードの監査モードの変更を許可するには、ユーザに AUDITOR 属性を割り当てます。

305 - ADMIN ユーザに許可されたコマンドです

アクションを要求しているユーザに ADMIN 属性があるため、CA Access Control がアクションを許可したことを示します。

306 - Showuser（自分自身）、Showxusr が許可されています

CA Access Control がユーザまたは外部ユーザに対して、CA Access Control データベース内にある自分のレコードのプロパティの表示を許可したことを示します。

注: このメッセージは監査レコードとして書き込まれません。

307 - ユーザが所有していないカテゴリを設定しようとしています

セキュリティ カテゴリを割り当てようとしているユーザがそのセキュリティ カテゴリを所有していないため、CA Access Control がセキュリティ カテゴリの割り当ての試行を拒否したことを示します。

308 - ユーザが所有していないセキュリティ ラベルを設定しようとしました

セキュリティラベルを割り当てようとしているユーザがそのセキュリティラベルを所有していないため、CA Access Control がセキュリティ ラベルの割り当ての試行を拒否したことを示します。

309 - ユーザが自分のレベルより高いセキュリティ レベルを設定しようとしています

ユーザの持つセキュリティ レベルが割り当てようとしているセキュリティ レベルよりも低いため、CA Access Control がユーザへのセキュリティ レベルの割り当てを拒否したことを示します。

310 - ADMIN ではないユーザがユーザ モードを設定しようとしています

属性を設定しようとするユーザに ADMIN 属性がないため、CA Access Control が管理者属性の設定を拒否したことを示します。

311 - オブジェクト所有者に許可されたコマンドです

ユーザがレコードを所有しているため、CA Access Control がアクションを許可したことを示します。

312 - ネイティブ ファイルの所有者は CA Access Control に定義できます

UNIX で該当

ファイルの所有者がファイルを CA Access Control に定義したため、CA Access Control がアクションを許可したことを示します。

注: seos.ini ファイルの lang セクションの use_unix_file_owner トークンが yes に設定されている場合、ファイルの所有者はファイルを CA Access Control に定義できます。

313 - GROUP-ADMIN ユーザに許可されたコマンドです

CA Access Control が、GROUP-ADMIN 属性を持つユーザにグループ内のレコードの変更を許可したことを示します。

314 - GROUP-ADMIN ユーザはグループに対して join/join- を実行できます

CA Access Control が、GROUP-ADMIN 属性を持つユーザにグループへのユーザの追加またはグループからのユーザの削除を許可したことを示します。

315 - GROUP-AUDITOR/ADMIN はグループを一覧表示できます

ユーザにそのグループに対する GROUP-ADMIN または GROUP-AUDITOR 属性があるため、CA Access Control がグループ内のレコードのプロパティを一覧表示することを許可したことを示します。

316 - 監査担当者は任意のオブジェクトを一覧表示できます

CA Access Control が AUDITOR 属性を持つユーザにデータベース内のデータの表示を許可したことを示します。

317 - OPERATOR は任意のオブジェクトを一覧表示できます

CA Access Control が OPERATOR 属性を持つユーザにデータベース内のデータの表示を許可したことを示します。

318 - GROUP-AUDITOR はグループの有効範囲内のオブジェクトを一覧表示できます

CA Access Control が GROUP-AUDITOR 属性を持つユーザに対して、データベース内のグループに関するデータの表示を許可したことを示します。

319 - GROUP-OPERATOR はグループの有効範囲内のオブジェクトを一覧表示できます

CA Access Control が GROUP-OPERATOR 属性を持つユーザに対して、データベース内のグループに関するデータの表示を許可したことを示します。

320 - CLASS-ADMIN ユーザに許可されたコマンドです

ADMIN クラスの ACL に含まれるユーザによってアクションが実行されたため、CA Access Control がアクションを許可したことを示します。

321 - アクセス権を持つ PWMANAGER/ADMIN に許可されたコマンドです

ユーザに PWMANAGER または ADMIN 属性があるため、CA Access Control がユーザにパスワードの変更を許可したことを示します。

322 - この操作を許可するルールがありません

操作を許可するルールが見つからなかったため、CA Access Control が操作を拒否したことを示します。

324 - ユーザが sepass を使用して自分のパスワードを変更しています

CA Access Control がユーザに sepass ユーティリティまたはパスワード Policy Model を使用して自分のパスワードを変更することを許可したことを示します。

326 - ユーザがユーザ自身の「ログイン情報」を作成しました

CA Access Control がユーザに自分自身のログイン情報の作成を許可したことを示します。

327 - GROUP-PWMANAGER に実行が許可されたコマンドです

コマンドを実行したユーザに GROUP-PWMANAGER 属性があるため、CA Access Control がコマンドを許可したことを示します。

329 - PWMANAGER がユーザを有効にしました

その他のユーザを有効にしたユーザに PWMANAGER 属性があるため、CA Access Control がユーザに別のユーザを有効（再アクティブ化）することを許可したことを示します。

330 - ドメイン変更が許可されたコマンドです

Windows で該当

CA Access Control がユーザに、新しいコンピュータをドメインに追加するなどの DOMAIN クラスの変更を許可したことを示します。

331 - PWMANAGER に実行が許可されたコマンドです

コマンドを実行したユーザに PWMANAGER 属性があるため、CA Access Control がコマンドの実行を許可したことを示します。

332 - ネイティブ フラグの変更は PWMANAGER に許可されています

Windows で該当

ユーザに PWMANAGER 属性があるため、CA Access Control がユーザ アカウントに割り当てられたアカウント フラグの修正をユーザに許可したことを示します。

333 - 「次回ログインする際にパスワードを変更する必要がある」属性の変更は PWMANAGER に許可されています

Windows で有効

ユーザに PWMANAGER 属性があるため、CA Access Control がユーザ カウントの「次回ログインする際にパスワードを変更する必要がある」属性の変更をユーザに許可したことを示します。

334 - GROUP-PWMANAGER に実行が許可されたコマンドです

コマンドを実行したユーザに GROUP-PWMANAGER 属性があるため、CA Access Control がコマンドを許可したことを示します。

335 - 「ログイン情報」の編集は PWMANAGER に許可されています

ユーザに PWMANAGER 属性があるため、CA Access Control がユーザ カウントの「ログイン情報」属性の編集をユーザに許可したことを示します。

336 - 監査担当ユーザに許可されたコマンドです

ユーザに AUDITOR 属性があるため、CA Access Control がユーザにコマンドの実行を許可したことを示します。

337 - コマンドとデータベース情報を調整できませんでした

コマンドに埋め込まれたオブジェクトが CA Access Control データベースに存在しないため、CA Access Control がコマンドを実行しなかったことを示します。コマンドを再実行する前に、コマンド構文を確認してください。

338 - 暗黙的な要求からコマンドを作成しています

CA Access Control が暗黙的な要求から発生したコマンドを作成したことを示します。

339 - SEOS_syscall モジュール アンロードの準備チェック

UNIX で該当

アクセス元が「secons –scl」コマンドを実行して、インターセプトされたシステム コールで実行中のプロセスがあるかどうかを確認していることを示します。CA Access Control は SEOS_syscall モジュールのアンロードを許可しません。

シャットダウン イベントの承認 stage code

シャットダウン イベントの承認 stage code は、CA Access Control がシャットダウン イベントに対して実行するアクションを決定するステージを示しています。

詳細情報:

シャットダウン イベント (P. 678)

451 - ユーザは OPERATOR です

シャットダウン シーケンスを実行したユーザが OPERATOR 属性を持っているため、CA Access Control がシャットダウン要求を許可したことを示します。

452 - ユーザは ADMIN または SPECIAL です

シャットダウン シーケンスを実行したユーザに ADMIN 属性が割り当てられているため、CA Access Control がシャットダウン要求を許可したことを示します。

453 - _seagent は CA Access Control をシャットダウンする権限があります

UNIX で該当

_seaqent は CA Access Control をシャットダウンする権限があるため、CA Access Control がシャットダウン要求を許可したことを示します。

460 - ユーザは CA Access Control をシャットダウンする権限がありません

要求しているユーザには CA Access Control をシャットダウンする権限がないため、CA Access Control がシャットダウン要求を拒否したことを示します。

600 — CA Access Control を終了しようとしています。

ユーザが kill コマンドを実行することにより、CA Access Control を終了しようとしたため、CA Access Control がシャットダウン リクエスト拒否したことを示します。

パスワード確認イベントの承認 Stage Code

パスワード確認イベントの承認 stage code は、CA Access Control がパスワード確認イベントに対して実行するアクションを決定するステージを示します。

詳細情報:

パスワード確認イベント (P. 681)

0 - パスワード品質が確認されました

ユーザがパスワードを正常に変更し、新しいパスワードがパスワード品質ルールをすべて満たしていることを示します。

1 - パスワードが短すぎます

新しいパスワードの長さがパスワード ポリシーの最低文字数を満たしていないため、パスワード変更が失敗したことを示します。

2 - パスワードにユーザ名が含まれています

新しいパスワードにユーザのユーザ名が含まれているため、パスワード変更が失敗したことを示します。

3 - パスワードに含まれる小文字の数が少なすぎます

新しいパスワードにパスワード ポリシーで定義された小文字の最低文字数が含まれていないため、パスワード変更が失敗したことを示します。

4 - パスワードに含まれる大文字の数が少なすぎます

新しいパスワードにパスワード ポリシーで定義された大文字の最低文字数が含まれていないため、パスワード変更が失敗したことを示します。

5 - パスワードに含まれる数字の数が少なすぎます

新しいパスワードにパスワード ポリシーで定義された数字の最低文字数が含まれていないため、パスワード変更が失敗したことを示します。

6 - パスワードのそのほかの文字が少なすぎます

新しいパスワードにパスワード ポリシーで定義されたそのほかの文字の最低文字数が含まれていないため、パスワード変更が失敗したことを示します。

7 - パスワードに同じ文字の繰り返しが多すぎます

新しいパスワードにパスワード ポリシーで定義された最低数を超えて同じ文字の繰り返しが含まれているため、パスワード変更が失敗したことを示します。

8 - 現在のパスワードと同じです

新しいパスワードが現在のパスワードと同じであるため、パスワード変更が失敗したことを示します。以前に使用していないパスワードを選択する必要があります。

9 - 以前に使用されたパスワードです。別のパスワードを選択します

新しいパスワードが以前に使用されたパスワードであるため、パスワード変更が失敗したことを示します。以前に使用していないパスワードを選択する必要があります。

10 - パスワードに含まれる英字の数が少なすぎます

新しいパスワードにパスワード ポリシーで定義された英字の最低文字数が含まれていないため、パスワード変更が失敗したことを示します。

11 - パスワードに含まれる英数字の数が少なすぎます

新しいパスワードにパスワード ポリシーで定義された英数字の最低文字数が含まれていないため、パスワード変更が失敗したことを示します。

12 - パスワードは最近変更されました。現在再び変更することはできません

パスワードが最近変更されて現在変更することができないため、パスワード変更が失敗したことを示します。パスワード ポリシーで定義されたパスワードの変更禁止期間の経過後にパスワードを変更する必要があります。

13 - パスワードが使用済みパスワードに含まれているか、使用済みパスワードを含んでいます

パスワードが使用済みパスワードに含まれているか、または使用済みパスワードを含んでいるため、パスワード変更が失敗したことを示します。新しいパスワードが使用済みパスワードに含まれていない、および使用済みパスワードを含んでいないことを確認する必要があります。

16 - パスワードが長すぎます

新しいパスワードがパスワード ポリシーで定義された最大文字数よりも長いため、パスワード変更が失敗したことを示します。

20 - パスワードが一致しません。

新しいパスワードが[パスワードの確認]フィールドに入力したパスワードと一致しないため、パスワード変更が失敗したことを示します。

21 - 定義済みの禁止文字を含めることはできません

新しいパスワードにパスワード ポリシーで定義された禁止文字が含まれているため、パスワード変更が失敗したことを示します。

22 - 以前に使用されたパスワードです

入力したパスワードが以前に使用されたパスワードであるため、CA Access Control がアクセスを拒否することを示します。使用する新しいパスワードがパスワード ポリシーに準拠していることを確認してください。

23 - パスワードが使用済みパスワードに含まれているか、使用済みパスワードを含んでいます

使用したパスワードが使用済みパスワードに含まれているか、使用済みパスワードが新しいパスワードに含まれているために、パスワード変更の試行が失敗したことを示します。以前に使用したパスワードを含まない新しいパスワードを選択する必要があります。

24 - パスワードが辞書ファイルに存在します

新しいパスワードが DICTIONARY クラスまたは DICTIONARY ファイルに定義されているため、パスワード変更が失敗したことを示します。DICTIONARY クラスまたは DICTIONARY ファイルに定義されていないパスワードを選択する必要があります。

100 - 不正な引数です

無効なデータが認証エンジンに送信されたため、パスワード変更が失敗したことを示します。

以下のいずれかが発生したときに、CA Access Control は監査ログにこのメッセージを書き込むことがあります。

- メモリ上の問題
- CA Access Control のさまざまなモジュールの、最新アップグレードまでのバージョン間の不一致

混在する CA Access Control 環境がないことと、クライアントとサーバが同じバージョンの CA Access Control を使用していることを確認する必要があります。 詳細については、当社テクニカル サポート（http://www.ca.com/jp/support/）にお問い合わせください。

ユーザのトレース メッセージの承認 Stage Code

ユーザのトレース イベントの承認 stage code は、CA Access Control がユーザ アクティビティ イベントに対して実行するアクションを決定するステージを示します。

詳細情報:

ユーザのトレース メッセージ (P. 683)

994 - 情報メッセージ

ユーザがトレース監査レコードにアクセスしたことを示します。

注: これは情報が含まれたメッセージのみであり、seaudit –tr コマンドの実行により表示されます。

995 - 内部リソースへのアクセスが許可されませんでした

アクセス元が内部的に保護された FILE リソースへの不正なアクセスを試行したことを示します。たとえば seos.audit レコードです。

996 - 内部リソースへのアクセスが許可されました

CA Access Control が内部的なバイパスによるリソースへのアクセスを許可したことを示します。例: reading /etc/passwd

997 - ユーザが setuid¥setgid ディレクトリを実行できます

（UNIX のみ）

アクセス元が setuid¥setgid フラグ ビットでマークされたディレクトリを実行しようとしたため、CA Access Control がイベントをバイパスしたことを示します。このステージは TRACE レコード メッセージの一部です。

998 - 許可は「Audit Mode Only」に設定されています

Windows のみ。

CA Access Control が「Audit Mode Only」で動作するように設定されていることを示します。

999 - リソースが保護されていません（ルールが存在するかどうか確認してください）

CA Access Control が保護されていないリソースへのアクセスを許可することを示します。

レコードを作成した理由を示す理由コード

レコードが作成された理由を示す理由コードは、CA Access Control がイベントに対して作成する監査レコードを決定するステージを示します。

0 - 操作をログに記録するよう要求されていません

操作をログに記録する特定の要求が存在しないため、CA Access Control はデフォルトでこの操作をログに記録したことを示します。

2 - ユーザ監査モードはログ記録を要求します

アクセス元の監査プロパティまたはそのプロファイルがレコードの結果と一致したため、CA Access Control が操作をログに記録したことを示します。たとえば、ユーザが AUDIT_MODE プロパティに FAILURE 値を設定して実行したアクションは、ユーザが保護されたリソースへのアクセスに失敗したときのみログに記録されます

3 - リソース監査モードはログ記録を要求しました

リソースの RAUDIT プロパティがレコードの結果と一致したため、CA Access Control が操作をログに記録したことを示します。

4 - 警告モードのリソース

WARNING プロパティがリソースまたはリソースのクラスに設定されたため、CA Access Control が操作をログに記録したことを示します。

5 - CA Access Control serevu ユーティリティは監査を要求しました

UNIX で該当

ユーザがログイン試行に失敗したときなど、serevu ユーティリティが監査レコードを要求したため、CA Access Control が操作をログに記録したことを示します。

7 - 送信接続レコード

UNIX で該当

正常な送信接続が発生したため、CA Access Control が操作をログに記録したことを示します。

8 - CA Access Control pam サポート UNIX がログインに失敗しました

UNIX で該当

ログイン パスワードの試行に失敗したときなど、PAM モジュールが監査を要求したため、CA Access Control が操作をログに記録したことを示します。

9 - CALENDAR クラスの日時の制約チェック

CALENDAR クラスの日時の制約チェックが監査レコードのログ記録を必要としたため、CA Access Control がこのメッセージをログに記録したことを示します。

10 - 操作をログに記録する特定の要求です

CA Access Control デーモンの強制終了の試行などの操作をログに記録する特定の要求のため、CA Access Control がこの操作をログに記録したことを示します。

11 - CA Access Control secons ユーティリティは監査を要求しました

UNIX で該当

Syscall モニタ オプションが sued である(secons-scl)ために、CA Access Control がこの操作をログに記録したことを示します。

監査ログの FILE レコードでの大文字の使用

Windows で該当

FILE クラス レコードの監査レコードは、CA Access Control のリリースによって監査ログで異なる形式で表示されます。

- すべての r5 および r8 リリースでは、ファイル パスが小文字で示されます。
- r12.0 および r12.0 SP1 では、オペレーティング システムがコンピュータ上のパスを表わすのと同じ方法で、ファイル パスが大文字になります。
- r12.5 以降では、CA Access Control FILE ルールに表されるのと同じ方法でファイル パスが大文字になります。

例: 監査ログの FILE レコードでの大文字の使用

以下の表は、CA Access Control のリリースごとに、監査ログに監査レコードがどのように表されるかを示しています。対象のファイル名は C:¥tmp¥TeSt.txt で、これに対して C:¥TMP¥TEST.txt という FILE レコードが作成されます。

リリース	監査ファイル内の表示形式
r5 と r8	C:¥tmp¥test.txt
r12.0 と r12.0 SP1	C:¥tmp¥TeSt.txt
r12.5 以降	C:¥TMP¥TEST.txt

付録 B: トレース メッセージ

このセクションには、以下のトピックが含まれています。

表記法

すべてのメッセージは、日時のプレフィクスで始まり、大文字で表記されたイベントタイプおよび「:」、「*!*」、または「>」などの記号がその後に示されます。以下に記号の意味を示します。

:

CA Access Control がイベントの発生を知らせるシグナルを受け取ったか、何らかのアクションを実行しました。

>

CA Access Control による認証の判断が *D*(拒否)、*P*(許可)、または *BYPASS*(アクセス ルールの解釈が不要なイベント。たとえば、現在の UID と同じ UID に対する setuid 要求など)という結果になりました。

!

CA Access Control が、エラー(不明プロセスからの要求など)を検出しました。

メッセージ

ここで説明するイベント引数の前には、前のセクションで説明した記号が付きます。

ACTION: CA Access Control が P=ppp を強制終了しました。

CA Access Control が setuid 要求またはログイン要求を拒否し、予防的手段として要求元プロセス(ppp)を強制終了(kill)しました。

ALARM ! UID uuu がシステムに侵入しました。

不明プロセスから fork、exec、setuid などの要求を受け取りました。この要求元プロセスは CA Access Control で認識できません。また、このプロセスには、システム内の他のどのプロセスにも設定されていない UID が割り当てられています。つまり、このユーザは CA Access Control に認識されずにログインしたことになります。このような状況が起きるのは、ソフトウェアのバグが原因である場合か、CA Access Control が現在のプロセス ステータスをスキャンした直後から初期化を完了する前までの間に、ユーザがログインした場合です。

APIAUTH ! P=ppp U=uuu ChangePasswd (user) エラー 0xerr

ユーザ *uuu* に関連付けられたプロセス *ppp* が、*user* のパスワードの変更を要求しました。この要求によりエラーが発生し、16 進数のエラー コードが返されました。semsgtool ユーティリティを使用してエラーの種類を確認してください。

APIAUTH ! P=ppp U=uuu CheckPasswd (user) エラー 0xerr

ユーザ *uuu* に関連付けられたプロセス *ppp* が、*user* の新しいパスワードの有効性チェックを要求しました。この要求によりエラーが発生し、16 進数のエラー コードが返されました。semsgtool ユーティリティを使用してエラーの種類を確認してください。

APIAUTH ! P=ppp U=uuu エラー、不明な API サービス nnn

CA Access Control プログラミング インターフェースがサポートしていないサービス コードが、アプリケーション インターフェースを通してプロセス *ppp* から渡されました。おそらくユーザ エラーが原因です。エラーの原因を調べて問題を修正し、再コンパイルしてください。

APIAUTH ! P=ppp U=uuu GeneralResourceProc エラー nnn >description

UID uuu で動作するプロセス ppp が一般リソースへのアクセスを要求しましたが、指定されたリソースを解決できませんでした。指定されたクラスが定義されていないか、指定されたアクセスが認証されていません。おそらくユーザ エラーです。コードを調べて修正し、再コンパイルしてください。

APIAUTH ! P=ppp U=uuu VerifyCreate は ROOT に対してのみ許可されます

UID uuu で動作するプロセス ppp が ACEE を作成するための VerifyCreate 要求を発行しました。この操作は、UID 0（root）に関連付けられたマルチユーザ プロセスに対してのみ許可されます。

指定したプロセスがマルチユーザ プロセスとして実行するプロセスである場合は、root 権限でプロセスを再実行してください。そうでない場合は、プロセスによってこの要求が発行された理由を確認してください。

APIAUTH : P=ppp U=uuu VerifyDelete は ROOT に対してのみ許可されます

UID uuu で動作するプロセス ppp が、ACEE を削除するための VerifyDelete 要求を発行しました。この操作は、UID 0（root）に関連付けられたマルチユーザ プロセスに対してのみ許可されます。

指定されたプロセスがマルチユーザ プロセスとして実行するプロセスである場合は、root 権限でプロセスを再実行してください。そうでない場合は、この要求が発行された理由を確認してください。

APIAUTH ! P=ppp U=uuu LoginProc エラー nnn >description

UID *uuu* で動作するプロセス *ppp* がユーザのログイン検証を要求しました。CA Access Control のログイン検証手続きは失敗しました。ベンダーのテクニカル サポート担当者に連絡してください。

APIAUTH ! P=ppp U=uuu NULL ACEE エラー VerifyCreate（ACEEH=hhh）

「サーバ」とマークされたユーザ プロセスが ACEE の作成要求を発行しました（おそらく、サーバ プロセスはアクセサのログインを処理していました）。結果は NULL ACEE であり、理由は以下のいずれかです。

- 指定されたユーザが CA Access Control データベースに定義されていません。
- VerifyCreate 要求の発行元から提供された情報が間違っています。
- 指定されたユーザにログインが許可されていません。

APIAUTH ! P=ppp U=uuu NULL ACEE エラー VerifyDelete (ACEEH=hhh)

ユーザ *uuu* に関連付けられたプロセス *ppp* (おそらく「サーバ」プロセスとしてマークされています) が、ACEE ハンドル *hhh* の削除を要求しました (この要求は、おそらくユーザのログオフの処理の一部です)。ただし、このハンドルに関連付けられた ACEE がないため、CA Access Control はこのハンドルを削除できませんでした。

APIAUTH : P=ppp U=uuu Request with ACEEH=1 > New ACEEH=hhh

UID *uuu* で動作するプロセス *ppp* が一般リソースへのアクセスを要求し、-1 の ACEE ハンドルを指定しました。CA Access Control は、要求元プロセスに関連付けられている ACEE ハンドルを使用しました。このメッセージは一般に、リソースへのアクセスを要求するシングル ユーザ プロセスです。特にアクションは必要ありません。

APIAUTH ! P=ppp U=uuu VerifyCreate (ACEEH=hhh) エラー nnn

UID uuu で動作するプロセス ppp が (ACEE を作成するための) VerifyCreate 要求を発行しました。VerifyCreate プロシージャの実行に失敗しました。ベンダーのテクニカル サポート担当者に連絡してください。

APIAUTH > P=ppp U=uuu VerifyCreate DENY (Result=[P/D/C]) string

以下のいずれかの理由で VerifyCreate 要求が拒否されました。

- 指定されたユーザは時間帯または曜日の制限ルールによりログインできない。
- ユーザは指定された端末から操作できない。
- 指定されたパスワードが間違っている (パスワードが入力された場合)。
- 続けて表示されるメッセージに示されたいずれかの理由。

APIAUTH > P=ppp U=uuu VerifyCreate (ACEEH=hhh) OK !

VerifyCreate 要求が許可されました。アクセサ環境エレメント (ACEE) は、ストレージに組み込まれています。CA Access Control によって、呼び出し元プログラムに ACEE ハンドル (ACEEH) が返されました。指定されたユーザが CA Access Control に対して定義されていない場合、この機能は -1 の ACEEH を返します。

APIAUTH ! P=ppp U=uuu VerifyDelete (ACEEH=hhh) [OK ! | エラー 0xerr]

ユーザ *uuu* に関連付けられたプロセス *ppp* (おそらく「サーバ」プロセスとしてマークされています) が、ACEE ハンドル *hhh* の削除を要求しました (この要求は、おそらくユーザのログオフの処理の一部です)。VerifyDelete 要求は承認されるか、またはエラーになります。エラーの場合は、err の前に 16 進数のエラーコードが表示されます。semsgtool ユーティリティを使用してエラーの種類を確認してください。

APIAUTH > P=ppp U=uuu VerifyRequest (ACEEH=hhh, C=ccc, R=rrr, A=nnn) DENY (Result='D') Why? detaileddenialreason

アクセス権 *xxx* が設定されたクラス *ccc* のリソース *rrr* へのアクセス要求が拒否されました。ACEEH が「-1」の場合は、ユニバーサル アクセス ルールに基づいてアクセスが拒否されました。ACEEH が「-1」以外の場合は、指定したハンドルに関連付けられたユーザに基づいてアクセスが拒否されました。2 行目には、拒否の理由についての詳しい説明が表示されます。

APIAUTH > P=ppp U=uuu VerifyRequest (ACEEH=hhh, C=ccc, R=rrr, A=xxx) PASS

アクセス権 *xxx* が設定されたクラス *ccc* のリソース *rrr* へのアクセス要求が許可されました。ACEEH が「-1」の場合 (ユーザが CA Access Control に定義されていない場合) は、リソースへのアクセスがユニバーサル アクセス ルールに基づいて許可されました。ACEEH が「-1」以外の場合は、指定したハンドルに関連付けられたユーザのアクセス ルールに基づいてアクセスが許可されました。

CONNECT : P=ppp U=uuu ACEEH=hhh ipip : port1 からソケット 6000 ホスト=iiii

UID *uuu* に関連付けられたプロセス *ppp* がホスト *iiii* (X 端末または端末) 上でウィンドウを開く要求を発行しました。

注: ポート番号は常に 6000 です。その他の TCP/IP 接続要求は CA Access Control によって無視されます。

CONNECT > P=ppp U=uuu ipip : port1 からソケット 6000 ホスト =iiii BYPASS

プロセス *ppp* で実行しているプログラムが登録済みの XDM プログラムであったため、CA Access Control はアクセス ルールを解釈せずに CONNECT 要求を無視しました。

CONNECT >Result: [P/D/C] P=ppp ACEEH=hhh TERM=ttt Why? detaileddecisiontext

CONNECT の結果は *D*(拒否)または *P*(許可)です。2 行目に、理由についての詳しい説明が表示されます。

エラー : fork できません。エラー番号 nnn。

初期化時に、CA Access Control は数回の分岐(fork)を経てデーモンになります。fork 要求が失敗しました。エラーの原因は、エラー番号で表示されます。

問題の原因を特定できない場合は、ベンダーのテクニカル サポート担当者に連絡してください。

エラー : CA Access Control エージェントの実行に失敗しました。ddd

Engine は Agent デーモンを起動できません。seagent 実行可能ファイルが適切な場所(通常は *ACInstallDir*/bin/seagent)にあるかどうか確認してください。このファイルが適切な場所にある場合は、ベンダーのテクニカル サポート担当者に問題をレポートしてください。メッセージ テキスト内の *ddd* は、seagent の実行を試みた際に、CA Access Control がオペレーティング システムから受け取ったエラー番号です。

エラー : ログイン プログラム エラーのメモリを取得できませんでした。エラー! NFS デバイスのメモリを取得できませんでした。エラー! PRIV プログラムのメモリを取得できませんでした。エラー! XDM プログラムのメモリを取得できませんでした。

これらのメッセージは、メモリが著しく不足していることを意味します。使用しているコンピュータが CA Access Control を実行するためのメモリの必要条件を満たしていないか、ソフトウェアにバグがあります。ベンダーのテクニカル サポート担当者に連絡してください。

エラー : PROC テーブルのメモリを取得できませんでした。

seosd は、起動時にすべての実行中プロセスをスキャンし、各プロセスについて必要な情報をすべて取得する必要があります。このスキャンを実行するためのメモリの割り当てに失敗したため、seosd は終了します。これは、メモリが大幅に不足していることが原因です。

エラー : ログイン プログラムの登録に失敗しました: programname

起動時に、CA Access Control はログイン プログラムとして扱うすべての実行可能ファイルを登録します。ログイン プログラムのリストは、各オペレーティング システム環境の CA Access Control コードに定義されます。

起動時に、指定された *programname* がファイル システムで見つかりませんでした。CA Access Control はこのプログラム無視し、起動プロセスを続行します。

エラー : 特権プログラムの登録に失敗しました: programname

起動時に、CA Access Control は特権プログラムとして扱うすべての実行可能ファイルを登録します。起動時に、指定された *programname* がファイル システムで見つかりませんでした。CA Access Control はこのプログラム無視し、起動プロセスを続行します。

特権プログラムのリストは、各オペレーティング システム環境の CA Access Control コードに定義されます。

エラー : XDM プログラムの登録に失敗しました: programname

起動時に、CA Access Control は XDM プログラムとして扱うすべての実行可能ファイルを登録します。XDM プログラムのリストは、各オペレーティング システム環境の CA Access Control コードに定義されます。

起動時に、指定された *programname* がファイル システムで見つかりませんでした。CA Access Control はこのプログラム無視し、起動プロセスを続行します。

エラー: FileDb リスト用のメモリがありません。

起動時に、seosd は保護対象ファイルのリストを保持するためのメモリの割り当てに失敗しました。おそらくメモリが大幅に不足していることが原因です。seosd デーモンは終了します。

エラー : GroupDb リスト用のメモリがありません。エラー : HostDb リスト用のメモリがありません。 エラー : ServDb リスト用のメモリがありません。エラー : UserDb リスト用のメモリがありません。

これらのメッセージは、メモリが著しく不足していることを意味します。使用しているコンピュータに CA Access Control を実行するのに必要なメモリがないか、ソフトウェアにバグがあります。ベンダーのテクニカル サポート担当者に連絡してください。

エラー : PreMatureExec。FORK Child=ppp Parent=PPP を予測しています。

このメッセージは、プロセス ID (*ppp*) が EXEC システム コールを発行したが、このコールを seosd が認識できないことを示しています。通常、このようなメッセージは、EXEC 要求に先行する FORK システム コールがまだ seosd に通知されていないことを意味します。UNIX カーネルに対する CA Access Control の拡張機能である SEOS_syscall が維持するシリアライゼーション ロックに問題がある可能性があります。

メッセージ テキストの *ppp* が seagent の PID である場合は、このメッセージを無視できます。同じメッセージが何度も表示される場合は、ベンダーのテクニカル サポート担当者に問題をレポートしてください。

エラー : P=ppp 実行に失敗しました。

CA Access Control は EXEC イベントを受信しましたが、実行可能ファイルの i-node 番号は 0 でした。このメッセージは、#! シェル プログラムの宣言行が先頭に含まれていないスクリプト ファイルを起動する場合に表示されます。何も行う必要はありません。

エラー : CA Access Control ファイル テーブルの設定に失敗しました

seosd がファイル テーブル (CA Access Control のすべての保護対象ファイルを示すテーブル) の設定を試みましたが、この要求は SEOS_syscall によって拒否されました。最も可能性の高い原因は、カーネルのメモリ不足、または seosd と SEOS_syscall のバージョンの不整合です。CA Access Control によるファイル保護機能は正常に動作を続行することができません。

可能な場合は、バージョンの不整合を解消してください。上記のような問題がない場合は、ベンダーのテクニカル サポート担当者に連絡してください。

エラー : seosini_ShutDown rv=errorno

CA Access Control の停止中にエラーが発生しました。ベンダーのテクニカル サポート担当者にエラーをレポートしてください。

エラー : 一般的な「パス」文字列です

ファイルの保護のために包括的なルールを定義しようとしました。newfile コマンドまたは newres FILE コマンドが使用された可能性があります。ただし、指定されたパスは、包括的なファイル アクセス ルールに使用することはできません。ファイル ルールが定義されていません。

エラー : 不明な要求 : タイプ : ttt、Pid=ppp、Buff=bbb

CA Access Control がシステム コールから要求を受け取りましたが、要求タイプ *ttt* を認識できません。CA Access Control のシステム コールと seosd のソフトウェア バージョンの不整合か、ソフトウェアのエラーが原因です。要求の発行元はプロセス *ppp* で、*bbb* は要求バッファの出力です。ベンダーのテクニカル サポート担当者に問題を報告してください。

EXEC : P=ppp U=uuu G=ggg (D=ddd I=iii) Pgm:ProgramName [Attached to: ipaddress]

CA Access Control が UID *uuu* および GID *ggg* に関連付けられたプロセス *ppp* からプログラム実行イベントを受け取りました (ggg の値が「-1」の場合は、そのプロセスの GID が CA Access Control に登録されていないことを示します)。メッセージ テキストの *ddd* と *iii* はそれぞれ、ファイルのデバイス番号と i-node を表します。*Program-Name* は、プログラムの起動に使用されるゼロ引数です。指定されたプログラムは通常のプログラムです (つまり、setuid または setgid ではありません)。したがって、CA Access Control は、データベース アクセス ルール決定メカニズムを呼び出さずに、プログラムの実行を許可します。プロセスが関連付けられている *ip-address* が取得可能な場合は、メッセージ テキストにその IP アドレスが表示されます。

EXEC sg : P=ppp U=uuu G=ggg (D=ddd I=iii) Pgm : ProgramName[Attached to: ipaddress]

CA Access Control が UID *uuu* および GID *ggg* に関連付けられたプロセス *ppp* からプログラム実行イベントを受け取りました (*ggg* の値が「-1」の場合は、そのプロセスの GID が CA Access Control に登録されていないことを示します)。メッセージ テキストの *ddd* と *iii* はそれぞれ、ファイルのデバイス番号と i-node を表します。*Program-Name* は、プログラムの起動に使用されるゼロ引数です。指定されたプログラムは setgid プログラムです。したがって、CA Access Control は、データベース アクセス ルール決定メカニズムを呼び出して、プログラムの実行を許可するかどうかを決定します。プロセスが関連付けられている *ip-address* が取得可能な場合は、メッセージ テキストにその IP アドレスが表示されます。

EXECsu: P=ppp U=uuu G=ggg(D=ddd I=iii)Pgm: ProgramName[Attached to: ipaddress]

CA Access Control が UID *uuu* および GID *ggg* に関連付けられたプロセス *ppp* からプログラム実行イベントを受け取りました (*ggg* の値が「-1」の場合は、そのプロセスの GID が CA Access Control に登録されていないことを示します)。メッセージ テキストの *ddd* と *iii* はそれぞれ、ファイルのデバイス番号と i-node を表します。*Program-Name* は、プログラムの起動に使用されるゼロ引数です。指定されたプログラムは setuid プログラムです。したがって、CA Access Control は、データベース アクセス ルール決定メカニズムを呼び出して、プログラムの実行を許可するかどうかを決定します。プロセスが関連付けられている *ip-address* が取得可能な場合は、メッセージ テキストにその IP アドレスが表示されます。

EXECsusg: P=ppp U=uuu G=ggg(D=ddd I=iii)Pgm: ProgramName[Attached to: ipaddress]

CA Access Control が UID *uuu* および GID *ggg* に関連付けられたプロセス *ppp* からプログラム実行イベントを受け取りました (*ggg* の値が「-1」の場合は、そのプロセスの GID が CA Access Control に登録されていないことを示します)。メッセージ テキストの *ddd* と *iii* はそれぞれ、ファイルのデバイス番号と i-node を表します。*Program-Name* は、プログラムの起動に使用されるゼロ引数です。指定されたプログラムは setuid および setgid プログラムです。したがって、CA Access Control は、データベース アクセス ルール決定メカニズムを呼び出して、プログラムの実行を許可するかどうかを決定します。プロセスが関連付けられている *ip-address* が取得可能な場合は、メッセージ テキストにその IP アドレスが表示されます。

EXEC > P=ppp U=uuu(R=rrr E=eee S=sss)to(E=EEE)BYPASS

プログラムは setuid、setgid、またはその両方であるため、アクセス ルール決定メカニズムを呼び出して実行を許可するかどうか判断する必要があります。ただし、ファイル *EEE* の所有者が現在の有効な UID(*eee*)の所有者と同一であったため、CA Access Control はこのチェックを省略しました。プログラムの実行によってプロセスの権限の適用範囲を変更することはできません。データベースで trusted プログラムとして定義されているプログラムが変更または何らかの方法で改ざんされた場合、そのプログラムの実行は許可されません。

EXEC > Result: 'R' [stage=sss gstag=ggg ACEEH=hhh rv=rc]Why? detaileddecisiontext

CA Access Control がユーザのプログラム実行権限をチェックした結果は *R* でした。*R* は D(拒否)または P(許可)のいずれかです。段階 *sss* と許可段階 *ggg* は、結果を特定した決定フローのフェーズを示します。プログラムに対するアクセサとして、ACEE ハンドル *hhh* が使用されました。結果が「C」(チェック)の場合は、CA Access Control で決定が行われなかったことを意味します。この場合は、ソフトウェア エラーが原因と考えられるので、ベンダーのテクニカル サポート担当者に連絡して、戻り値 *rc* をレポートしてください。*Detailed-Decision-text* は、段階および許可段階についての説明です。結果が *P* の場合、プログラムは正常に実行されます。結果が *D* の場合、プログラムは実行されず、ユーザはプログラムの実行拒否メッセージを受け取ります。

EXECARGS:「実行引数」

EXEC syscall により、CA Access Control では、実行されたコマンド ラインと渡されたすべての引数が表示されます。

EXIT :終了しています...

CA Access Control がシャットダウン プロセスを開始しました。システム コールのインターセプトは無効になります。

致命的 ! seosrt_InitDatabase(nnn)内 Layer = nnn Stage = nnn Return Code = 0xnnn

CA Access Control が、データベース I/O ルーチンの初期化に失敗しました。以下の原因が考えられます。

- seos.ini ファイルの dbdir トークンで識別されるディレクトリに CA Access Control データベースが存在しません。
- CA Access Control を起動するユーザが root ユーザではありません。
- データベースが壊れています。

問題を修正できない場合は、ベンダーのテクニカル サポート担当者に連絡してください。

FILE : P=ppp U=uuu(D=dev I=inode)acc : pathname

ユーザ ID *uuu* に関連付けられたプロセス *ppp* が、CA Access Control の保護ファイルにアクセスを試みました。メッセージ テキストの *dev* および *inode* は、アクセス先ファイルのデバイスおよび i-node です。*acc* はアクセス モード(READ、WRITE など)、*pathname* はアクセス先ファイルの実際のパス名を表します。

FILE > Result 'D' CA Access Control File Only 'filename'

このファイルにアクセスできるのは CA Access Control のみであるため、ファイルへのアクセス結果は D(拒否)です。アクセス ルールでアクセスが許可されていても、CA Access Control ではこのファイルへのアクセスを拒否するようにハードコードされています。

FILE > Result: 'R' [stage=sss gstag=gs ACEEH=hhh rv=rv(recordname)Why? detailedreasontext

ファイルへのアクセス要求の結果 R は、D (拒否)または P(許可)のいずれかです。段階 *sss* と許可段階 *gs* は、2 行目の(「理由」の後の)テキスト文字列の理由にマッピングされます。メッセージ テキストの *hhh* は、要求元アクセサに関連付けられたアクセサ ハンドルであり、*record-name* はアクセスの拒否または許可を決定するアクセス ルール レコードの名前です。

FORK : P=ppp U=uuu G=ggg Child=cppp Pgm: ProgramName

CA Access Control が、UID *uuu* および GID *ggg* に関連付けられたプロセス *ppp* からの fork 要求をインターセプトしました。子プロセス ID は *cppp* です。*Program-Name* は、親プロセスで実行中(かつ、最初は子プロセスでも実行中)のプログラムを示します。CA Access Control は fork 要求を拒否しないため、fork 要求は必ず許可されます。vfork や kfork などのさまざまな fork システム コールも fork 要求としてレポートされます。

GETCRED: P=ppp、チケットによるクレデンシャルを取得します。

これは通知のみを行うメッセージであり、*ppp*(通常は Policy Model デーモンである sepmdd のプロセス ID)が特定のチケット ホルダ(sepmdd のサービスを要求したクライアント プロセス)の認証を要求したことを示します。詳細については、この付録の GTICKET の説明および「ユーティリティの詳細」の sepmdd の説明を参照してください。

GPEERNAM: P=ppp, ADDR=addr, N=desc

CA Access Control が、現在のプロセスに関連付けられている IP アドレスを確認するための getpeername() システム コールをインターセプトしました。このシステム コールは常に許可されます。メッセージ テキストの *ppp* は、getpeername() コールの発行元プロセスの ID を示し、*addr* はソケット記述子 *desc* に関連付けられた IP アドレスを示します。

GTICKET: P=ppp、認証チケットを取得します。

これは通知のみを行うメッセージであり、*ppp* が seosd に対して認証チケットの発行を要求したことを示します。Policy Model クライアント(sepmd)が sepmdd と通信するたびに、サーバは渡されたチケットを通じてクライアントの身元を確認します。クライアントは、ソケット通信を使用して、取得したチケットをサーバに送信します。次に、サーバはこのチケットを seosd に渡し、GETCRED 要求を発行して、そのチケット フォルダのクレデンシャルを取得します。sepmdd は、この方法でサービスの要求元クライアントの身元を確認します。

INET : P=ppp ipaddress: localport からポート portnumber

CA Access Control は、TCP/IP サービス *port-number* を要求するリモート *ip-address* によって発行されたインターネット着信要求をインターセプトしました。

INET > Result: 'R' ipaddr>locport, stg=stage gtsg=gstageWHY ? DetailedReasonText

インターネット要求の結果 *R* は P(許可)または D(拒否)です。メッセージ テキストの *ip_addr* は、要求の IP アドレスです。*Detailed-Reason-Text* は、決定フローのどの段階および許可段階で、要求元ホストに TCP/IP サービスを拒否または許可する最終決定が行われたのかを説明します。

INFO : AutoDisabling Tracedue to tight fsspace(space)

トレース ファイルが保存されているファイル システム内の空き容量が、seos.ini ファイルの trace_space_saver トークンで指定されたしきい値を下回ると、トレース機能は自動的に無効になります。メッセージ テキストの *space* は、ファイル システムの空き容量を示します。

INFO ：空き容量を取得できません（エラー番号 =err）

トレース機能の自動無効化機能が、ファイル システムの空き容量を判断できません。メッセージ テキストの *err* は、UNIX の statfs() 呼び出しから返された整数のエラー番号です。ベンダーのテクニカル サポート担当者に問題を報告してください。

INFO ：DB クエリ

seosd デーモンが、データベースから情報を取得する要求を受け取りました。

INFO ：DB 要求

seosd デーモンが、CA Access Control データベースのデータの変更要求またはクエリ要求を受け取りました。

INFO ：フィルタ マスク：「mask」が登録されています。

trcfilter.init ファイルから読み込まれる各フィルタ マスクが seosd デーモンによって登録され、マスクに一致するメッセージはトレース ファイルに送られません。

INFO ：GroupList に nnn 個のエントリが登録されています。

NIS サーバ環境で実行する seosd の起動時に、（/etc/group および NIS マップからの）すべてのグループ エントリがキャッシュされるため、ypserv プロセスおよび TCP/IP 要求を呼び出さずに GID をグループ名に変換できます。このメッセージは、seos.ini ファイルの under_NIS_server トークンが YES に設定されていることも意味します。CA Access Control を実行している端末が NIS サーバ以外の場合は、under_NIS_server トークンを「NO」に設定します。メッセージ テキストの *nnn* は、キャッシュされたグループ エントリの数を示します。

INFO ：HostList に nnn 個のエントリが登録されています。

seosd デーモンは、起動時に /etc/hosts からのすべてのエントリをキャッシュします。メッセージ テキストの *nnn* は、キャッシュされたホスト エントリの数を示します。

INFO　: ログイン プログラム: programnam が登録されています。

seosd デーモンは、ユーザがシステムにログインする際に使用するすべてのプログラムを認識する必要があります。CA Access Control では、ログイン プログラムによって起動された setuid システム コールは setuid 要求ではなく、ログイン要求として扱われます。メッセージ テキストの *programname* は、登録されているログイン プログラムの完全パスです。seosd デーモンは、CA Access Control のスタートアップ コードからログイン プログラムの名前を内部的に取得します。

INFO　: NFS Device Majors が登録されました。nnn 個のエントリがあります。

trusted プログラムに対して Watchdog が実行するチェックには、ファイルが存在するデバイス番号のチェックも含まれます。NFS がマウントされたファイル システム(特に自動マウントされたファイル システム)では、ブート後にデバイス番号の値が変わる可能性があるため、これらのファイル システム上にファイルがあると、このチェックでエラーが生じる場合があります。このため、CA Access Control では、変更される可能性のあるマイナー デバイス番号を無視できるように、NFS ファイル システムのメジャー デバイスが登録されます。CA Access Control には、各環境について、NFS がマウントされたファイル システムのメジャー デバイス番号のリストがあります。ご使用のネットワーク マウント ファイル システムが CA Access Control で認識されない場合は、ベンダーのテクニカル サポート担当者にリストへのメジャー デバイス番号の追加について問い合わせてください。メッセージ テキストの *nnn* は、NFS にマウントされたファイル システムとして登録されているメジャー デバイス番号の数です。

INFO　: P=ppp が終了しました

プロセス *ppp* が終了しました。seosd は、その ACEE(アクセサ環境エレメント)から、このプロセス番号の関連付けを解除します。プロセス *ppp* がその ACEE に関連付けられた最後のプロセスであった場合(つまり、同じ環境を使用する他の親プロセスやサブプロセスがない場合)、ACEE はストレージから削除されます。このメッセージは、プロセスの終了直後に表示されるのではなく、CA Access Control が内部テーブルのプロセス エントリを再利用するために何らかの「ガベージ コレクション」を実行したときにのみ表示されます。

INFO : P=ppp 実行に失敗しました

このメッセージは、(CA Access Control が実行を許可した後で) UNIX が要求を拒否したため、プロセス *ppp* が最後の EXEC syscall の実行に失敗したことを示します。したがって、CA Access Control は、このプロセスに関連付けられていた以前の実行可能ファイルの値を、このプロセス ID で実行中のプログラムとして復元します。ほとんどの場合、プロセスは終了します。これは必ずしもエラーではないので、特にアクションは必要ありません。ただし、UNIX ツールを使用して、実行が失敗した原因を特定する必要があります。ほとんどの場合、シェル スクリプトの先頭行に「#!/bin/sh」というヘッダがないことが原因です。

INFO : P=ppp 不明な TTY タイプ typename です

seosd デーモンは、プロセス *ppp* が実際の TTY または擬似 TTY を使用しているかどうかを判断できません。ベンダーのテクニカル サポート担当者に連絡してください。

INFO : 特権プログラム: programname が登録されています。

seosd デーモンにより、いくつかの特権プログラムが登録されます。特権プログラムは、SURROGATE クラスをチェックせずに、任意のユーザに対して setuid を実行することができます。現時点では、フローの要件により、特権プログラムに指定できるのは /bin/sendmail のみです。特権プログラムの数はできるだけ少なくする必要があります。seoswd で、すべての特権プログラムを監視し、プログラムの信頼性を確認することをお勧めします。メッセージ テキストの *programname* は、登録されているプログラムの完全パスです。

INFO : Restricted File Table Set に nnn 個のエントリがあります

seosd の起動時には、CA Access Control の保護ファイルについて *nnn* 個のエントリが検出され、このリストは UNIX カーネルに対する CA Access Control の拡張機能に渡されました。これは通知のみのメッセージです。

INFO : SEOS_syscall の登録を解除します。rc=nnn

seosd は、シャットダウン後に再起動できるように、シャットダウン中にカーネルから登録を解除します。メッセージ テキストの *nnn* はリターン コードであり、0 と表示されます。リターン コードが 0 以外の場合は、ベンダーのテクニカル サポート担当者に連絡してください。

INFO　: ServList に nnn 個のエントリが登録されています。

seosd デーモンは起動時に /etc/services からのすべてのエントリをキャッシュします。*メッセージテキスト*の nnn は、キャッシュされたホスト エントリの数を示します。

INFO　: サービス リストに nnn 個の portmapper エントリが登録されています ServList に nnn 個の portmapper エントリが登録されています。

seosd の起動時に、portmapper によって解決される nnn 個の TCP/IP サービスが登録されました。これは通知のみのメッセージです。

INFO　: サイトの設定

seagent デーモン（CA Access Control の他の端末との通信を処理する CA Access Control デーモン）が、リモート端末からの接続要求を seosd に送信しました。

INFO　: PV を設定しています。C=%s O=%s P=%s

seoswd デーモンにより、クラス *ccc* のオブジェクト *ooo* にプロパティ *ppp* の値が設定されます。

INFO　: UserList に nnn 個のエントリが登録されています。

NIS サーバ環境で実行する seosd の起動時に、（/etc/passwd および NIS マップからの）すべてのユーザ エントリがキャッシュされるため、ypserv プロセスおよび TCP/IP 要求を呼び出さずに、UID をユーザ名に変換できます。このメッセージは、seos.ini ファイルの under_NIS_server トークンが YES に設定されていることも意味します。CA Access Control を実行しているコンピュータが NIS サーバ以外の場合は、seos.ini の under_NIS_server トークンを NO に設定します。メッセージ テキストの *nnn* は、キャッシュされたユーザ エントリの数を示します。

INFO　: XDM プログラム: programname が登録されています

XDM プログラムは、X 端末でユーザ ID およびパスワード ボックスを表示するプログラムです。XDM プログラムは *superuser* 権限で実行しますが、通常、この権限では X 端末でウィンドウを開くことはできません。しかし、XDM プログラムは、ユーザが指定するユーザ ID およびパスワードを示すボックスを表示するために X 端末のウィンドウを開く必要があります。したがって、CONNECT 要求の発行元プログラムが XDM プログラムとして登録されている場合は、seosd による端末チェックが省略されます。

KILL : P=ppp U=uuu が [Process | All Except] (nn) を強制終了(kill)します:(proclist)

ユーザ *uuu* に関連付けられたプロセス *ppp* が、*proclist* 内のすべてのプロセス(またはリスト内のプロセスを除くすべてのプロセス)の強制終了(kill)を試みました。メッセージ テキストの *nn* は、ターゲット プロセスの数を示します。

KILL > Result 'R' [stage=sss gstag=gs rv=rr] ACEEH=hhhWhy? detailedreasontext

kill イベントの結果 R は P(許可)または D(拒否)です。メッセージ テキストの *sss*、*gs*、および *rr* は、CA Access Control の決定ルーチンの段階、許可段階、および戻り値を示し、*hhh* は kill イベントに関連付けられたアクセサ ハンドルを示します。2 行目に表示される *detailed-reason-text* は、stage code および許可 stage code の結果を示します。

LOGIN : P=ppp User=uuu Terminal=ttt

seosd デーモンが、プロセス番号 *ppp* で、端末 *ttt* に対して操作を行っているユーザ *uuu* からのログイン要求をインターセプトしました。このメッセージの後にログイン結果メッセージが表示されます。

LOGIN >Result: 'R' [stage=stage gstag=gstage rv=nnn] ACEEH=hhh[Why? detaileddenialreason]

ログイン要求の結果 R は P(許可)または D(拒否)です。メッセージ テキストの *stage* および *gstage* は、ログイン要求の許可または拒否の決定を行う CA Access Control のフローの段階を示す番号です。ログインが許可された場合、*hhh* は発行元プロセスに関連付けられた ACEE ハンドルとなります。ログインが拒否された場合、*hhh* は「-1」に設定され、2 行目に *detailed-denial-reason* が表示されます。*detailed-denial-reason* にリソースへのアクセスに関連するメッセージが表示された場合(「リソースへのアクセスを許可するルールがありません」など)、問題のリソースは、ユーザがログイン要求を発行した端末を意味します。

LOGIN > Result: 'D' すべてのログインが無効です

現在、すべてのユーザに対してログインが無効になっているため、ログイン要求は拒否されました。

LOGIN > Result: 'D' U=uuu に対するログインが無効です

特定のユーザに対してログインが無効になっているため、ログイン要求は拒否されました。そのユーザはすでにログインしている可能性があります。

MESSAGE: string

コンソール要求により、トレース ファイルにマーカ メッセージが書き込まれます。

NEWPASS: 新規パスワードの設定

sepass ユーティリティが、ユーザ ID に新しいパスワードを設定するように要求しました。

PW_ATTCK: P= ppp が nnn 回の試行を sss 秒間に端末から行いました

登録されているいずれかのログイン プログラムを実行中のプロセス *ppp* がユーザとパスワードの組み合わせを *nnn* 回試みて、ログインに失敗したことが seosd デーモンにより検出されました。CA Access Control では、メッセージ テキストに指定された端末からパスワードを推測する攻撃が行われたものと判断され、CA Access Control 監査ファイルに監査レコードが書き込まれました。PWATTACK 監査レコードが作成されると、ログ ルーティング デーモン(selogrcd および selogrd)によるアクションが実行される場合があります。

RESTART: Watchdog によって DBSERV が再起動されました(P=ppp)

seoswd デーモンが seosd を再起動しました。メッセージ テキストの *ppp* は、seosd のプロセス ID です。

SCONSOLE: 以下の UID のログインが無効です: uuu

CA Access Control のコンソール ユーティリティ(secons)が、ユーザ ID *uuu* のログイン要求を無効化する要求を発行しました。これ以降、指定されたユーザ ID からのログイン要求は拒否されます。

SCONSOLE: U=uuu のログインはすでに無効になっています

secons ユーティリティが、ユーザ ID *uuu* に対するログイン要求の無効化を要求しました。ただし、このユーザ ID についてはすでにログインが無効になっています。

SCONSOLE: U=uuu のログインは無効ではありません

secons ユーティリティが、ユーザ ID *uuu* についてログインを再び有効にするように要求しました。ただし、このユーザ ID についてはすでにログインが有効になっています。

SCONSOLE: 現在ログインは無効です

secons ユーティリティが、すべてのユーザについてログインの無効化を要求しました。これ以降、すべてのユーザのログイン要求は拒否されます。

SCONSOLE: 現在ログインは有効です

secons ユーティリティが、すべてのユーザについてログインの無効化を要求しました。これ以降、ログイン要求は許可されます。

SCONSOLE: U=uuu のログインは再度有効になっています

secons ユーティリティが、指定したユーザのログインを再び有効にするように要求しました。これ以降、この特定のユーザのログイン要求は許可されます。

SCONSOLE: 無効ログイン テーブルに空き容量がありません

secons ユーティリティが、特定のユーザについてログインの無効化を要求しました。ただし、ログイン無効テーブルがいっぱいになっています。ベンダーのテクニカル サポート担当者に連絡してください。

SCONSOLE: U=uuu は操作を行う権限がありません

OPERATIONS 属性を持たないユーザが、OPERATIONS ユーザ以外には使用が許可されない secons スイッチを使用しようとしました。

SCONSOLE: U=uuu には U=uuu2 のログインを無効にする権限がありません

ユーザ *uuu* が secons を使用して、ユーザ *uuu2* のログインを無効にしようとしました。ただし、*uuu2* のログインを無効にできるのは、root ユーザおよび *uuu2* のみです。

SCONSOLE: U=uuu には U=uuu2 のログインを再度有効にする権限がありません

ユーザ *uuu* が secons を使用して、ユーザ *uuu2* のログインを有効にしようとしました。*uuu2* のログインを再度有効にできるのは、root ユーザおよび *uuu2* のみです。

SETGRPS: P=ppp to grouplist

プロセス *ppp* が、*grouplist* に指定されたグループに対して setgroups システム コールを発行しました。

SGID : P=ppp U=uuu G=ggg to GGG (GROUP.groupname) ACEEH=hhh D=devnum I=inode

UID *uuu* および GID *ggg* の権限で実行するプロセス *ppp* が GID *GGG* に対して setgid システム コールを発行しました。CA Access Control は、SURROGATE クラスおよびオブジェクト *GROUP.groupname* を使用してそのプロセスの権限をチェックし、その要求のアクセサ ハンドルとして *hhh* を使用します。メッセージ テキストの *devnum* および *inode* は、発行元プログラムのデバイスおよび i-node を示します。このメッセージの後に「SGID Result」メッセージが表示されます。

SGID > P=ppp U=uuu (RG=rg EG=eg SG=sg) to (RG=trg EG=teg SG=tsg) ()BYPASS

CA Access Control によって、setgid 要求が SURROGATE アクセス ルールのチェックなしに許可されました。メッセージ テキストの *ppp* は発行元プロセスの ID であり、*uuu* はこのプロセスに関連付けられたユーザ ID です。*rg*、*eg*、および *sg* は、そのプロセスの実際の GID、有効な GID、および保存されている GID です。*trg*、*teg*、および *tsg* は、setgid 要求の発行に使用されたターゲットの有効な GID、実際の GID、および保存されている GID です。チェックが省略される理由は、現在の実際の GID または保存されている GID がターゲット GID と同じであり、setgid 要求が実行されてもユーザのセキュリティ範囲が変化しないためです。

SGID > Result: 'R' [stage=stage gstag=gstage ACEEH=hhh]Why? detailedreasontext

CA Access Control により、setgid 要求が SURROGATE アクセス ルールと照合されました。結果 R は P (許可) または D (拒否) です。この判断はアクセサ ハンドル *hhh* に代わって行われました。メッセージ テキストの *detailed-reason-text* は、拒否または許可の理由を示します。

SHUTDOWN! **要求が拒否されました。U=uuu はサーバをシャットダウンする権限がありません**

ユーザ ID *uuu* が secons を使用して seosd を停止しようとしましたが、このユーザのプロファイルには OPERATIONS 属性が割り当てられていません。したがって、要求は拒否されました。

SHUTDOWN: **オペレータの要求により、サーバをシャットダウンしています。**

権限のあるオペレータからの要求を受けて、seosd デーモンがシャットダウンを開始しました。

SHUTDOWN: CA Access Control デーモン daemonname を終了しています。P=ppp RV=nnn

CA Access Control は、シャットダウン プロセスの一部として、デーモン *ppp* を終了しました。また、CA Access Control は seoswd および seagent も終了します。

STARTUP: CA Access Control デーモン PID=ppp

seosd デーモンが起動しました。そのプロセス ID は *ppp* です。

STREAM c: P= ppp がストリーム Id=iii を閉じます

プロセス *ppp* がストリーム ID *iii* を持つストリームを閉じました。CA Access Control はストリームの開閉操作をすべて追跡し、後で特定のストリーム ID を持つプロセスに代わって TCP/IP 要求が処理されるときに、そのストリームを所有するプロセスのプロセス ID を決定します。

STREAM o: P=ppp がストリーム Id=iii を開きます

プロセス *ppp* がストリーム ID *iii* を持つストリームを開きました。CA Access Control はストリームの開閉操作をすべて追跡し、後で特定のストリーム ID を持つプロセスに代わって TCP/IP 要求が処理されるときに、そのストリームを所有するプロセスのプロセス ID を決定します。

SUID > P=ppp U=uuu(R=r E=e S=s)to(R=tr E=te S=ts)(reason)BYPASS

CA Access Control によって、setuid 要求が SURROGATE アクセス ルールのチェックなしに許可されました。メッセージ テキストの *ppp* は発行元プロセスの ID で、*uuu* はこのプロセスに関連付けられたユーザ ID です。*r*、*e*、および *s* は、このプロセス *ppp* の実際の UID、有効な UID、および保存されている UID です。*tr*、*te*、および *ts* は、setuid 要求が発行されたターゲットの有効な UID、実際の UID、および保存されている UID です。チェックが省略される理由は、現在の実際の UID または保存されている UID がターゲット UID と同じであり、setuid 要求が実行されてもユーザのセキュリティ範囲が変化しないためです。その他に考えられる理由としては、setuid システム コールの発行元プログラムが特権プログラムであること(この場合、*reason* は For Priv)、または発行元プログラムが実際のログインの前後に UID を数回変更するログイン プログラムであること(この場合、*reason* は For Login)があります。

SUID : P=ppp U=uuu(R=r E=e S=s)to USER.username(R=tr E=te S=ts)D=devnum I=inode

ユーザ ID *uuu* の権限で実行中のプロセス *ppp* が、現在の実際の UID、有効な UID、または保存されている UID を UID *uuu* に変更する setuid システム コールを発行しました。CA Access Control は、この要求の SURROGATE クラスおよびオブジェクト USER.*username* を使用して、プロセスの権限をチェックします。メッセージ テキストの *devnum* および *inode* は、発行元プログラムのデバイスおよび i-node を示します。このメッセージの後に「SUID Result」メッセージが表示されます。

SUID > Result: 'R' [stage=stage gstag=gstage ACEEH=hhh rv=rv]Why? detailedreasontext

CA Access Control により、setuid 要求が SURROGATE アクセス ルールと照合されました。結果 R は P(許可)または D(拒否)です。この判断はアクセサ ハンドル *hhh* に代わって行われました。メッセージ テキストの *detailed-reason-text* は、拒否または許可の理由を示します。

VERPASS: パスワードの確認

CA Access Control が、ユーザのパスワード有効性の検証要求を受け取りました。

WAKE_UP: サーバを起動しています

seosd デーモンが初期化を開始しました。

警告: P=ppp ACEEH=hhh を関連付けます

CA Access Control はすべての fork 要求に対して、プロセスとアクセサ ハンドル(ACEEH)の関連付けを実行します。このメッセージは、ハンドル *hhh* が「-1」であるか、*hhh* が有効なアクセサ ハンドルではないため、関連付けができないことを示しています。hhh が有効なアクセサ ハンドルではない場合は、ベンダーのテクニカル サポート担当者に連絡してください。

警告: P=ppp を確認できません

このメッセージは、不明な P= メッセージの後に表示され、不明なプロセスによって fork 要求が発行されたことを意味します。CA Access Control は、UNIX でそのユーザに関連付けられているユーザの確認を試みました。この確認作業を完了できませんでした。プロセスがすでに終了していた可能性があります。原因がわからない場合は、ベンダーのテクニカル サポート担当者に連絡してください。

警告: P=ppp ACEEH=hhh の関連付けを解除します

CA Access Control は、終了したすべてのプロセスについて、プロセスとアクセサ ハンドル(ACEEH)の関連付けを解除します。このメッセージは、ハンドル *hhh* が「-1」であるため、または *hhh* が有効なアクセサ ハンドルではないため、関連付けを解除できないことを示しています。hhh が有効なアクセサ ハンドルではない場合は、ベンダーのテクニカル サポート担当者に連絡してください。

警告: P=ppp のエントリの ExecArg が NULL ではありません

この警告は、CA Access Control がシステムで認識できない新しいプロセスを検出し、そのプロセスで実行されているプログラムが不明な場合に表示されます。多くの場合、このメッセージは無視できます。要求した結果がシステムで生成されない場合は、ベンダーのテクニカル サポート担当者に連絡してください。

警告: P=ppp の ACEEH を取得できませんでした

CA Access Control はプロセス *ppp* の権限をチェックするよう要求されましたが、そのプロセスには有効なアクセサ ハンドルがありませんでした。ほとんどの場合、このプロセスに関連付けられているユーザが CA Access Control で定義されているユーザではないか、またはこのプロセスが CA Access Control システムにとって不明であることが原因です。いずれの場合も、このプロセスには CA Access Control によってユニバーサル アクセス権限のみが与えられます。要求した結果がシステムで生成されない場合は、ベンダーのテクニカル サポート担当者に連絡してください。

警告: P=0 のログイン ???

AIX 以外のシステムの起動時にこのメッセージが表示された場合は、このメッセージを無視することができます。通常の操作時(seosd の稼動中)や、AIX システムでの起動時にこのメッセージが表示された場合は、ソフトウェア エラーが発生したことを意味します。この場合は、ベンダーのテクニカル サポート担当者に連絡してください。

警告: CA Access Control が P=ppp の強制終了(kill)に失敗しました。理由 =nnn

ループホールの発生を防ぐ手段として、CA Access Control では機密性の高い権限を取得しようとするプロセスが強制終了(kill)されます。このようなイベントとしては、権限のない UID の代理要求(setuid システム コール)などがあります。CA Access Control は、違反しているプロセスを強制終了(kill)しようとしましたが、失敗しました。失敗の理由の詳細は、kill システム コールから返される reason code に示されます。

警告: P=ppp のエントリの端末が NULL ではありません

この警告は、CA Access Control がシステムで認識できない新しいプロセスを検出し、そのプロセスで実行されているプログラムが不明な場合に表示されます。多くの場合、このメッセージは無視できます。要求した結果がシステムで生成されない場合は、ベンダーのテクニカル サポート担当者に連絡してください。

警告: 不明な P=ppp

このメッセージは、CA Access Control が認識できないプロセスによって fork 要求が発行されたことを示します。seoswd または seagent の起動時にこのメッセージが表示された場合は、無視することができます。seoswd または seagent の起動時以外にこのメッセージが表示された場合は、CA Access Control がそのプロセスの実際の権限を確認できないことが原因であるソフトウェア エラーと考えられます。この場合は、ベンダーのテクニカル サポート担当者に連絡してください。

WATCHDOG: Ask if I'm Here (AYT)

seoswd デーモンが、seosd が稼動中であり、要求した応答を返すかどうかを確認しようとしました。メッセージ テキストの AYT は、seoswd の「are you there」チャレンジ メッセージです。このメッセージは無視できます。trcfilter.init ファイルで、このメッセージが表示されないようにしてください。このメッセージは、seoswd が正常に動作していることを意味します。

WATCHDOG: initializationtext を初期化します

seoswd 初期化メッセージ。このメッセージは無視できます。

WATCHDOG: ログ logtext

seoswd デーモンがログ要求を発行しました。ログ要求の内容は *log-text* に記述されています。

WATCHDOG: SecFile operation result

seoswd デーモンが、保護ファイルに関する情報を取得するデーモンを要求しました。メッセージ テキストの *operation* は、GETFIRST または GETNEXT になります。情報を取得できた場合は結果が OK になり、CA Access Control データベースにこれ以上保護ファイルがない場合は結果が NOFOUND になります。このメッセージは、seoswd が保護ファイルをスキャンする際に正常な動作が実行されたことを表します。

WATCHDOG: タイマ

seoswd デーモンは（seos.ini ファイルの設定に従って）数秒単位でタイマ要求を発行します。trcfilter.init ファイルで、このメッセージが表示されないように設定してください。

WATCHDOG: Trust プログラム: programname [OK | NOTOK]

seoswd デーモンが指定されたプログラムを trusted プログラムと定義しました。これは、指定されたプログラムがデジタル署名テストで安全と判断されたことを意味します。メッセージ テキストの OK は、trust 操作が正常に完了したことを意味し、NOTOK は、seoswd がプログラムを trusted と定義できなかったことを意味します。NOTOK の場合は、データベースが壊れている可能性があります。その場合は、ベンダーのテクニカル サポート担当者に連絡してください。

WATCHDOG: Untrust プログラム: programname [OK | NOTOK]

seoswd デーモンが、指定されたプログラムを untrusted プログラムとして定義しました。これは、指定されたプログラムが seoswd によるデジタル署名チェックで安全とみなされなかったことを意味します。メッセージ テキストの OK は、untrust 操作が正常に完了したことを意味し、NOTOK は、seoswd がプログラムを untrusted と定義できなかったことを意味します。NOTOK の場合は、データベースが壊れている可能性があります。その場合は、ベンダーのテクニカル サポート担当者に連絡してください。

付録 C: 文字列マッチング

このセクションには、以下のトピックが含まれています。

ワイルドカード表現

このセクションでは、ワイルドカード表現を構築するときに使用される構文について説明します。

CA Access Control では、ワイルドカードによる一致および文字リストを使用して、文字列マッチング(グロビング)を実行します。

ワイルドカードによる一致

CA Access Control では、以下のワイルドカード文字を使用できます。

文字	一致
* (アスタリスク)	0 個以上の文字列
? (疑問符)	任意の 1 文字

文字リスト

角かっこ([ ])で囲まれた文字リストには、1 つ以上の文字を使用できます。CA Access Control では、正または負の一致基準としてこれらの文字を使用します。

文字リストは 1 つ以上の文字で構成されています。このタイプのリストの場合、CA Access Control は、リスト内の任意の 1 文字と一致します。かっこ内のリストの前にカレット記号(^)がある場合は、CA Access Control はリスト内に含まれない任意の 1 文字と一致します。

範囲は文字の範囲を指定する文字リストのタイプとなります。CA Access Control は、リスト内のすべての文字に包括的に一致します。カレット記号(^)がリストの前にある場合、CA Access Control では、指定されたリスト内のすべての文字が除外されます。範囲の下限および上限を指定したり、最初または最後の文字のみを指定したりすることができます。

使用できる文字リストを以下の表に示します。この構文では、角かっこを使用することに注意してください。表現 *ch1*、*ch2*、および *chN* は、それぞれ 1 つの文字を表します。

リスト	説明
[*ch1ch2...chN***]**	CA Access Control は、角かっこで囲まれたリスト内の任意の 1 文字と一致します。
[^*ch1ch2...chN***]**	CA Access Control は、角かっこで囲まれたリスト内に含まれない任意の 1 文字と一致します。
[*ch1-ch2***]**	CA Access Control は、範囲内の任意の 1 文字と包括的に一致します。
[^*ch1-ch2***]**	CA Access Control は、包括的な範囲内に含まれない任意の 1 文字と一致します。
[-*ch2***]**	CA Access Control は、指定された文字(*ch2*)以下の ASCII 値を持つ任意の 1 文字と一致します。
[^-*ch2***]**	CA Access Control は、指定された文字(*ch2*)以上の ASCII 値を持つ任意の 1 文字と一致します。
[*ch1-***]**	CA Access Control は、指定された文字(*ch1*)以上の ASCII 値を持つ任意の 1 文字と一致します。
[^*ch1-***]**	CA Access Control は、指定された文字(*ch1*)以下の ASCII 値を持つ任意の 1 文字と一致します。

例: ワイルドカードによる一致

任意の 1 文字に一致するパターンを指定するには、疑問符(?)を使用します。

指定する文字	一致する文字
mmc?	mmc3、mmcx、mmc5
mmc?.t	mmc1.t、mmc2.t

指定する文字	一致する文字
mmc04.?	mmc04.a、mmc04.1

0 個以上の任意の文字列に一致するパターンを指定するには、アスタリスク(*)を使用します。

指定する文字	一致する文字
i.c	main.c、list.c、など
st*.h	stdio.h、stdlib.h、string.h、など
*	指定されたクラスのすべてのレコード

リスト内の任意の文字に一致するパターンを指定するには、以下の例のいずれかに従います。

指定する文字	一致する文字
[abcgk]	a、b、c、g、または k
[^abcgk]	a、b、c、g、または k 以外の任意の文字(A、B、d、e、f、@ など)。
[a-z]	a から z の間にある任意の文字。
[^a-z]	「a」より小さく「z」より大きい ASCII 値を持つ任意の文字。
[Z-]	Z の ASCII 値より大きい ASCII 値を持つ任意の文字(a、b、¥、~ など)。
[^-A]	「A」の ASCII 値以上の ASCII 値を持つ任意の文字(B、a、c、~ など)。

付録 D: 使用されているポート

このセクションには、以下のトピックが含まれています。

UNIX で使用されているポート

CA Access Control では、以下の TCP ポートが Windows 上でデフォルトとして使用されます。

数値	説明	リスナ	送信者	コメント
8891	CA Access Control クライアント アプリケーション	CA Access Control エージェント	dbmgr（seosd が実行中の場合）、devcalc、dmsmgr、policydeploy、policyreport、sechkey（リモート コンピュータを管理中の場合）、secons、segrace、segracex、seini（リモート コンピュータを管理中の場合）、selang（seosd が実行中の場合）、senable、sepass、sereport、seretrust、serevu、sesu、sesudo、sewhoami、sepmdd（PMD）	デフォルトのポート番号は、/etc/services ファイル設定を変更することよって変更できます。これを行うには、以下の行を追加し、CA Access Control デーモンを再起動します。 `seoslang2 port-number/tcp`
5249	SSL 通信	CA Access Control エージェント	**注**: FIPS 準拠の通信が提供されているコンポーネントの詳細については、「*リリース ノート*」を参照してください。	FIPS 140-2 準拠

数値	説明	リスナ	送信者	コメント
8892	リモート コンピュータから seosd を起動中	seosload	selaod	seload を使用してデーモンをリモート コンピュータでロードする場合は、リモート コンピュータの inetd（インターネット サービス デーモン）によって rseloadd プログラムが実行されます。このプログラムは seload をローカルで実行して終了し、このポートのパラメータを受け取ります。 デフォルトのポート番号は、/etc/services ファイル設定を変更することよって変更できます。これを行うには、以下の行を追加し、CA Access Control デーモンを再起動します。 `seosload  port-number/ tcp` **注**: このポート上の通信は、機密情報を送信することがないため、暗号化されません。

Windows で使用されているポート

CA Access Control では、以下の TCP ポートが Windows 上でデフォルトとして使用されます。

数値	説明	リスナ	送信者	コメント
8891	CA Access Control クライアント アプリケーション	CA Access Control エージェント	selang.exe、sepmdd.exe（PMD）、eACSigUpdate.exe、SegraceW.exe（猶予ログインおよびパスワード設定）、secons.exe（リモート シャットダウンおよび IP アドレス更新）、policydeploy.exe、devcalc.exe、policyfetcher.exe	デフォルトのポート番号は、%SystemRoot%¥drivers¥etc¥services ファイル設定を変更することよって変更できます。これを行うには、以下の行を追加し、CA Access Control サービスを再起動します。 `seoslang2 port-number/tcp`
5249	SSL 通信	CA Access Control エージェント	**注**: FIPS 準拠の通信が提供されているコンポーネントの詳細については、「*リリース ノート*」を参照してください。	FIPS 140-2 準拠

サーバ コンポーネントで使用されているポート

CA Access Control では、以下の TCP ポートがサーバ コンポーネントでデフォルトとして使用されます。

数値	説明	リスナ	送信者
7222	レポート スナップショット	配布サーバ	レポート エージェント
7243	SSL を使用したレポート スナップショット	配布サーバ	レポート エージェント
5248	ローカル Web ベースのインターフェース通信	CA Access Control Web サービス	CA Access Control エンドポイント管理、CA Access Control エンタープライズ管理

これらのポート以外にも、以下のポートを開く必要があります。

- 配布サーバまたは CA Access Control エンタープライズ管理 と通信するには、これらが個別のコンピュータに存在する場合、中央データベース コンピュータ上でポートを開く必要があります。
- リモート コンピュータから InfoView アプリケーションにアクセスするには、レポート ポータル（BusinessObjects）のコンピュータ上でポートを開く必要があります（デフォルトで 8080）。
- Web ベースのインターフェースにリモート コンピュータからアクセスするには、CA Access Control エンドポイント管理 および CA Access Control エンタープライズ管理 コンピュータ上でポートを開く必要があります（デフォルトで 18080）。
- リモート コンピュータから Web ベースのインターフェースにアクセスするには、Oracle Database をインストールしたコンピュータ上でポートを開く必要があります（デフォルトで 8080 または 7443（SSL））。
- CA Access Control エージェント経由で接続するには、以下のコンポーネントに対して、拡張ポリシー管理サーバ コンポーネント上でポートを開く必要があります（デフォルトで 8891 または 5249（SSL））。
  - DH に対して DMS
  - DMS に対して DH
  - リモート サーバ上の DH に対して licyfetcher および devcalc

UNIX 認証ブローカ で使用されるポート

UNIX 認証ブローカ では、以下の TCP ポートが UNIX 上でデフォルトとして使用されます。

数値	[Description]	リスナ	送信者
88	Kerberos トラフィック	Active Directory	UNIX 認証ブローカ
389	Kerberized LDAP	Active Directory	UNIX 認証ブローカ
445	Microsoft ディレクトリ サービス	Active Directory	UNIX 認証ブローカ
464	Kerberos kpasswd	Active Directory	UNIX 認証ブローカ
3268	グローバル カタログ	Active Directory	UNIX 認証ブローカ

数値	［Description］	リスナ	送信者
7222	レポート スナップショット	配布サーバ	レポート エージェント
7243	SSL を使用したレポート スナップショット	配布サーバ	レポート エージェント

UNIX 認証ブローカ は UNIX 上で以下の UDP をデフォルトとして使用します。

数値	説明	リスナ	送信者
53	DNS	Active Directory	UNIX 認証ブローカ
88	Kerberos トラフィック	Active Directory	UNIX 認証ブローカ
123	NTP	Active Directory	UNIX 認証ブローカ
389	Kerberized LDAP	Active Directory	UNIX 認証ブローカ
464	Kerberos kpasswd	Active Directory	UNIX 認証ブローカ

付録 E: レポート データベース スキーマ

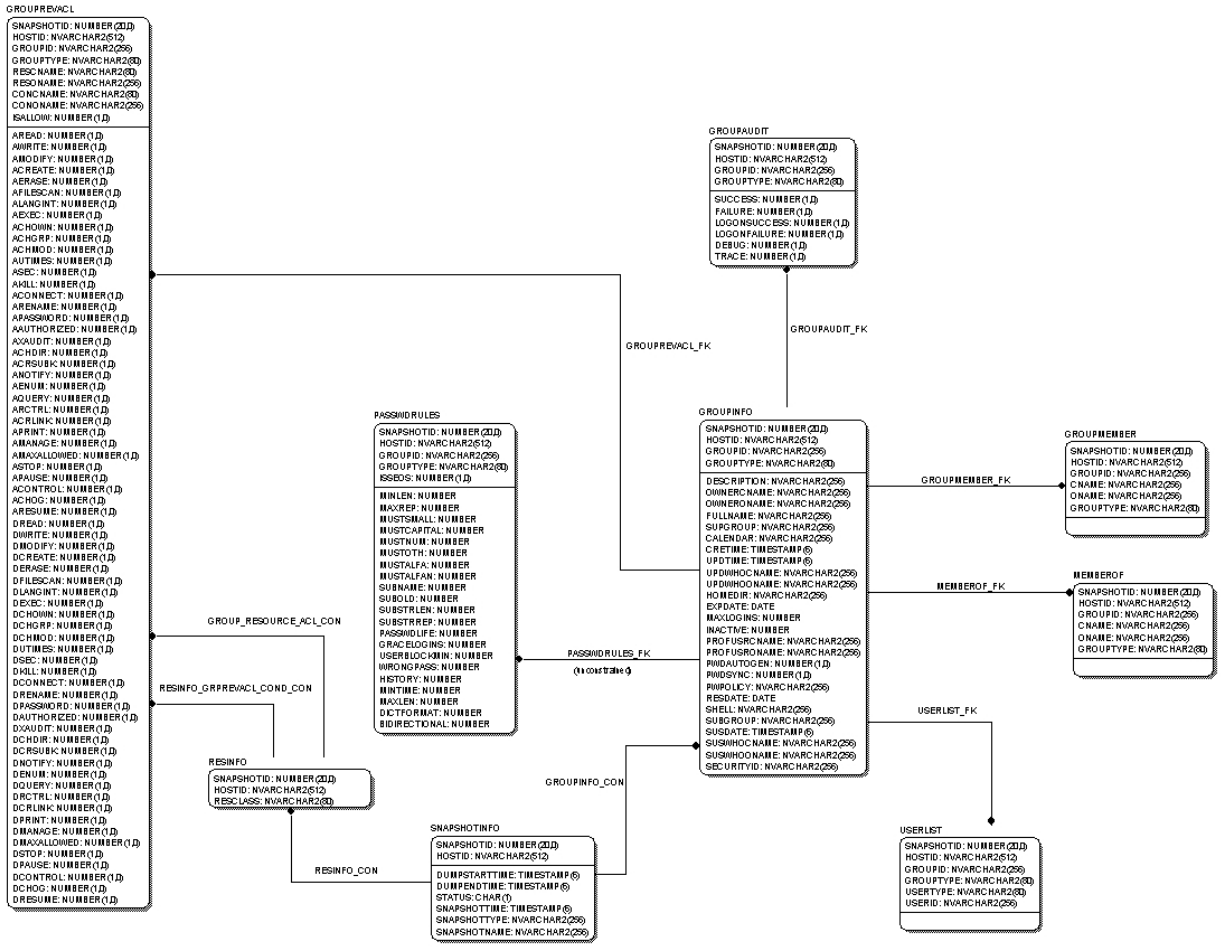
このセクションには、以下のトピックが含まれています。

スキーマに関するブロック図

以下のトピックでは、CA Access Control レポート データベースのスキーマに関するブロック図を示します。

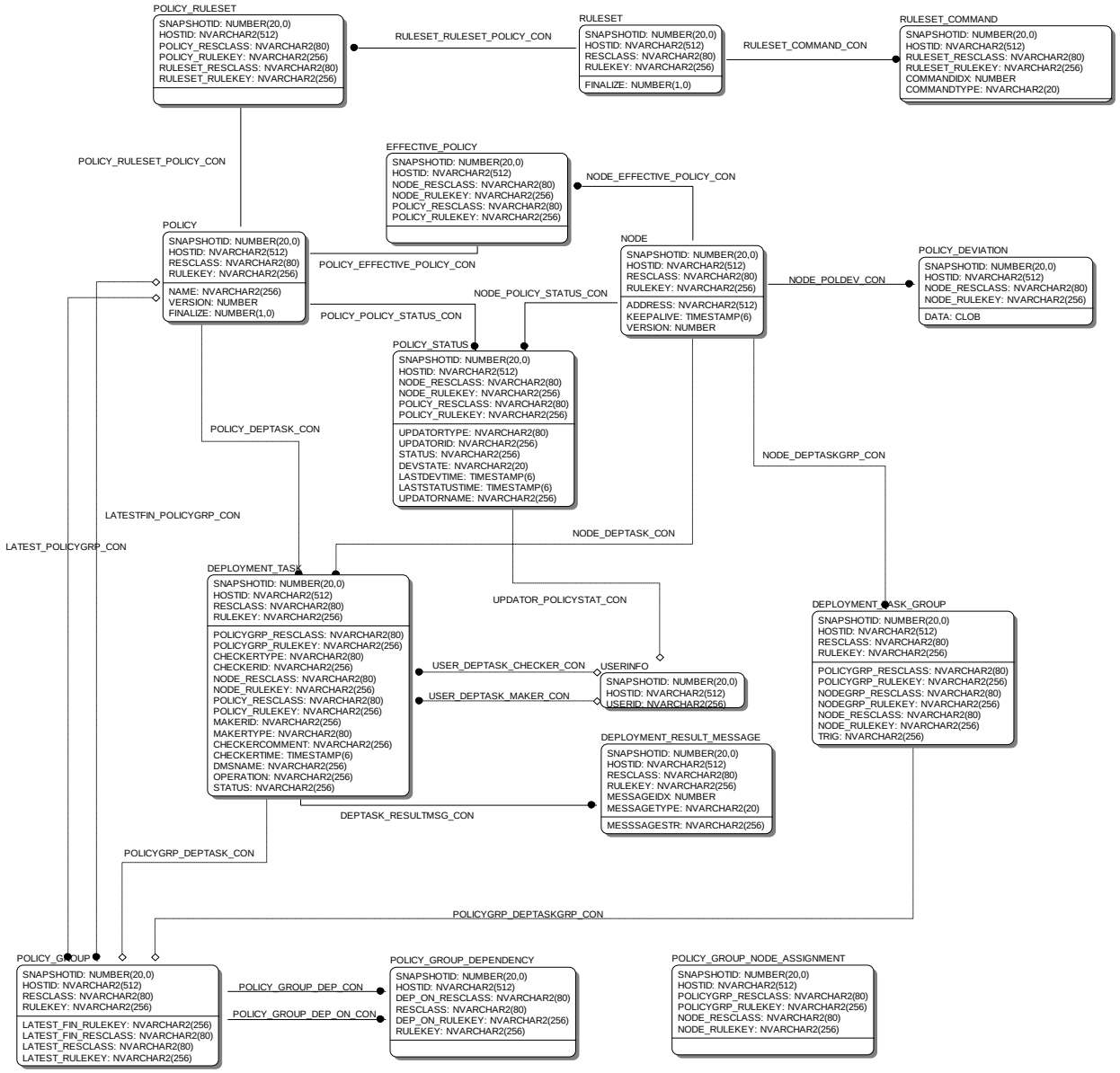
グループ

次のブロック図は、グループに関連したテーブルを示しています。



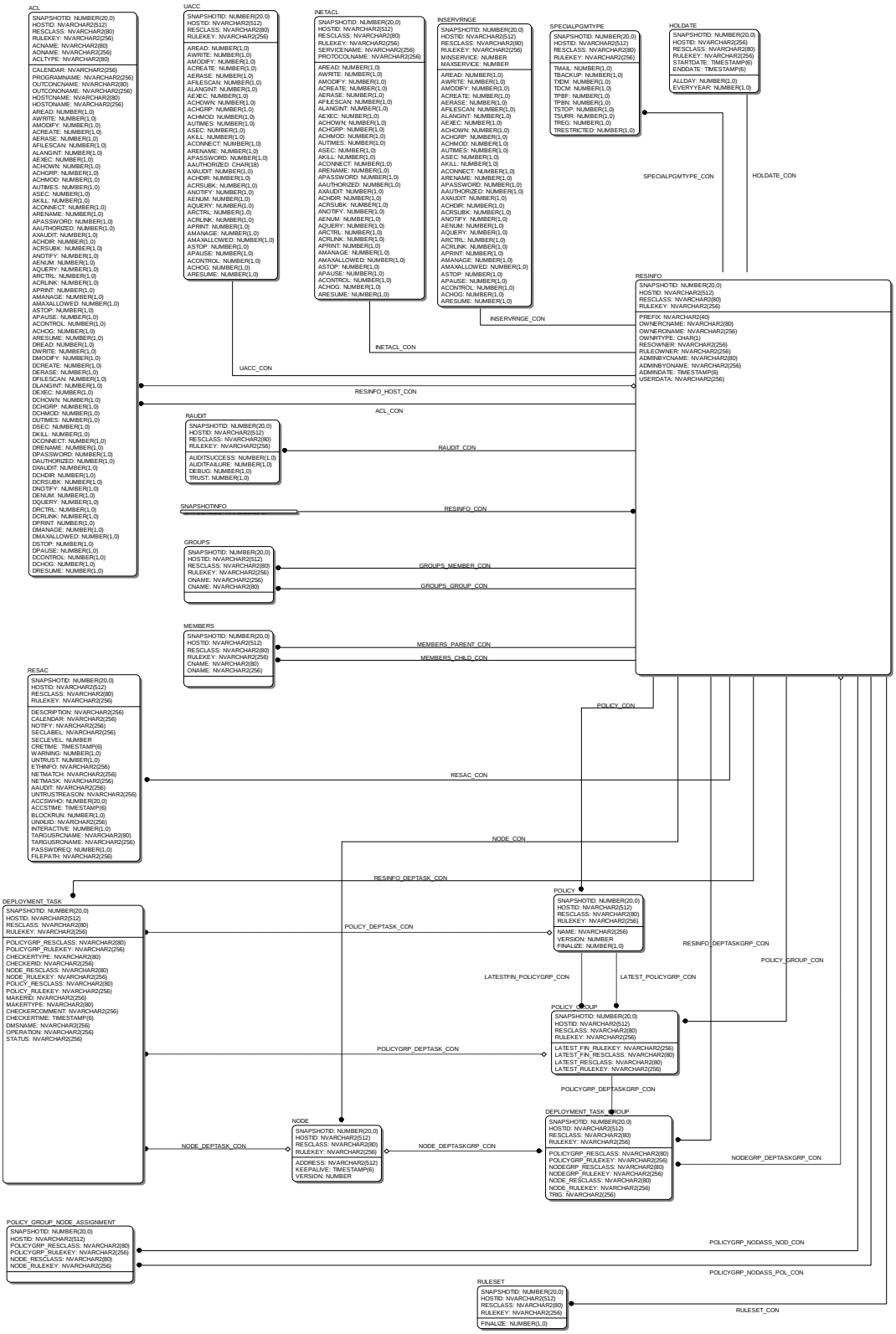
ポリシー管理

次のブロック図は、ポリシー管理に関連したテーブルを示しています。



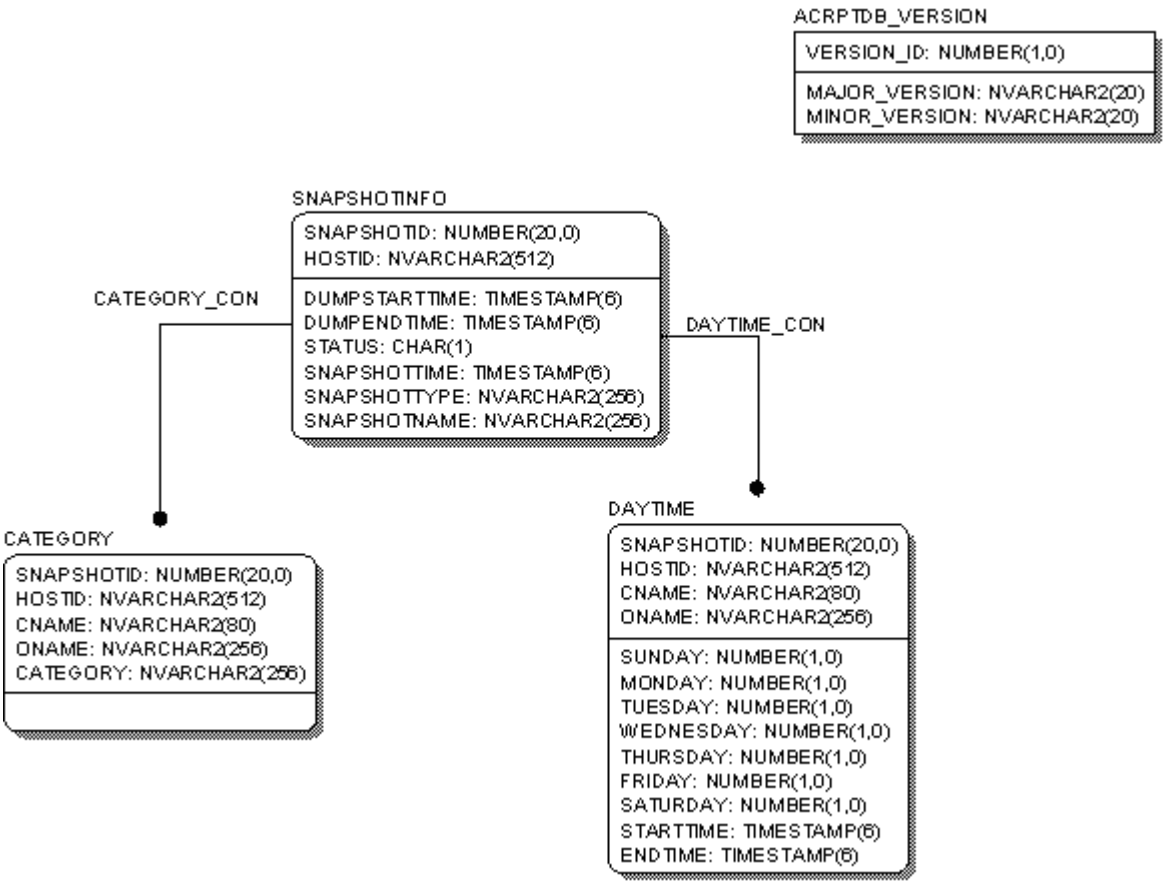
リソース

次のブロック図は、リソースに関連したテーブルを示しています。


ACL
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
RESCLASS: NVARCHAR2(80)
RULEKEY: NVARCHAR2(256)
ACNAME: NVARCHAR2(80)
AONAME: NVARCHAR2(256)
ACLTYPE: NVARCHAR2(80)
UACC
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
RESCLASS: NVARCHAR2(80)
RULEKEY: NVARCHAR2(256)
INETACL
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
RESCLASS: NVARCHAR2(80)
RULEKEY: NVARCHAR2(256)
SERVICENAME: NVARCHAR2(256)
PROTOCOLNAME: NVARCHAR2(256)
INSERVRNGE
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
RESCLASS: NVARCHAR2(80)
RULEKEY: NVARCHAR2(256)
MINSERVICE: NUMBER
MAXSERVICE: NUMBER
SPECIALPGMTYPE
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
RESCLASS: NVARCHAR2(80)
RULEKEY: NVARCHAR2(256)
HOLDATE
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(256)
RESCLASS: NVARCHAR2(80)
RULEKEY: NVARCHAR2(256)
STARTDATE: TIMESTAMP(6)
ENDDATE: TIMESTAMP(6)
SPECIALPGMTYPE_CON
HOLDATE_CON
RESINFO
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
RESCLASS: NVARCHAR2(80)
RULEKEY: NVARCHAR2(256)
INSERVRNGE_CON
INETACL_CON
UACC_CON
RESINFO_HOST_CON
ACL_CON
RAUDIT
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
RESCLASS: NVARCHAR2(80)
RULEKEY: NVARCHAR2(256)
RAUDIT_CON
SNAPSHOTINFO
RESINFO_CON
GROUPS
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
RESCLASS: NVARCHAR2(80)
RULEKEY: NVARCHAR2(256)
GROUPS_MEMBER_CON
GROUPS_GROUP_CON
MEMBERS
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
RESCLASS: NVARCHAR2(80)
RULEKEY: NVARCHAR2(256)
MEMBERS_PARENT_CON
MEMBERS_CHILD_CON
RESAC
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
RESCLASS: NVARCHAR2(80)
RULEKEY: NVARCHAR2(256)
POLICY_CON
RESAC_CON
NODE_CON
RESINFO_DEPTASK_CON
DEPLOYMENT_TASK
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
RESCLASS: NVARCHAR2(80)
RULEKEY: NVARCHAR2(256)
POLICY
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
RESCLASS: NVARCHAR2(80)
RULEKEY: NVARCHAR2(256)
POLICY_DEPTASK_CON
RESINFO_DEPTASKGRP_CON
POLICY_GROUP_CON
LATESTFIN_POLICYGRP_CON
LATEST_POLICYGRP_CON
POLICY_GROUP
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
RESCLASS: NVARCHAR2(80)
RULEKEY: NVARCHAR2(256)
POLICYGRP_DEPTASK_CON
POLICYGRP_DEPTASKGRP_CON
NODE
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
RESCLASS: NVARCHAR2(80)
RULEKEY: NVARCHAR2(256)
NODE_DEPTASK_CON
NODE_DEPTASKGRP_CON
DEPLOYMENT_TASK_GROUP
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
RESCLASS: NVARCHAR2(80)
RULEKEY: NVARCHAR2(256)
NODEGRP_DEPTASKGRP_CON
POLICY_GROUP_NODE_ASSIGNMENT
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
POLICYGRP_RESCLASS: NVARCHAR2(80)
POLICYGRP_RULEKEY: NVARCHAR2(256)
NODE_RESCLASS: NVARCHAR2(80)
NODE_RULEKEY: NVARCHAR2(256)
POLICYGRP_NODASS_NOD_CON
POLICYGRP_NODASS_POL_CON
RULESET
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
RESCLASS: NVARCHAR2(80)
RULEKEY: NVARCHAR2(256)
RULESET_CON

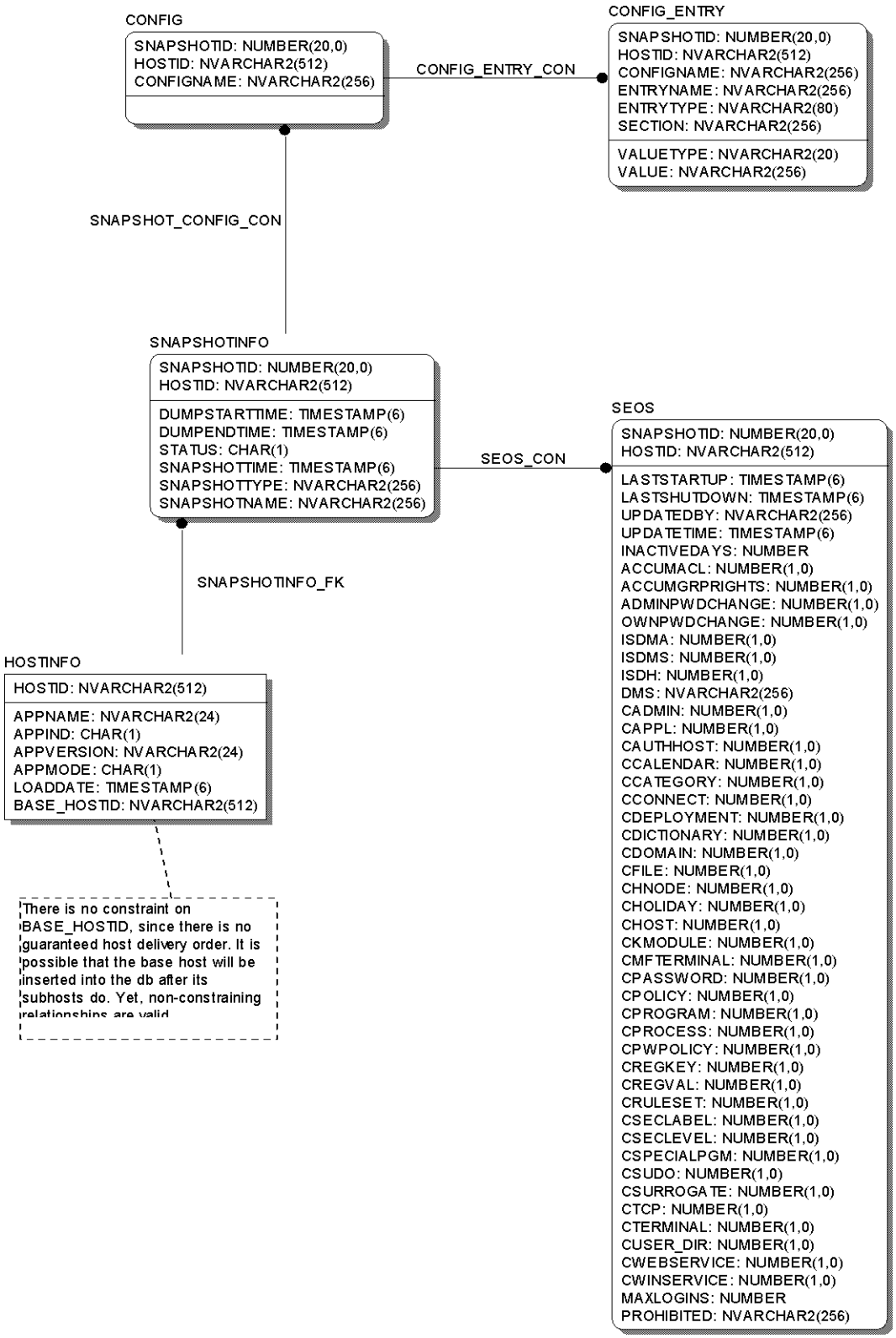
共有プロパティ

次のブロック図は、ユーザ、グループ、およびリソース オブジェクトの間の共有プロパティを示しています。



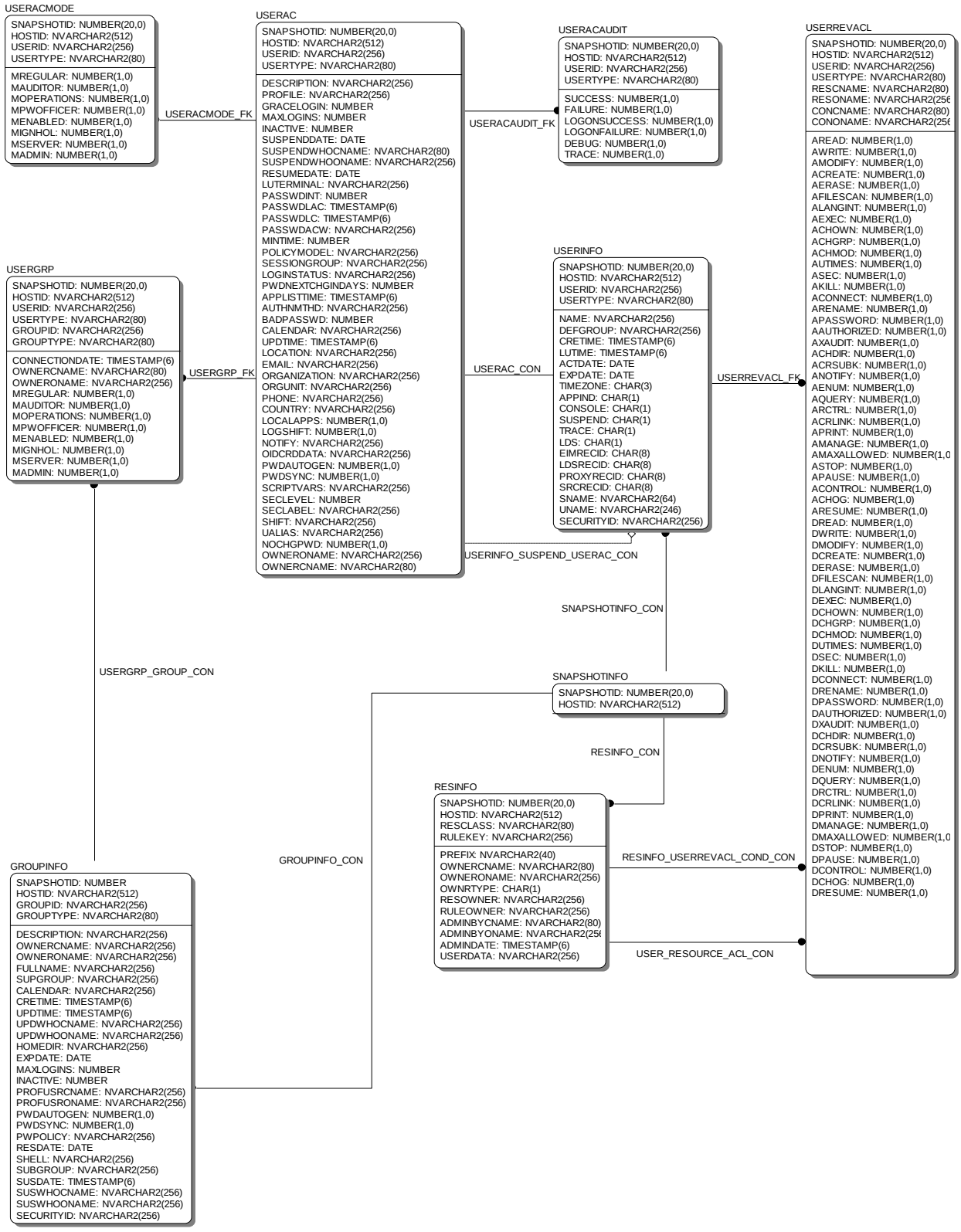
スナップショット

次のブロック図は、スナップショットおよびエンドポイントに関連したテーブルを示しています。


CONFIG
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
CONFIGNAME: NVARCHAR2(256)
CONFIG_ENTRY_CON
CONFIG_ENTRY
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
CONFIGNAME: NVARCHAR2(256)
ENTRYNAME: NVARCHAR2(256)
ENTRYTYPE: NVARCHAR2(80)
SECTION: NVARCHAR2(256)
VALUETYPE: NVARCHAR2(20)
VALUE: NVARCHAR2(256)
SNAPSHOT_CONFIG_CON
SNAPSHOTINFO
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
DUMPSTARTTIME: TIMESTAMP(6)
DUMPENDTIME: TIMESTAMP(6)
STATUS: CHAR(1)
SNAPSHOTTIME: TIMESTAMP(6)
SNAPSHOTTYPE: NVARCHAR2(256)
SNAPSHOTNAME: NVARCHAR2(256)
SEOS_CON
SEOS
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
LASTSTARTUP: TIMESTAMP(6)
LASTSHUTDOWN: TIMESTAMP(6)
UPDATEDBY: NVARCHAR2(256)
UPDATETIME: TIMESTAMP(6)
INACTIVEDAYS: NUMBER
ACCUMACL: NUMBER(1,0)
ACCUMGRPRIGHTS: NUMBER(1,0)
ADMINPWDCHANGE: NUMBER(1,0)
OWNPWDCHANGE: NUMBER(1,0)
ISDMA: NUMBER(1,0)
ISDMS: NUMBER(1,0)
ISDH: NUMBER(1,0)
DMS: NVARCHAR2(256)
CADMIN: NUMBER(1,0)
CAPPL: NUMBER(1,0)
CAUTHHOST: NUMBER(1,0)
CCALENDAR: NUMBER(1,0)
CCATEGORY: NUMBER(1,0)
CCONNECT: NUMBER(1,0)
CDEPLOYMENT: NUMBER(1,0)
CDICTIONARY: NUMBER(1,0)
CDOMAIN: NUMBER(1,0)
CFILE: NUMBER(1,0)
CHNODE: NUMBER(1,0)
CHOLIDAY: NUMBER(1,0)
CHOST: NUMBER(1,0)
CKMODULE: NUMBER(1,0)
CMFTERMINAL: NUMBER(1,0)
CPASSWORD: NUMBER(1,0)
CPOLICY: NUMBER(1,0)
CPROGRAM: NUMBER(1,0)
CPROCESS: NUMBER(1,0)
CPWPOLICY: NUMBER(1,0)
CREGKEY: NUMBER(1,0)
CREGVAL: NUMBER(1,0)
CRULESET: NUMBER(1,0)
CSECLABEL: NUMBER(1,0)
CSECLEVEL: NUMBER(1,0)
CSPECIALPGM: NUMBER(1,0)
CSUDO: NUMBER(1,0)
CSURROGATE: NUMBER(1,0)
CTCP: NUMBER(1,0)
CTERMINAL: NUMBER(1,0)
CUSER_DIR: NUMBER(1,0)
CWEBSERVICE: NUMBER(1,0)
CWINSERVICE: NUMBER(1,0)
MAXLOGINS: NUMBER
PROHIBITED: NVARCHAR2(256)
SNAPSHOTINFO_FK
HOSTINFO
HOSTID: NVARCHAR2(512)
APPNAME: NVARCHAR2(24)
APPIND: CHAR(1)
APPVERSION: NVARCHAR2(24)
APPMODE: CHAR(1)
LOADDATE: TIMESTAMP(6)
BASE_HOSTID: NVARCHAR2(512)
There is no constraint on BASE_HOSTID, since there is no guaranteed host delivery order. It is possible that the base host will be inserted into the db after its subhosts do. Yet, non-constraining relationships are valid

ユーザ

次のブロック図は、ユーザに関連したテーブルを示しています。


USERACMODE
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
USERID: NVARCHAR2(256)
USERTYPE: NVARCHAR2(80)
MREGULAR: NUMBER(1,0)
MAUDITOR: NUMBER(1,0)
MOPERATIONS: NUMBER(1,0)
MPWOFFICER: NUMBER(1,0)
MENABLED: NUMBER(1,0)
MIGNHOL: NUMBER(1,0)
MSERVER: NUMBER(1,0)
MADMIN: NUMBER(1,0)
USERACMODE_FK
USERAC
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
USERID: NVARCHAR2(256)
USERTYPE: NVARCHAR2(80)
DESCRIPTION: NVARCHAR2(256)
PROFILE: NVARCHAR2(256)
GRACELOGIN: NUMBER
MAXLOGINS: NUMBER
INACTIVE: NUMBER
SUSPENDDATE: DATE
SUSPENDWHOCNAME: NVARCHAR2(80)
SUSPENDWHOONAME: NVARCHAR2(256)
RESUMEDATE: DATE
LUTERMINAL: NVARCHAR2(256)
PASSWDINT: NUMBER
PASSWDLAC: TIMESTAMP(6)
PASSWDLC: TIMESTAMP(6)
PASSWDACW: NVARCHAR2(256)
MINTIME: NUMBER
POLICYMODEL: NVARCHAR2(256)
SESSIONGROUP: NVARCHAR2(256)
LOGINSTATUS: NVARCHAR2(256)
PWDNEXTCHGINDAYS: NUMBER
APPLISTTIME: TIMESTAMP(6)
AUTHNMTHD: NVARCHAR2(256)
BADPASSWD: NUMBER
CALENDAR: NVARCHAR2(256)
UPDTIME: TIMESTAMP(6)
LOCATION: NVARCHAR2(256)
EMAIL: NVARCHAR2(256)
ORGANIZATION: NVARCHAR2(256)
ORGUNIT: NVARCHAR2(256)
PHONE: NVARCHAR2(256)
COUNTRY: NVARCHAR2(256)
LOCALAPPS: NUMBER(1,0)
LOGSHIFT: NUMBER(1,0)
NOTIFY: NVARCHAR2(256)
OIDCRDDATA: NVARCHAR2(256)
PWDAUTOGEN: NUMBER(1,0)
PWDSYNC: NUMBER(1,0)
SCRIPTVARS: NVARCHAR2(256)
SECLEVEL: NUMBER
SECLABEL: NVARCHAR2(256)
SHIFT: NVARCHAR2(256)
UALIAS: NVARCHAR2(256)
NOCHGPWD: NUMBER(1,0)
OWNERONAME: NVARCHAR2(256)
OWNERCNAME: NVARCHAR2(80)
USERACAUDIT_FK
USERACAUDIT
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
USERID: NVARCHAR2(256)
USERTYPE: NVARCHAR2(80)
SUCCESS: NUMBER(1,0)
FAILURE: NUMBER(1,0)
LOGONSUCCESS: NUMBER(1,0)
LOGONFAILURE: NUMBER(1,0)
DEBUG: NUMBER(1,0)
TRACE: NUMBER(1,0)
USERREVACL
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
USERID: NVARCHAR2(256)
USERTYPE: NVARCHAR2(80)
RESCNAME: NVARCHAR2(80)
RESONAME: NVARCHAR2(256
CONCNAME: NVARCHAR2(80)
CONONAME: NVARCHAR2(256
AREAD: NUMBER(1,0)
AWRITE: NUMBER(1,0)
AMODIFY: NUMBER(1,0)
ACREATE: NUMBER(1,0)
AERASE: NUMBER(1,0)
AFILESCAN: NUMBER(1,0)
ALANGINT: NUMBER(1,0)
AEXEC: NUMBER(1,0)
ACHOWN: NUMBER(1,0)
ACHGRP: NUMBER(1,0)
ACHMOD: NUMBER(1,0)
AUTIMES: NUMBER(1,0)
ASEC: NUMBER(1,0)
AKILL: NUMBER(1,0)
ACONNECT: NUMBER(1,0)
ARENAME: NUMBER(1,0)
APASSWORD: NUMBER(1,0)
AAUTHORIZED: NUMBER(1,0)
AXAUDIT: NUMBER(1,0)
ACHDIR: NUMBER(1,0)
ACRSUBK: NUMBER(1,0)
ANOTIFY: NUMBER(1,0)
AENUM: NUMBER(1,0)
AQUERY: NUMBER(1,0)
ARCTRL: NUMBER(1,0)
ACRLINK: NUMBER(1,0)
APRINT: NUMBER(1,0)
AMANAGE: NUMBER(1,0)
AMAXALLOWED: NUMBER(1,0
ASTOP: NUMBER(1,0)
APAUSE: NUMBER(1,0)
ACONTROL: NUMBER(1,0)
ACHOG: NUMBER(1,0)
ARESUME: NUMBER(1,0)
DREAD: NUMBER(1,0)
DWRITE: NUMBER(1,0)
DMODIFY: NUMBER(1,0)
DCREATE: NUMBER(1,0)
DERASE: NUMBER(1,0)
DFILESCAN: NUMBER(1,0)
DLANGINT: NUMBER(1,0)
DEXEC: NUMBER(1,0)
DCHOWN: NUMBER(1,0)
DCHGRP: NUMBER(1,0)
DCHMOD: NUMBER(1,0)
DUTIMES: NUMBER(1,0)
DSEC: NUMBER(1,0)
DKILL: NUMBER(1,0)
DCONNECT: NUMBER(1,0)
DRENAME: NUMBER(1,0)
DPASSWORD: NUMBER(1,0)
DAUTHORIZED: NUMBER(1,0)
DXAUDIT: NUMBER(1,0)
DCHDIR: NUMBER(1,0)
DCRSUBK: NUMBER(1,0)
DNOTIFY: NUMBER(1,0)
DENUM: NUMBER(1,0)
DQUERY: NUMBER(1,0)
DRCTRL: NUMBER(1,0)
DCRLINK: NUMBER(1,0)
DPRINT: NUMBER(1,0)
DMANAGE: NUMBER(1,0)
DMAXALLOWED: NUMBER(1,0
DSTOP: NUMBER(1,0)
DPAUSE: NUMBER(1,0)
DCONTROL: NUMBER(1,0)
DCHOG: NUMBER(1,0)
DRESUME: NUMBER(1,0)
USERGRP
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
USERID: NVARCHAR2(256)
USERTYPE: NVARCHAR2(80)
GROUPID: NVARCHAR2(256)
GROUPTYPE: NVARCHAR2(80)
CONNECTIONDATE: TIMESTAMP(6)
OWNERCNAME: NVARCHAR2(80)
OWNERONAME: NVARCHAR2(256)
MREGULAR: NUMBER(1,0)
MAUDITOR: NUMBER(1,0)
MOPERATIONS: NUMBER(1,0)
MPWOFFICER: NUMBER(1,0)
MENABLED: NUMBER(1,0)
MIGNHOL: NUMBER(1,0)
MSERVER: NUMBER(1,0)
MADMIN: NUMBER(1,0)
USERGRP_FK
USERAC_CON
USERREVACL_FK
USERINFO
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
USERID: NVARCHAR2(256)
USERTYPE: NVARCHAR2(80)
NAME: NVARCHAR2(256)
DEFGROUP: NVARCHAR2(256)
CRETIME: TIMESTAMP(6)
LUTIME: TIMESTAMP(6)
ACTDATE: DATE
EXPDATE: DATE
TIMEZONE: CHAR(3)
APPIND: CHAR(1)
CONSOLE: CHAR(1)
SUSPEND: CHAR(1)
TRACE: CHAR(1)
LDS: CHAR(1)
EIMRECID: CHAR(8)
LDSRECID: CHAR(8)
PROXYRECID: CHAR(8)
SRCRECID: CHAR(8)
SNAME: NVARCHAR2(64)
UNAME: NVARCHAR2(246)
SECURITYID: NVARCHAR2(256)
USERINFO_SUSPEND_USERAC_CON
SNAPSHOTINFO_CON
USERGRP_GROUP_CON
SNAPSHOTINFO
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
RESINFO_CON
RESINFO
SNAPSHOTID: NUMBER(20,0)
HOSTID: NVARCHAR2(512)
RESCLASS: NVARCHAR2(80)
RULEKEY: NVARCHAR2(256)
PREFIX: NVARCHAR2(40)
OWNERCNAME: NVARCHAR2(80)
OWNERONAME: NVARCHAR2(256)
OWNRTYPE: CHAR(1)
RESOWNER: NVARCHAR2(256)
RULEOWNER: NVARCHAR2(256)
ADMINBYCNAME: NVARCHAR2(80)
ADMINBYONAME: NVARCHAR2(256
ADMINDATE: TIMESTAMP(6)
USERDATA: NVARCHAR2(256)
RESINFO_USERREVACL_COND_CON
USER_RESOURCE_ACL_CON
GROUPINFO_CON
GROUPINFO
SNAPSHOTID: NUMBER
HOSTID: NVARCHAR2(512)
GROUPID: NVARCHAR2(256)
GROUPTYPE: NVARCHAR2(80)
DESCRIPTION: NVARCHAR2(256)
OWNERCNAME: NVARCHAR2(256)
OWNERONAME: NVARCHAR2(256)
FULLNAME: NVARCHAR2(256)
SUPGROUP: NVARCHAR2(256)
CALENDAR: NVARCHAR2(256)
CRETIME: TIMESTAMP(6)
UPDTIME: TIMESTAMP(6)
UPDWHOCNAME: NVARCHAR2(256)
UPDWHOONAME: NVARCHAR2(256)
HOMEDIR: NVARCHAR2(256)
EXPDATE: DATE
MAXLOGINS: NUMBER
INACTIVE: NUMBER
PROFUSRCNAME: NVARCHAR2(256)
PROFUSRONAME: NVARCHAR2(256)
PWDAUTOGEN: NUMBER(1,0)
PWDSYNC: NUMBER(1,0)
PWPOLICY: NVARCHAR2(256)
RESDATE: DATE
SHELL: NVARCHAR2(256)
SUBGROUP: NVARCHAR2(256)
SUSDATE: TIMESTAMP(6)
SUSWHOCNAME: NVARCHAR2(256)
SUSWHOONAME: NVARCHAR2(256)
SECURITYID: NVARCHAR2(256)

テーブル

以下の表では、スキーマ内のテーブルを示し、各テーブルについて概説しています。

名前	コメント
ACL	大部分の CA Access Control リソースに対するアクセス制御リスト。このリストでは、CA Access Control プロパティ(ACL、NACL、PACL、CACL、CALACL)が組み合わされています。 ACL - 標準のアクセス制御リスト。リソースへのアクセスを許可されたユーザまたはグループの名前(あるいはその両方)、および各ユーザまたはグループに与えられたアクセス権のレベルが登録されています。 NACL - 拒否アクセス制御リスト。リソースへのアクセスが許可されていないユーザまたはグループの名前が登録されています。 PACL 強調 - プログラム アクセス制御リスト。リストにアクセスするプログラムによって異なります。各 PACL には、ユーザ名およびグループ名、アクセス権限レベル、および特定のリソースにアクセスするためにユーザが実行する必要があるプログラムやシェル スクリプトの名前が登録されています。 CACL - 条件付きアクセス制御リスト CALACL - カレンダ アクセス制御リスト。Unicenter(R)TNG カレンダに依存するリソース ACL です。 Axxxx および Dxxxx 列は、サポートされているすべてのタイプのリソースについて、サポートされているすべての許可(A)権限と拒否(D)権限を示します。特定のタイプのリソースにのみ適用される特権もあります。たとえば、開始、停止、および一時停止を行う特権は、プロセスおよびサービスにのみ適用でき、ファイルには適用できません。
ACRPTDB_VERSION	DB のスキーマ バージョン。DB スキーマのアップグレードを制御するのに使用されます。
カテゴリ	リソース オブジェクト/ユーザ オブジェクト/グループ オブジェクトの B1 機能(セキュリティ カテゴリ)

名前	コメント
CONFIG	CA Access Control 設定ストア。0 個以上の設定エントリを保持します（CONFIG_ENTRY を参照）。
CONFIG_ENTRY	設定ストア内の単一の設定エントリ
DAYTIME	ユーザがリソースにアクセスできる曜日と時間帯を指定します。
DEPLOYMENT_RESULT_MESSAGE	デプロイ タスクの結果メッセージ
DEPLOYMENT_TASK	1 つのポリシー デプロイ タスク（1 つのノードで 1 つのポリシーをデプロイ/デプロイ解除」する動作）を示します。
DEPLOYMENT_TASK_GROUP	デプロイに関連した以下のタスクのうちの 1 つだけを示します。 1. ノード グループへのノードの割り当て 2. ノードへのポリシー グループの割り当て 3. ノード グループへのポリシー グループの割り当て 以上のように、タスクはバイナリです。ここで、1 番目の演算子はノードまたはポリシー グループです。2 番目の演算子はノードまたはノード グループです。
DISTRIBUTION_HOST	障害回復モード用の分散ホスト CA Access Control クラス SEOS の DH および DHDR プロパティ内の要素に対応します。
EFFECTIVE_POLICY	どのポリシーが Policy Model 内のどのノードに関連するかを示す参照。暗黙的な関係（ノード グループやポリシー グループなど介する）を含みます。
GROUPAUDIT	グループ オブジェクトの監査設定
GROUPINFO	グループ オブジェクト情報
GROUPMEMBER	このグループに属するグループ
GROUPREVACL	グループ リバース ACL。すなわち、特定の条件が与えられた場合に、特定のリソースに対してグループが有する ACL です。 Axxx 列および Dxxxx 列（許可/拒否列）のそれぞれの詳細については、ACL テーブルを参照してください。

名前	コメント
GROUPS	リソース オブジェクトおよびユーザ オブジェクトに関するグループ プロパティ。USER レコードが属するユーザ グループ（GROUP レコード）のリスト。このプロパティには、グループ管理者権限（GROUP-ADMIN）など、ユーザが属するグループ単位でユーザに割り当てられるグループ権限も含まれます。 このプロパティで設定するグループ リストは、ネイティブ環境の GROUPS プロパティで設定するユーザ リストとは異なる場合があります。
HOLDATE	休日オブジェクトの休日情報
HOSTINFO	ホスト情報は、ネットワーク内の CA Access Control エンドポイントを表します。
INETACL	INET-ACL - インターネット アクセス制御リスト ローカル ホストからクライアント ホストのグループに提供可能なサービスおよび各サービスのアクセス タイプです。アクセス制御リストの各要素には、以下の情報が含まれます。 1. サービス参照 - サービスへの参照（ポート番号または名前） すべてのサービスを指定する場合は、サービス参照としてアスタリスク（*）を入力します。 2. 許可されるアクセス - クライアント ホストが有する、サービスに対するアクセス権のタイプです。有効なアクセス タイプおよび付与されるアクセス許可は、次のとおりです。 - read - ローカル ホストは、ホスト グループにサービスを提供できます。 - none - ローカル ホストは、ホスト グループにサービスを提供できません。 Axxx 列および Dxxxx 列（許可/拒否列）のそれぞれの詳細については、ACL テーブルを参照してください。
INSERVRNGE	サービス範囲 ACL です。INETACL プロパティと同様です。ローカル ホストがクライアント ホストのグループに提供する各サービスを明示的に指定する代わりに、サービスの範囲を指定します。 Axxx 列および Dxxxx 列（許可/拒否列）のそれぞれの詳細については、ACL テーブルを参照してください。

名前	コメント
LOCAL_PMD_SUBSCRIBER	ポリシー モデル サブスクリプション エントリを表します。各エントリは sepmd -L selang コマンドによって提供される個々のサブスクリプション エントリに対応します。
LOGINAPPL	LOGINAPPL クラスは、ログイン アプリケーションを制御および検出します。これにより、ユーザはログイン アプリケーションの定義とアクセス制御ルールの設定を行い、このアプリケーションを使用してログインを制御可能です。 各列の記述には、適切な CA Access Control のクラス、プロパティ、およびそれが表す値への参照が含まれています。詳細については、「*selang リファレンス ガイド*」を参照してください。
MEMBEROF	このグループが属するグループです。
MEMBERS	リソース オブジェクトの Members プロパティです。
NODE	ポリシー準拠が適用される必要がある CA Access Control ホストを定義します。 ノード グループは、簡単なリソース エンティティで表されます（RESINFO/RESAC を参照）。 ノードとノード グループの間の関係は、ほかのリソースの場合と同様に GROUPS/MEMBERS メカニズムにより処理されます（GROUPS/MEMBERS/RESINFO テーブルを参照）。
NODE_ADDRESS	ノードの 0 個以上のネットワーク アドレスです。CA Access Control クラス HNODE の HNODE_IP プロパティに対応します。
NODE_ALIAS	ノードの 0 個以上のエイリアスです。CA Access Control クラス HNODE の ALIAS プロパティに対応します。
NODE_DEVIATION	ホストレベルの偏差の詳細です。
NODE_SUBSCRIPTION_STATUS	ポリシー配布を目的とする、さまざまな HNODE 間でのサブスクリプションの関係およびステータスを示します。
PASSWDRULES	パスワード ルールを指定します。このプロパティには、CA Access Control でのパスワード保護の処理方法を決定する多くのフィールドが含まれています。ルールの一覧については、USER クラスの変更可能なプロパティである PROFILE を参照してください。

名前	コメント
POLICY	ノードの準拠状態およびその状態を適用することが必要な操作を示します。各ポリシー エンティティは、別のポリシーの初期バージョンまたは後続バージョンのいずれかを表します。初期ポリシーは常に 1 つのポリシー グループに割り当てられます（POLICY_GROUP テーブルを参照）。そのポリシーの後続のバージョンもすべて、このポリシー グループに含められます。
OLICY_DEVIATION	ノードの有効なポリシーからのノードの偏差（ポリシー準拠）を示します。
POLICY_GROUP	同一の初期ポリシーの後続バージョンであるすべてのポリシーが含まれます。
POLICY_GROUP_DEPENDENCY	ほかのポリシー グループに依存しているポリシー グループを示します。このテーブルに、独立したポリシー グループは示されません。
POLICY_GROUP_NODE_ASSIGNMENT	Policy Model 内でどのポリシーがどのノード（またはノードのグループ）に割り当てられているかを示します。ノードにポリシーが割り当てられると、NODE_RESCLASS は HNODE になります。ノード グループにポリシーが割り当てられると、NODE_RESCLASS は GHNODE になります。 このテーブルは、ノードの割り当ておよびノード グループの割り当てに使用されます。 ポリシー グループとノード（またはノード グループ）との関係は、ほかのリソースの場合と同様に GROUPS/MEMBERS メカニズムによって処理されます（GROUPS/MEMBERS/RESINFO テーブルを参照）。
POLICY_RULESET	ポリシーとそのルールセットの間のリンクです。
POLICY_STATUS	ポリシーが関連付けられた各ノードについてポリシーのステータス（ポリシーがデプロイまたはデプロイ解除されているかどうかなど）を記述します（EFFECTIVE_POLICY を参照）。
POLICYMODELINFO	Policy Model 情報です。特定のノードによってほかのノードに配布されるポリシーに関するステータスが含まれます。
RAUDIT	CA Access Control が監査ログに記録するアクセス イベントのタイプです。

名前	コメント
RESAC	CA Access Control リソース情報です。
RESINFO	CA Access Control リソース情報です。
RULESET	ポリシーのデプロイ/デプロイ解除の一環として実行されるコマンドセットです。
RULESET_COMMAND	単一の selang コマンド。selang コマンドの多くは、ルールセットを持っています。
SEOS	設定オプションの情報です。
SEOSSYSCALL	（r12.0 SP1）CA Access Control メイン カーネル モジュールで主に OS イベントのインターセプトで使われます。これら OS イベントは seosd をクエリして許可するか拒否するかが判断されます。
SNAPSHOTINFO	スナップショット情報は単一のローカル AC データベース（単一ホスト上の）から収集された、収集時点のすべてのデータを表します。
SPECIALPGMTYPE	SPECIALPGM クラスの特殊なプログラム タイプです。プログラム情報は、AC によって自動的に生成されます。Watchdog 機能は、このプロパティに格納されている情報を自動的に検証します。情報が変更されている場合、プログラムは CA Access Control により untrusted として定義されます。 各レコードは、CA Access Control クラス SPECIALPGM の SPECIALPGMTYPE プロパティを 1 つだけ表します。
SYSCALL	（r12.0 SP1）CA Access Control メイン カーネル モジュールで主に OS イベントのインターセプトで使われます。これら OS イベントは seosd をクエリして許可するか拒否するかが判断されます。
SYSCALLUSERSPECIALPGM	（r12.0 SP1）CA Access Control メイン カーネル モジュールで主に OS イベントのインターセプトで使われます。これら OS イベントは seosd をクエリして許可するか拒否するかが判断されます。

名前	コメント
UACC	デフォルトのアクセス権限とは、オブジェクトのアクセス制御リストに含まれていないアクセサがオブジェクトへのアクセスを要求した場合に与えられる権限です。デフォルトのアクセス権限は、データベースに定義されていないユーザにも適用されます。Axxx 列および Dxxxx 列（許可/拒否列）のそれぞれの詳細については、ACL テーブルを参照してください。 各レコードは、さまざまな CA Access Control リソース クラスの UACC プロパティを表します。 Axxx 列および Dxxxx 列（許可/拒否列）のそれぞれの詳細については、ACL テーブルを参照してください。
USERAC	CA Access Control ユーザ情報です。このテーブル内の各レコードは、USER/XUSER クラスの 1 つの CA Access Control オブジェクトの AC 固有のプロパティを表します。
USERACAUDIT	CA Access Control ユーザの監査設定です。 各レコードは、CA Access Control クラス USER/XUSER の CA Access Control プロパティ AUDIT_MODE の 1 つのエントリを表します。
USERACMODE	CA Access Control のユーザ モード（OBJ_TYPE）です。 各レコードは、CA Access Control クラス USER/XUSER の CA Access Control プロパティ OBJ_TYPE の 1 つのエントリを表します。
USERGRP	グループへのユーザの接続です。 各レコードは、CA Access Control クラス USER/XUSER の CA Access Control プロパティ GROUPS の 1 つのエントリを表します。
USERINFO	基本的なユーザ情報です。各ユーザは、このテーブル内にレコードを持つ必要があります。このテーブルは、ユーザ情報のほかのセグメントを表すほかの USER テーブルの親となります。
USERLIST	グループ オブジェクトのユーザ リスト（メンバ） 各レコードは、CA Access Control クラス GROUP/XGROUP の CA Access Control プロパティ USERLIST の 1 つの OID エントリを表します。

名前	コメント
USERREVACL	ユーザ リバース ACL。すなわち、特定の条件が与えられた場合に、特定のリソースに対してユーザが有する ACL です。 Axxx 列および Dxxxx 列（許可/拒否列）のそれぞれの詳細については、ACL テーブルを参照してください。 各レコードは、CA Access Control クラス USER/XUSER の CA Access Control プロパティ REVACL の 1 つのエントリを表します。

ACL テーブルの列

次の表で、ACL テーブルの列の属性を説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	この ACL レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	この ACL レコードのホスト ID
RESCLASS	はい	NVARCHAR2(80)	NOT NULL	この ACL レコードのリソース クラス名（例: FILE、PROCESS など）
RULEKEY	はい	NVARCHAR2(256)	NOT NULL	この ACL レコードのリソース オブジェクト名
ACNAME	はい	NVARCHAR2(80)	NOT NULL	アクセサ クラス名
AONAME	はい	NVARCHAR2(256)	NOT NULL	アクセサ オブジェクト名
ACLTYPE	はい	NVARCHAR2(80)	NOT NULL	アクセス タイプ（たとえば、R = 読み取り、W = 書き込み）
ISALLOW	はい	NUMBER(1,0)	NOT NULL	このレコード内のどの列が該当するか: Axxx（許可）または Dxxx（拒否）。特に、許可 ACL エントリなのか、または拒否 ACL エントリなのか。

名前	主キー	データタイプ	NULL オプション	コメント
CONDHASH	はい	NUMBER(20,0)	NOT NULL	これは、ACLTYPE に応じて、この ACL について条件のハッシュされた値を示します。 PACL の場合、PROGRAMNAME フィールドのハッシュを表すことになります。 CACL の場合は、ハッシュは OUTCONCNAME、OUTCONONAME、HOSTCNAME、HOSTONAME を対象にします。 CALACL の場合、CALENDAR のハッシュとなります。 ACL および NACL の場合は 0 となります。
CALENDAR	いいえ	NVARCHAR2(256)	NULL	カレンダ名（CALACL レコードの場合）
PROGRAMNAME	いいえ	NVARCHAR2(256)	NULL	プログラム名（PACL レコードの場合）
OUTCONCNAME	いいえ	NVARCHAR2(80)	NULL	ACLTYPE=CACL のとき、このフィールドは Outgoing Connection クラスの名前を保持します。GROUP または XGROUP の場合、関連するレコードは GROUPINFO テーブル内にあります。USER または XUSER の場合、関連するレコードは USERINFO テーブル内にあります。 ほかの ACLTYPE 値の場合、このフィールドは NULL です。

名前	主キー	データタイプ	NULL オプション	コメント
OUTCONONAME	いいえ	NVARCHAR2(256)	NULL	ACLTYPE=CACL のとき、このフィールドは Outgoing Connection オブジェクト名を保持します。ほかの ACNAME 値の場合、このフィールドは NULL です。
HOSTCNAME	いいえ	NVARCHAR2(80)	NULL	ACLTYPE=CACL のとき、このフィールドは Host クラスの名前（すなわち「HOST」）を保持し、RESINFO テーブル内の対応するレコードと関連付けられます。ほかの ACNAME 値の場合、このフィールドは NULL です。
HOSTONAME	いいえ	NVARCHAR2(256)	NULL	ACLTYPE=CACL のとき、このフィールドは Host オブジェクトの名前を保持します。ほかの ACNAME 値の場合、このフィールドは NULL です。
AREAD	いいえ	NUMBER(1,0)	NULL	読み取りアクセス
AWRITE	いいえ	NUMBER(1,0)	NULL	書き込みアクセス
AMODIFY	いいえ	NUMBER(1,0)	NULL	変更アクセス
ACREATE	いいえ	NUMBER(1,0)	NULL	作成アクセス
AERASE	いいえ	NUMBER(1,0)	NULL	消去アクセス
AFILESCAN	いいえ	NUMBER(1,0)	NULL	ファイル スキャン アクセス
ALANGINT	いいえ	NUMBER(1,0)	NULL	
AEXEC	いいえ	NUMBER(1,0)	NULL	実行アクセス
ACHOWN	いいえ	NUMBER(1,0)	NULL	所有者変更アクセス
ACHGRP	いいえ	NUMBER(1,0)	NULL	グループ変更アクセス
ACHMOD	いいえ	NUMBER(1,0)	NULL	chmod ユーティリティ アクセスを起動
AUTIMES	いいえ	NUMBER(1,0)	NULL	ファイル/フォルダ リソース更新時間を更新するためのアクセス

名前	主キー	データタイプ	NULL オプション	コメント
ASEC	いいえ	NUMBER(1,0)	NULL	
AKILL	いいえ	NUMBER(1,0)	NULL	
ACONNECT	いいえ	NUMBER(1,0)	NULL	接続アクセス
ARENAME	いいえ	NUMBER(1,0)	NULL	リネームアクセス
APASSWORD	いいえ	NUMBER(1,0)	NULL	
AAUTHORIZED	いいえ	NUMBER(1,0)	NULL	
AXAUDIT	いいえ	NUMBER(1,0)	NULL	
ACHDIR	いいえ	NUMBER(1,0)	NULL	フォルダ リソースを現在の作業ディレクトリとして設定するアクセス
ACRSUBK	いいえ	NUMBER(1,0)	NULL	
ANOTIFY	いいえ	NUMBER(1,0)	NULL	通知アクセス
AENUM	いいえ	NUMBER(1,0)	NULL	列挙アクセス
AQUERY	いいえ	NUMBER(1,0)	NULL	クエリ アクセス
ARCTRL	いいえ	NUMBER(1,0)	NULL	
ACRLINK	いいえ	NUMBER(1,0)	NULL	
APRINT	いいえ	NUMBER(1,0)	NULL	出力アクセス
AMANAGE	いいえ	NUMBER(1,0)	NULL	管理アクセス
AMAXALLOWED	いいえ	NUMBER(1,0)	NULL	
ASTOP	いいえ	NUMBER(1,0)	NULL	停止アクセス
APAUSE	いいえ	NUMBER(1,0)	NULL	一時停止アクセス
ACONTROL	いいえ	NUMBER(1,0)	NULL	コントロール アクセス
ACHOG	いいえ	NUMBER(1,0)	NULL	
ARESUME	いいえ	NUMBER(1,0)	NULL	再開アクセス
DREAD	いいえ	NUMBER(1,0)	NULL	読み取り拒否
DWRITE	いいえ	NUMBER(1,0)	NULL	書き込み拒否
DMODIFY	いいえ	NUMBER(1,0)	NULL	変更拒否
DCREATE	いいえ	NUMBER(1,0)	NULL	作成拒否

名前	主キー	データタイプ	NULL オプション	コメント
DERASE	いいえ	NUMBER(1,0)	NULL	消去拒否
DFILESCAN	いいえ	NUMBER(1,0)	NULL	
DLANGINT	いいえ	NUMBER(1,0)	NULL	
DEXEC	いいえ	NUMBER(1,0)	NULL	実行拒否
DCHOWN	いいえ	NUMBER(1,0)	NULL	
DCHGRP	いいえ	NUMBER(1,0)	NULL	
DCHMOD	いいえ	NUMBER(1,0)	NULL	
DUTIMES	いいえ	NUMBER(1,0)	NULL	
DSEC	いいえ	NUMBER(1,0)	NULL	
DKILL	いいえ	NUMBER(1,0)	NULL	強制終了拒否
DCONNECT	いいえ	NUMBER(1,0)	NULL	接続拒否
DRENAME	いいえ	NUMBER(1,0)	NULL	リネーム拒否
DPASSWORD	いいえ	NUMBER(1,0)	NULL	
DAUTHORIZED	いいえ	NUMBER(1,0)	NULL	
DXAUDIT	いいえ	NUMBER(1,0)	NULL	
DCHDIR	いいえ	NUMBER(1,0)	NULL	
DCRSUBK	いいえ	NUMBER(1,0)	NULL	
DNOTIFY	いいえ	NUMBER(1,0)	NULL	通知拒否
DENUM	いいえ	NUMBER(1,0)	NULL	列挙拒否
DQUERY	いいえ	NUMBER(1,0)	NULL	クエリ拒否
DRCTRL	いいえ	NUMBER(1,0)	NULL	
DCRLINK	いいえ	NUMBER(1,0)	NULL	
DPRINT	いいえ	NUMBER(1,0)	NULL	
DMANAGE	いいえ	NUMBER(1,0)	NULL	管理拒否
DMAXALLOWED	いいえ	NUMBER(1,0)	NULL	
DSTOP	いいえ	NUMBER(1,0)	NULL	停止拒否

名前	主キー	データタイプ	NULL オプション	コメント
DPAUSE	いいえ	NUMBER(1,0)	NULL	一時停止拒否
DCONTROL	いいえ	NUMBER(1,0)	NULL	コントロール拒否
DCHOG	いいえ	NUMBER(1,0)	NULL	
DRESUME	いいえ	NUMBER(1,0)	NULL	再開拒否

ACRPTDB_VERSION テーブルの列

次の表で、ACRPTDB_VERSION テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
VERSION_ID	いいえ	NUMBER(1,0)	NOT NULL	この値は常に 1 であることが必要です。
MAJOR_VERSION	いいえ	NVARCHAR2(20)	NULL	メジャー バージョン
MINOR_VERSION	いいえ	NVARCHAR2(20)	NULL	マイナー バージョン

CATEGORY テーブルの列

次の表で、CATEGORY テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID
CNAME	はい	NVARCHAR2(80)	NOT NULL	レコードのクラス名
ONAME	はい	NVARCHAR2(256)	NOT NULL	レコードのオブジェクト名

名前	主キー	データタイプ	NULL オプション	コメント
カテゴリ	はい	NVARCHAR2(256)	NOT NULL	レコードのカテゴリ名。リソースに 1 つ以上のセキュリティ カテゴリが割り当てられている場合は、リソースに割り当てられているすべての強調セキュリティ カテゴリがユーザのセキュリティ カテゴリ リストに含まれている場合にのみ、ユーザにリソースへのアクセス権が与えられます。

CONFIG テーブルの列

次の表で、CONFIG テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
CONFIGNAME	はい	NVARCHAR2(256)	NOT NULL	レコードのカテゴリ名。リソースに 1 つ以上のセキュリティ カテゴリが割り当てられている場合は、リソースに割り当てられているすべての強調セキュリティ カテゴリがユーザのセキュリティ カテゴリ リストに含まれている場合にのみ、ユーザにリソースへのアクセス権が与えられます。

CONFIG_ENTRY テーブルの列

次の表で、CONFIG_ENTRY テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
CONFIGNAME	はい	NVARCHAR2(256)	NOT NULL	環境設定ストアの名前
ENTRYID	はい	NVARCHAR2(256)	NOT NULL	環境設定エントリ名
ENTRYTYPE	はい	NVARCHAR2(80)	NOT NULL	config エントリ タイプ。「section」という値の場合、このエントリの VALUE および VALUETYPE は NULL です。
SECTION	いいえ	NVARCHAR2(256)	NOT NULL	エントリのセクション名。ENRYTYPE=section の場合、このフィールドはセクションの名前と一致します。そうでない場合、このフィールドはこのエントリを含むセクションの名前と一致します。
ENTRYNAME	いいえ	NVARCHAR2(256)	NULL	環境設定エントリ名。この列は、トークン要素である AC config の NAME プロパティに対応します。
VALUETYPE	いいえ	NVARCHAR2(20)	NULL	ENTRYTYPE が NULL 以外の場合のエントリ値のタイプ
VALUE	いいえ	NVARCHAR2(256)	NULL	ENTRYTYPE が NULL 以外の場合のエントリの値

DAYTIME テーブルの列

次の表で、DAYTIME テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID
CNAME	はい	NVARCHAR2(80)	NOT NULL	レコードのクラス名
ONAME	はい	NVARCHAR2(256)	NOT NULL	レコードのオブジェクト名
SUNDAY	いいえ	NUMBER(1,0)	NULL	日曜日にアクセス可
MONDAY	いいえ	NUMBER(1,0)	NULL	月曜日にアクセス可
TUESDAY	いいえ	NUMBER(1,0)	NULL	火曜日にアクセス可
WEDNESDAY	いいえ	NUMBER(1,0)	NULL	水曜日にアクセス可
THURSDAY	いいえ	NUMBER(1,0)	NULL	木曜日にアクセス可
FRIDAY	いいえ	NUMBER(1,0)	NULL	金曜日にアクセス可
SATURDAY	いいえ	NUMBER(1,0)	NULL	土曜日にアクセス可
STARTTIME	いいえ	TIMESTAMP(6)	NULL	開始時刻より後にアクセス可
ENDTIME	いいえ	TIMESTAMP(6)	NULL	終了時刻より前にアクセス可

DEPLOYMENT_RESULT_MESSAGE テーブルの列

次の表で、DEPLOYMENT_RESULT_MESSAGE テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子

名前	主キー	データタイプ	NULL オプション	コメント
RESCLASS	はい	NVARCHAR2(80)	NOT NULL	アクセス許可が適用されるエンティティのリソース クラス。リソースの AC OID の CNAME に対応します。
RULEKEY	はい	NVARCHAR2(256)	NOT NULL	CA CA-ACF2 : アクセス許可が見つかったルールのルール セット キー。 CA Top Secret : リソースの Owned Resource マスク。 リソースの AC OID の ONAME に対応します。
MESSAGEIDX	はい	NUMBER	NOT NULL	メッセージが順番に表示されます。この列はメッセージのインデックスを表し、ほかのメッセージに対する位置を示します。AC クラス DEPLOYMENT の AC プロパティ RESULT_MESSAGE のコマンドインデックス コンポーネントに対応します。
MESSSAGESTR	はい	NVARCHAR2(256)	NULL	メッセージの本文。AC クラス DEPLOYMENT の AC プロパティ RESULT_MESSAGE のコマンド文字列コンポーネントに対応します。

DEPLOYMENT_TASK テーブルの列

次の表で、DEPLOYMENT_TASK テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子

名前	主キー	データタイプ	NULL オプション	コメント
RESCLASS	はい	NVARCHAR2(80)	NOT NULL	アクセス許可が適用されるエンティティのリソース クラス。リソースの AC OID の CNAME に対応します。
RULEKEY	はい	NVARCHAR2(256)	NOT NULL	CA ACF2: アクセス許可が見つかったルールのルール セット キー。CA Top Secret: リソースの Owned Resource マスク。リソースの AC OID の ONAME に対応します。
POLICYGRP_RESCLASS	いいえ	NVARCHAR2(80)	NULL	アクセス許可が適用されるエンティティのリソース クラス。DEPLOYMENT クラスの AC OID プロパティ GPOLICY の CNAME に対応します。
POLICYGRP_RULEKEY	いいえ	NVARCHAR2(256)	NULL	CA ACF2: アクセス許可が見つかったルールのルール セット キー。CA Top Secret: リソースの Owned Resource マスク。DEPLOYMENT クラスの AC OID プロパティ GPOLICY の ONAME に対応します。
CHECKERTYPE	いいえ	NVARCHAR2(80)	NULL	このユーザの AC クラス（USER、XUSER）DEPLOYMENT クラスの AC OID プロパティ CHECKER の CNAME に対応します。
CHECKERID	いいえ	NVARCHAR2(256)	NULL	このオブジェクトのシステム上での識別子。DEPLOYMENT クラスの AC OID プロパティ CHECKER の ONAME に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
NODE_RESCLASS	いいえ	NVARCHAR2(80)	NULL	アクセス許可が適用されるエンティティのリソース クラス。DEPLOYMENT クラスの AC OID プロパティ HNODEY の CNAME に対応します。
NODE_RULEKEY	いいえ	NVARCHAR2(256)	NULL	CA ACF2: アクセス許可が見つかったルールのルール セット キー。CA Top Secret: リソースの Owned Resource マスク。DEPLOYMENT クラスの AC OID プロパティ HNODE の ONAME に対応します。
POLICY_RESCLASS	いいえ	NVARCHAR2(80)	NULL	アクセス許可が適用されるエンティティのリソース クラス。DEPLOYMENT クラスの AC OID プロパティ POLICY の CNAME に対応します。
POLICY_RULEKEY	いいえ	NVARCHAR2(256)	NULL	CA ACF2: アクセス許可が見つかったルールのルール セット キー。CA Top Secret: リソースの Owned Resource マスク。DEPLOYMENT クラスの AC OID プロパティ POLICY の ONAME に対応します。
MAKERID	いいえ	NVARCHAR2(256)	NULL	このオブジェクトのシステム上での識別子。DEPLOYMENT クラスの AC OID プロパティ MAKER の ONAME に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
MAKERTYPE	いいえ	NVARCHAR2(80)	NULL	maker のクラス。値が USER および XUSER の場合、maker レコードは USERINFO テーブル内にあります。値が GROUP または XGROUP の場合は、GROUPINFO テーブル内にあります。DEPLOYMENT クラスの AC OID プロパティ MAKER の CNAME に対応します。
CHECKERCOMMENT	いいえ	NVARCHAR2(256)	NULL	チェッカによって作成されるコメント。DEPLOYMENT クラスの AC プロパティ CHECKER_COMMENT に対応します。
CHECKERTIME	いいえ	TIMESTAMP(6)	NULL	チェック タイムスタンプ。DEPLOYMENT クラスの AC プロパティ CHECKER_TIME に対応します。
DMSNAME	いいえ	NVARCHAR2(256)	NULL	このタスクを生成した DMS の名前。DEPLOYMENT クラスの AC プロパティ DMS_NAME に対応します。
OPERATION	いいえ	NVARCHAR2(256)	NULL	このタスクで実行する必要がある操作（DEPLOY、UNDEPLOY）。DEPLOYMENT クラスの AC プロパティ OPERATION に対応します。
STATUS	いいえ	NVARCHAR2(256)	NULL	タスクのステータス（SUCCESS、WARNING、FAIL、NOACTION）。DEPLOYMENT クラスの AC プロパティ STATUS に対応します。

DEPLOYMENT_TASK_GROUP テーブルの列

次の表で、DEPLOYMENT_TASK_GROUP テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
RESCLASS	はい	NVARCHAR2(80)	NOT NULL	アクセス許可が適用されるエンティティのリソース クラス。リソースの AC OID の CNAME に対応します。
RULEKEY	はい	NVARCHAR2(256)	NOT NULL	CA ACF2: アクセス許可が見つかったルールのルール セット キー。CA Top Secret: リソースの Owned Resource マスク。 リソースの AC OID の ONAME に対応します。
POLICYGRP_RESCLASS	いいえ	NVARCHAR2(80)	NULL	アクセス許可が適用されるエンティティのリソース クラス。GDEPLOYMENT クラスの AC OID プロパティ POLICY の CNAME に対応します。
POLICYGRP_RULEKEY	いいえ	NVARCHAR2(256)	NULL	CA ACF2: アクセス許可が見つかったルールのルール セット キー。CA Top Secret: リソースの Owned Resource マスク。 GDEPLOYMENT クラスの AC OID プロパティ POLICY の ONAME に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
NODEGRP_RESCLASS	いいえ	NVARCHAR2(80)	NULL	アクセス許可が適用されるエンティティのリソース クラス。GDEPLOYMENT クラスの AC OID プロパティ GHNODE の CNAME に対応します。
NODEGRP_RULEKEY	いいえ	NVARCHAR2(256)	NULL	CA ACF2：アクセス許可が見つかったルールのルール セット キー。CA Top Secret：リソースの Owned Resource マスク。GDEPLOYMENT クラスの AC OID プロパティ GHNODE の ONAME に対応します。
NODE_RESCLASS	いいえ	NVARCHAR2(80)	NULL	アクセス許可が適用されるエンティティのリソース クラス。GDEPLOYMENT クラスの AC OID プロパティ HNODE の CNAME に対応します。
NODE_RULEKEY	いいえ	NVARCHAR2(256)	NULL	CA ACF2：アクセス許可が見つかったルールのルール セット キー。CA Top Secret：リソースの Owned Resource マスク。GDEPLOYMENT クラスの AC OID プロパティ HNODE の ONAME に対応します。
TRIG	いいえ	NVARCHAR2(256)	NULL	このタスク グループのトリガ（ASSIGN、UNASSIGN、DIRECTDEPLOY、DIRECTUNDEPLOY）。GDEPLOYMENT クラスの AC プロパティ TRIGGER に対応します。

DISTRIBUTION_HOST テーブルの列

次の表で、DISTRIBUTION_HOST テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
DH	はい	NVARCHAR2(256)	NOT NULL	DHTYPE 列の値に応じて、AC クラス SEOS の DH または DHDR プロパティ内の 1 つの要素に対応します。
DHTYPE	はい	NVARCHAR2(20)	NOT NULL	DHTYPE が「DR」である場合、DH 列は AC クラス SEOS の DHDR プロパティ内の 1 つの要素に対応します。 DHTYPE が「NORMAL」である場合、DH 列はこのクラスの DH プロパティに対応します。

EFFECTIVE_POLICY テーブルの列

次の表で、EFFECTIVE_POLICY テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子

名前	主キー	データタイプ	NULL オプション	コメント
NODE_RESCLASS	はい	NVARCHAR2(80)	NOT NULL	アクセス許可が適用されるエンティティのリソース クラス。リソースの AC OID の CNAME に対応します。
NODE_RULEKEY	はい	NVARCHAR2(256)	NOT NULL	CA ACF2 : アクセス許可が見つかったルールのルール セット キー。CA Top Secret : リソースの Owned Resource マスク。リソースの AC OID の ONAME に対応します。
POLICY_RESCLASS	はい	NVARCHAR2(80)	NOT NULL	アクセス許可が適用されるエンティティのリソース クラス。リソースの AC OID の CNAME に対応します。
POLICY_RULEKEY	はい	NVARCHAR2(256)	NOT NULL	CA ACF2 : アクセス許可が見つかったルールのルール セット キー。CA Top Secret : リソースの Owned Resource マスク。リソースの AC OID の ONAME に対応します。

GROUPAUDIT テーブルの列

次の表で、GROUPAUDIT テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID
GROUPID	はい	NVARCHAR2(256)	NOT NULL	レコードのグループ ID（名）
GROUPTYPE	はい	NVARCHAR2(80)	NOT NULL	グループのクラス（GROUP、XGROUP など）。AC グループ OID の CNAME に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
SUCCESS	いいえ	NUMBER(1,0)	NULL	成功したイベントを監査
FAILURE	いいえ	NUMBER(1,0)	NULL	失敗したイベントを監査
LOGONSUCCESS	いいえ	NUMBER(1,0)	NULL	成功したログオンを監査
LOGONFAILURE	いいえ	NUMBER(1,0)	NULL	失敗したログオンを監査
DEBUG	いいえ	NUMBER(1,0)	NULL	デバッグ モード以降のログ
TRACE	いいえ	NUMBER(1,0)	NULL	グループのトレース

GROUPINFO テーブルの列

次の表で、GROUPINFO テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID
GROUPID	はい	NVARCHAR2(256)	NOT NULL	レコードのグループ ID（名） AC グループ OID の ONAME に対応します。
GROUPTYPE	はい	NVARCHAR2(80)	NOT NULL	グループのクラス（GROUP、XGROUP など）。AC グループ OID の CNAME に対応します。
DESCRIPTION	いいえ	NVARCHAR2(256)	NULL	グループの説明およびコメント。AC クラス GROUP/XGROUP の AC プロパティ COMMENT に割り当てられます。

名前	主キー	データタイプ	NULL オプション	コメント
OWNERCNAME	いいえ	NVARCHAR2(256)	NULL	リソース レコードの所有者には、リソースに対する無制限のアクセス権が与えられます。ただし、前提として、所有者のセキュリティ レベル、セキュリティ ラベル、およびセキュリティ カテゴリに、リソースへのアクセスを許可する適切な権限が設定されている必要があります。リソースの所有者には、リソース レコードを更新および削除する権限が常に与えられます。AC クラス GROUP/XGROUP の AC プロパティ OWNER の CNAME に対応します。
OWNERONAME	いいえ	NVARCHAR2(256)	NULL	AC クラス GROUP/XGROUP の AC プロパティ OWNER の ONAME に対応します。
FULLNAME	いいえ	NVARCHAR2(256)	NULL	グループに関連付けられたフル ネーム。AC クラス GROUP/XGROUP の AC プロパティ FULL_NAME に対応します。
SUPGROUP	いいえ	NVARCHAR2(256)	NULL	親グループ（上位強調グループ）の名前です。AC クラス GROUP/XGROUP の AC プロパティ SUPGROUP に対応します。
CALENDAR	いいえ	NVARCHAR2(256)	NULL	Unicenter TNG で時間帯制限を表す Unicenter TNG カレンダ オブジェクトを指定します。AC は、これらのオブジェクトのリストを管理目的のみに使用し、オブジェクトを保護しません。AC クラス GROUP/XGROUP の AC プロパティ CALENDAR に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
CRETIME	いいえ	TIMESTAMP(6)	NULL	作成日時。AC クラス GROUP/XGROUP の AC プロパティ CREATE_TIME に対応します。
UPDTIME	いいえ	TIMESTAMP(6)	NULL	レコードが最後に変更された日時です。
UPDWHOCNAME	いいえ	NVARCHAR2(256)	NULL	レコードが最後に変更された日時です。AC クラス GROUP/XGROUP の AC プロパティ UPDATE_TIME に対応します。
UPDWHOONAME	いいえ	NVARCHAR2(256)	NULL	AC クラス GROUP/XGROUP の AC プロパティ UPDATE_WHO の ONAME に対応します。
HOMEDIR	いいえ	NVARCHAR2(256)	NULL	新しいグループ メンバに割り当てられるホーム ディレクトリです。AC クラス GROUP/XGROUP の AC プロパティ HOMEDIR に対応します。
EXPDATE	いいえ	DATE	NULL	グループ メンバのアカウントが失効する日付を設定します。AC クラス GROUP/XGROUP の AC プロパティ EXPIRE_DATE に対応します。
MAXLOGINS	いいえ	NUMBER	NULL	ユーザが同時にログインできる端末の最大数を設定します。値 0(ゼロ)は、ユーザが任意の数の端末から同時にログインできることを意味します。AC クラス GROUP/XGROUP の AC プロパティ MAXLOGINS に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
INACTIVE	いいえ	NUMBER	NULL	ユーザのステータスがシステムによって非アクティブに変更されるまでの必要経過日数を指定します。AC クラス GROUP/XGROUP の AC プロパティ INACTIVE に対応します。
PROFUSRCNAME	いいえ	NVARCHAR2(256)	NULL	AC クラス GROUP/XGROUP の AC プロパティ PROFUSR の CNAME に対応します。
PROFUSRONAME	いいえ	NVARCHAR2(256)	NULL	AC クラス GROUP/XGROUP の AC プロパティ PROFUSR の ONAME に対応します。
PWDAUTOGEN	いいえ	NUMBER(1,0)	NULL	アプリケーション パスワードをポリシー サーバで自動的に生成するかどうかを指定します。AC クラス GROUP/XGROUP の AC プロパティ PWD_AUTOGEN に対応します。
PWDSYNC	いいえ	NUMBER(1,0)	NULL	アプリケーション パスワードをユーザのほかのアプリケーションのパスワードと同一にするかどうかを指定します。AC クラス GROUP/XGROUP の AC プロパティ PWD_SYNC に対応します。
PWPOLICY	いいえ	NVARCHAR2(256)	NULL	アプリケーションに適用するパスワード ポリシーのレコード名。AC クラス GROUP/XGROUP の AC プロパティ PWPOLICY に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
RESDATE	いいえ	DATE	NULL	suspend パラメータを指定して無効にしたユーザ レコードを有効にします。AC クラス GROUP/XGROUP の AC プロパティ RESUME_DATE に対応します。
SHELL	いいえ	NVARCHAR2(256)	NULL	ユーザが login コマンドまたは su コマンドを起動した後に実行される初期プログラムまたはシェルの完全パスを指定します。AC クラス GROUP/XGROUP の AC プロパティ SHELL に対応します。
SUBGROUP	いいえ	NVARCHAR2(256)	NULL	このグループが親に指定されているグループのリストです。AC クラス GROUP/XGROUP の AC プロパティ SUBGROUP に対応します。
SUSDATE	いいえ	TIMESTAMP(6)	NULL	ユーザ レコードを無効にします。ただし、データベースには定義を残します。AC クラス GROUP/XGROUP の AC プロパティ SUSPEND_DATE に対応します。
SUSWHOCNAME	いいえ	NVARCHAR2(256)	NULL	一時停止日をアクティブにした管理者のクラス。AC クラス GROUP/XGROUP の AC プロパティ SUSPEND_WHO の CNAME に対応します。
SUSWHOONAME	いいえ	NVARCHAR2(256)	NULL	一時停止日をアクティブにした管理者のオブジェクト名。AC クラス GROUP/XGROUP の AC プロパティ SUSPEND_WHO の ONAME に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
SECURITYID	いいえ	NVARCHAR2(256)	NULL	このグループ エントリに対するベンダ固有のセキュリティ ID。AC クラス XGROUP の AC プロパティ SECURITY_ID に対応します。

GROUPMEMBER テーブルの列

次の表で、GROUPMEMBER テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID
GROUPID	はい	NVARCHAR2(256)	NOT NULL	レコードのグループ ID（名）
CNAME	はい	NVARCHAR2(256)	NOT NULL	メンバのクラス名
ONAME	はい	NVARCHAR2(256)	NOT NULL	メンバのオブジェクト名
GROUPTYPE	はい	NVARCHAR2(80)	NOT NULL	グループのクラス（GROUP、XGROUP など）。AC グループ OID の CNAME に対応します。

GROUPREVACL テーブルの列

次の表で、GROUPREVACL テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID
GROUPID	はい	NVARCHAR2(256)	NOT NULL	レコードのグループ ID（名）

名前	主キー	データタイプ	NULL オプション	コメント
GROUPTYPE	はい	NVARCHAR2(80)	NOT NULL	グループのクラス（GROUP、XGROUP など）。AC グループ OID の CNAME に対応します。
RESCNAME	はい	NVARCHAR2(80)	NOT NULL	リソース クラス名
RESONAME	はい	NVARCHAR2(256)	NOT NULL	リソース オブジェクト名
CONCNAME	はい	NVARCHAR2(80)	NOT NULL	条件クラス名（すなわち、PROGRAM、HOST、CALENDAR）。文字列が空でない場合、RESINFO テーブルに条件オブジェクトが存在することを示しています。ハイフン文字列（「-」）は、「無条件」を意味します。
CONONAME	はい	NVARCHAR2(256)	NOT NULL	条件オブジェクト名
ISALLOW	はい	NVARCHAR2(256)	NOT NULL	
AREAD	いいえ	NUMBER(1,0)	NULL	
AWRITE	いいえ	NUMBER(1,0)	NULL	
AMODIFY	いいえ	NUMBER(1,0)	NULL	
ACREATE	いいえ	NUMBER(1,0)	NULL	
AERASE	いいえ	NUMBER(1,0)	NULL	
AFILESCAN	いいえ	NUMBER(1,0)	NULL	
ALANGINT	いいえ	NUMBER(1,0)	NULL	
AEXEC	いいえ	NUMBER(1,0)	NULL	
ACHOWN	いいえ	NUMBER(1,0)	NULL	
ACHGRP	いいえ	NUMBER(1,0)	NULL	
ACHMOD	いいえ	NUMBER(1,0)	NULL	
AUTIMES	いいえ	NUMBER(1,0)	NULL	
ASEC	いいえ	NUMBER(1,0)	NULL	

名前	主キー	データタイプ	NULL オプション	コメント
AKILL	いいえ	NUMBER(1,0)	NULL	
ACONNECT	いいえ	NUMBER(1,0)	NULL	
ARENAME	いいえ	NUMBER(1,0)	NULL	
APASSWORD	いいえ	NUMBER(1,0)	NULL	
AAUTHORIZED	いいえ	NUMBER(1,0)	NULL	
AXAUDIT	いいえ	NUMBER(1,0)	NULL	
ACHDIR	いいえ	NUMBER(1,0)	NULL	
ACRSUBK	いいえ	NUMBER(1,0)	NULL	
ANOTIFY	いいえ	NUMBER(1,0)	NULL	
AENUM	いいえ	NUMBER(1,0)	NULL	
AQUERY	いいえ	NUMBER(1,0)	NULL	
ARCTRL	いいえ	NUMBER(1,0)	NULL	
ACRLINK	いいえ	NUMBER(1,0)	NULL	
APRINT	いいえ	NUMBER(1,0)	NULL	
AMANAGE	いいえ	NUMBER(1,0)	NULL	
AMAXALLOWED	いいえ	NUMBER(1,0)	NULL	
ASTOP	いいえ	NUMBER(1,0)	NULL	
APAUSE	いいえ	NUMBER(1,0)	NULL	
ACONTROL	いいえ	NUMBER(1,0)	NULL	
ACHOG	いいえ	NUMBER(1,0)	NULL	
ARESUME	いいえ	NUMBER(1,0)	NULL	
DREAD	いいえ	NUMBER(1,0)	NULL	
DWRITE	いいえ	NUMBER(1,0)	NULL	
DMODIFY	いいえ	NUMBER(1,0)	NULL	
DCREATE	いいえ	NUMBER(1,0)	NULL	
DERASE	いいえ	NUMBER(1,0)	NULL	

名前	主キー	データタイプ	NULL オプション	コメント
DFILESCAN	いいえ	NUMBER(1,0)	NULL	
DLANGINT	いいえ	NUMBER(1,0)	NULL	
DEXEC	いいえ	NUMBER(1,0)	NULL	
DCHOWN	いいえ	NUMBER(1,0)	NULL	
DCHGRP	いいえ	NUMBER(1,0)	NULL	
DCHMOD	いいえ	NUMBER(1,0)	NULL	
DUTIMES	いいえ	NUMBER(1,0)	NULL	
DSEC	いいえ	NUMBER(1,0)	NULL	
DKILL	いいえ	NUMBER(1,0)	NULL	
DCONNECT	いいえ	NUMBER(1,0)	NULL	
DRENAME	いいえ	NUMBER(1,0)	NULL	
DPASSWORD	いいえ	NUMBER(1,0)	NULL	
DAUTHORIZED	いいえ	NUMBER(1,0)	NULL	
DXAUDIT	いいえ	NUMBER(1,0)	NULL	
DCHDIR	いいえ	NUMBER(1,0)	NULL	
DCRSUBK	いいえ	NUMBER(1,0)	NULL	
DNOTIFY	いいえ	NUMBER(1,0)	NULL	
DENUM	いいえ	NUMBER(1,0)	NULL	
DQUERY	いいえ	NUMBER(1,0)	NULL	
DRCTRL	いいえ	NUMBER(1,0)	NULL	
DCRLINK	いいえ	NUMBER(1,0)	NULL	
DPRINT	いいえ	NUMBER(1,0)	NULL	
DMANAGE	いいえ	NUMBER(1,0)	NULL	
DMAXALLOWED	いいえ	NUMBER(1,0)	NULL	
DSTOP	いいえ	NUMBER(1,0)	NULL	
DPAUSE	いいえ	NUMBER(1,0)	NULL	

名前	主キー	データタイプ	NULL オプション	コメント
DCONTROL	いいえ	NUMBER(1,0)	NULL	
DCHOG	いいえ	NUMBER(1,0)	NULL	
DRESUME	いいえ	NUMBER(1,0)	NULL	

GROUPS テーブルの列

次の表で、GROUPS テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID
RESCLASS	はい	NVARCHAR2(80)	NOT NULL	リソース クラス名
RULEKEY	はい	NVARCHAR2(256)	NOT NULL	リソース オブジェクト名
ONAME	はい	NVARCHAR2(256)	NOT NULL	グループ内の参加オブジェクトのオブジェクト名
CNAME	はい	NVARCHAR2(80)	NOT NULL	グループ内の参加オブジェクトのクラス名

HOLDATE テーブルの列

次の表で、HOLDATE テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(256)	NOT NULL	レコードのホスト ID
RESCLASS	はい	NVARCHAR2(80)	NOT NULL	リソース クラス名（HOLIDAY とする必要があります）

名前	主キー	データタイプ	NULL オプション	コメント
RULEKEY	はい	NVARCHAR2(256)	NOT NULL	リソース オブジェクト名
STARTDATE	はい	TIMESTAMP(6)	NOT NULL	休日の開始日
ENDDATE	はい	TIMESTAMP(6)	NOT NULL	休日の終了日
ALLDAY	はい	NUMBER(1,0)	NULL	この場合、休日は終日イベントです。
EVERYYEAR	はい	NUMBER(1,0)	NULL	この場合、休日は毎年発生します。

HOSTINFO テーブルの列

次の表で、HOSTINFO テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
APPNAME	いいえ	NVARCHAR2(24)	NULL	セキュリティ データを含むセキュリティ アプリケーション名
APPIND	いいえ	CHAR(1)	NULL	アプリケーション インジケータ。このレコードが属するアプリケーションを示します。
APPVERSION	いいえ	NVARCHAR2(24)	NULL	セキュリティ アプリケーションのバージョン
APPMODE	いいえ	CHAR(1)	NULL	このレコードの有効な処理モード
LOADDATE	いいえ	TIMESTAMP(6)	NULL	セキュリティ情報がセキュリティ データベースからアンロードされた日付
BASE_HOSTID	いいえ	NVARCHAR2(512)	NULL	格納ホスト ID（存在する場合）

INETACL テーブルの列

次の表で、INETACL テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
RESCLASS	はい	NVARCHAR2(80)	NOT NULL	リソース クラス名
RULEKEY	はい	NVARCHAR2(256)	NOT NULL	リソース オブジェクト名
SERVICENAME	はい	NVARCHAR2(256)	NOT NULL	サービス名
PROTOCOLNAME	はい	NVARCHAR2(256)	NOT NULL	プロトコル名
AREAD	いいえ	NUMBER(1,0)	NULL	
AWRITE	いいえ	NUMBER(1,0)	NULL	
AMODIFY	いいえ	NUMBER(1,0)	NULL	
ACREATE	いいえ	NUMBER(1,0)	NULL	
AERASE	いいえ	NUMBER(1,0)	NULL	
AFILESCAN	いいえ	NUMBER(1,0)	NULL	
ALANGINT	いいえ	NUMBER(1,0)	NULL	
AEXEC	いいえ	NUMBER(1,0)	NULL	
ACHOWN	いいえ	NUMBER(1,0)	NULL	
ACHGRP	いいえ	NUMBER(1,0)	NULL	
ACHMOD	いいえ	NUMBER(1,0)	NULL	
AUTIMES	いいえ	NUMBER(1,0)	NULL	
ASEC	いいえ	NUMBER(1,0)	NULL	
AKILL	いいえ	NUMBER(1,0)	NULL	
ACONNECT	いいえ	NUMBER(1,0)	NULL	

名前	主キー	データタイプ	NULL オプション	コメント
ARENAME	いいえ	NUMBER(1,0)	NULL	
APASSWORD	いいえ	NUMBER(1,0)	NULL	
AAUTHORIZED	いいえ	NUMBER(1,0)	NULL	
AXAUDIT	いいえ	NUMBER(1,0)	NULL	
ACHDIR	いいえ	NUMBER(1,0)	NULL	
ACRSUBK	いいえ	NUMBER(1,0)	NULL	
ANOTIFY	いいえ	NUMBER(1,0)	NULL	
AENUM	いいえ	NUMBER(1,0)	NULL	
AQUERY	いいえ	NUMBER(1,0)	NULL	
ARCTRL	いいえ	NUMBER(1,0)	NULL	
ACRLINK	いいえ	NUMBER(1,0)	NULL	
APRINT	いいえ	NUMBER(1,0)	NULL	
AMANAGE	いいえ	NUMBER(1,0)	NULL	
AMAXALLOWED	いいえ	NUMBER(1,0)	NULL	
ASTOP	いいえ	NUMBER(1,0)	NULL	
APAUSE	いいえ	NUMBER(1,0)	NULL	
ACONTROL	いいえ	NUMBER(1,0)	NULL	
ACHOG	いいえ	NUMBER(1,0)	NULL	
ARESUME	いいえ	NUMBER(1,0)	NULL	

INSERVRNGE テーブルの列

次の表で、INSERVRNGE テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID

名前	主キー	データタイプ	NULL オプション	コメント
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
RESCLASS	はい	NVARCHAR2(80)	NOT NULL	アクセス許可が適用されるエンティティのリソース クラス。
RULEKEY	はい	NVARCHAR2(256)	NOT NULL	CA ACF2: アクセス許可が見つかったルールのルール セット キー。CA Top Secret: リソースの Owned Resource マスク。AC: リソース オブジェクト名
MINSERVICE	はい	NUMBER	NOT NULL	最小ポート数
MAXSERVICE	はい	NUMBER	NOT NULL	最大ポート数
AREAD	いいえ	NUMBER(1,0)	NULL	
AWRITE	いいえ	NUMBER(1,0)	NULL	
AMODIFY	いいえ	NUMBER(1,0)	NULL	
ACREATE	いいえ	NUMBER(1,0)	NULL	
AERASE	いいえ	NUMBER(1,0)	NULL	
AFILESCAN	いいえ	NUMBER(1,0)	NULL	
ALANGINT	いいえ	NUMBER(1,0)	NULL	
AEXEC	いいえ	NUMBER(1,0)	NULL	
ACHOWN	いいえ	NUMBER(1,0)	NULL	
ACHGRP	いいえ	NUMBER(1,0)	NULL	
ACHMOD	いいえ	NUMBER(1,0)	NULL	
AUTIMES	いいえ	NUMBER(1,0)	NULL	
ASEC	いいえ	NUMBER(1,0)	NULL	
AKILL	いいえ	NUMBER(1,0)	NULL	
ACONNECT	いいえ	NUMBER(1,0)	NULL	
ARENAME	いいえ	NUMBER(1,0)	NULL	

名前	主キー	データタイプ	NULL オプション	コメント
APASSWORD	いいえ	NUMBER(1,0)	NULL	
AAUTHORIZED	いいえ	NUMBER(1,0)	NULL	
AXAUDIT	いいえ	NUMBER(1,0)	NULL	
ACHDIR	いいえ	NUMBER(1,0)	NULL	
ACRSUBK	いいえ	NUMBER(1,0)	NULL	
ANOTIFY	いいえ	NUMBER(1,0)	NULL	
AENUM	いいえ	NUMBER(1,0)	NULL	
AQUERY	いいえ	NUMBER(1,0)	NULL	
ARCTRL	いいえ	NUMBER(1,0)	NULL	
ACRLINK	いいえ	NUMBER(1,0)	NULL	
APRINT	いいえ	NUMBER(1,0)	NULL	
AMANAGE	いいえ	NUMBER(1,0)	NULL	
AMAXALLOWED	いいえ	NUMBER(1,0)	NULL	
ASTOP	いいえ	NUMBER(1,0)	NULL	
APAUSE	いいえ	NUMBER(1,0)	NULL	
ACONTROL	いいえ	NUMBER(1,0)	NULL	
ACHOG	いいえ	NUMBER(1,0)	NULL	
ARESUME	いいえ	NUMBER(1,0)	NULL	

LOCAL_PMD_SUBSCRIBER テーブルの列

次の表で、LOCAL_PMD_SUBSCRIBER テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID

名前	主キー	データタイプ	NULL オプション	コメント
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
SUBSCRIBER_HOSTID	はい	NVARCHAR2(256)	NOT NULL	サブスクライバ Policy Model。sepmd -L selang コマンド出力の Subscriber 列に対応します。
ERRORCOUNT	いいえ	NUMBER	NULL	サブスクリプション エラー カウント。sepmd -L selang コマンド出力の Errors 列に対応します。
STATUS	いいえ	NVARCHAR2(256)	NULL	サブスクリプションのステータスの説明。sepmd -L selang コマンド出力の Flag 列に対応します。
OFFSET	いいえ	NUMBER	NULL	配布されるポリシーのファイルにある現在のサブスクリプション オフセット。sepmd -L selang コマンド出力の Offset 列に対応します。
NEXTCOMMAND	いいえ	NVARCHAR2(256)	NULL	配布されるポリシーのファイルにある現在のサブスクリプション コマンド。sepmd -L selang コマンド出力の Next Command 列に対応します。

LOGINAPPL テーブルの列

次の表で、LOGINAPPL テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID

名前	主キー	データタイプ	NULL オプション	コメント
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
RESCLASS	はい	NVARCHAR2(80)	NOT NULL	アクセス許可が適用されるエンティティのリソース クラス。リソースの AC OID の CNAME に対応します。
RULEKEY	はい	NVARCHAR2(256)	NOT NULL	CA ACF2 : アクセス許可が見つかったルールのルール セット キー。CA Top Secret : リソースの Owned Resource マスク。リソースの AC OID の ONAME に対応します。
LOGINHOW	いいえ	NVARCHAR2(256)	NULL	ログインの方法（pseudo、normal など）。AC クラス LOGINAPPL の LOGINHOW プロパティに対応します。
LOGINPATH	いいえ	NVARCHAR2(256)	NULL	ログイン アプリケーションの完全パス（または包括的なパス）です。AC クラス LOGINAPPL の LOGINPATH プロパティに対応します。
FNFSPGM	いいえ	NUMBER(1,0)	NULL	AC クラス LOGINAPPL の LOGINFLAG プロパティのログインフラグ NFSPGM に対応します。
FINOGRACE	いいえ	NUMBER(1,0)	NULL	AC クラス LOGINAPPL の LOGINFLAG プロパティのログインフラグ nograce に対応します。
FINOGRACEROOT	いいえ	NUMBER(1,0)	NULL	AC クラス LOGINAPPL の LOGINFLAG プロパティのログインフラグ nograceroot に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
FNOLOGIN	いいえ	NUMBER(1,0)	NULL	AC クラス LOGINAPPL の LOGINFLAG プロパティのログインフラグ nologin に対応します。
SSEID	いいえ	NUMBER(1,0)	NULL	AC クラス LOGINAPPL の LOGINSEQUENCE プロパティの SEID ログイン シーケンスに対応します。
SSUID	いいえ	NUMBER(1,0)	NULL	AC クラス LOGINAPPL の LOGINSEQUENCE プロパティの SUID ログイン シーケンスに対応します。
SSGID	いいえ	NUMBER(1,0)	NULL	AC クラス LOGINAPPL の LOGINSEQUENCE プロパティの SGID ログイン シーケンスに対応します。
SSGRP	いいえ	NUMBER(1,0)	NULL	AC クラス LOGINAPPL の LOGINSEQUENCE プロパティの SGRP ログイン シーケンスに対応します。
SFEID	いいえ	NUMBER(1,0)	NULL	AC クラス LOGINAPPL の LOGINSEQUENCE プロパティの FEID ログイン シーケンスに対応します。
SFUID	いいえ	NUMBER(1,0)	NULL	AC クラス LOGINAPPL の LOGINSEQUENCE プロパティの FUID ログイン シーケンスに対応します。
SFGID	いいえ	NUMBER(1,0)	NULL	AC クラス LOGINAPPL の LOGINSEQUENCE プロパティの FGID ログイン シーケンスに対応します。

名前	主キー	データタイプ	NULL オプション	コメント
SFGRP	いいえ	NUMBER(1,0)	NULL	AC クラス LOGINAPPL の LOGINSEQUENCE プロパティの FGRP ログイン シーケンスに対応します。
SN3EID	いいえ	NUMBER(1,0)	NULL	AC クラス LOGINAPPL の LOGINSEQUENCE プロパティの N3EID ログイン シーケンスに対応します。
SN3UID	いいえ	NUMBER(1,0)	NULL	AC クラス LOGINAPPL の LOGINSEQUENCE プロパティの N3UID ログイン シーケンスに対応します。
SN3GID	いいえ	NUMBER(1,0)	NULL	AC クラス LOGINAPPL の LOGINSEQUENCE プロパティの N3GID ログイン シーケンスに対応します。
SN3GRP	いいえ	NUMBER(1,0)	NULL	AC クラス LOGINAPPL の LOGINSEQUENCE プロパティの N3GRP ログイン シーケンスに対応します。

MEMBEROF テーブルの列

次の表で、MEMBEROF テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID
GROUPID	はい	NVARCHAR2(256)	NOT NULL	レコードのグループ ID（名）
CNAME	はい	NVARCHAR2(256)	NOT NULL	クラス名
ONAME	はい	NVARCHAR2(256)	NOT NULL	オブジェクト名

名前	主キー	データタイプ	NULL オプション	コメント
GROUPTYPE	はい	NVARCHAR2(80)	NOT NULL	グループのクラス（GROUP、XGROUP など）。AC グループ OID の CNAME に対応します。

MEMBERS テーブルの列

次の表で、MEMBERS テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
RESCLASS	はい	NVARCHAR2(80)	NOT NULL	アクセス許可が適用されるエンティティのリソース クラス。
RULEKEY	はい	NVARCHAR2(256)	NOT NULL	CA ACF2：アクセス許可が見つかったルールのルール セット キー。CA Top Secret：リソースの Owned Resource マスク。AC：リソース オブジェクト名
CNAME	はい	NVARCHAR2(80)	NOT NULL	メンバのクラス名
ONAME	はい	NVARCHAR2(256)	NOT NULL	メンバのオブジェクト名

NODE テーブルの列

次の表で、NODE テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID

名前	主キー	データタイプ	NULL オプション	コメント
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
RESCLASS	はい	NVARCHAR2(80)	NOT NULL	アクセス許可が適用されるエンティティのリソース クラス。リソースの AC OID の CNAME に対応します。
RULEKEY	はい	NVARCHAR2(256)	NOT NULL	CA ACF2 : アクセス許可が見つかったルールのルール セット キー。CA Top Secret : リソースの Owned Resource マスク。リソースの AC OID の ONAME に対応します。
KEEPALIVE	はい	TIMESTAMP(6)	NULL	最終キープアライブ日時。AC クラス HNODE の HNODE_KEEP_ALIVE プロパティに対応します。
VERSION	はい	NUMBER	NULL	ノード バージョン。AC クラス HNODE の AC プロパティ HNODE_VERSION に対応します。
ACID	はい	NVARCHAR2(256)	NULL	一意の AC ホスト ID。AC クラス HNODE の ACID プロパティに対応します。

NODE_ADDRESS テーブルの列

次の表で、NODE_ADDRESS テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID

名前	主キー	データタイプ	NULL オプション	コメント
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
RESCLASS	はい	NVARCHAR2(80)	NOT NULL	アクセス許可が適用されるエンティティのリソース クラス。リソースの AC OID の CNAME に対応します。
RULEKEY	はい	NVARCHAR2(256)	NOT NULL	CA ACF2 : アクセス許可が見つかったルールのルール セット キー。CA Top Secret : リソースの Owned Resource マスク。リソースの AC OID の ONAME に対応します。
ADDRESS	はい	NVARCHAR2(256)	NOT NULL	

NODE_ALIAS テーブルの列

次の表で、NODE_ALIAS テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
RESCLASS	はい	NVARCHAR2(80)	NOT NULL	アクセス許可が適用されるエンティティのリソース クラス。リソースの AC OID の CNAME に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
RULEKEY	はい	NVARCHAR2(256)	NOT NULL	CA ACF2: アクセス許可が見つかったルールのルール セット キー。CA Top Secret: リソースの Owned Resource マスク。リソースの AC OID の ONAME に対応します。
ALIAS	はい	NVARCHAR2(256)	NOT NULL	ノードの別名。AC クラス HNODE の ALIAS にある 1 つの文字列に対応します。

NODE_DEVIATION テーブルの列

次の表で、NODE_DEVIATION テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
RESCLASS	はい	NVARCHAR2(80)	NOT NULL	アクセス許可が適用されるエンティティのリソース クラス。リソースの AC OID の CNAME に対応します。
RULEKEY	はい	NVARCHAR2(256)	NOT NULL	CA ACF2: アクセス許可が見つかったルールのルール セット キー。CA Top Secret: リソースの Owned Resource マスク。リソースの AC OID の ONAME に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
DATA	はい	CLOB	NULL	未処理の偏差データ。DEVCALC 出力の先頭にある DEVCALC ヘッダ（すなわち、最初の POLICYSTART タグの前にあるすべてのデータ）に割り当てられます。

NODE_SUBSCRIPTION_STATUS テーブルの列

次の表で、NODE_SUBSCRIPTION_STATUS テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
PUBLISHERCNAME	はい	NVARCHAR2(80)	NOT NULL	公開ノード CNAME
SUBSCRIBERCNAME	はい	NVARCHAR2(80)	NOT NULL	購読ノード CNAME。AC クラス HNODE の SUBSCRIBER_STATUS プロパティのサブスクライバ OID コンポーネントのクラス名に対応します。
PUBLISHERONAME	はい	NVARCHAR2(256)	NOT NULL	公開ノード ONAME
SUBSCRIBERONAME	はい	NVARCHAR2(256)	NOT NULL	購読ノード ONAME。Subscriber OID のオブジェクト名に対応します。
STATUS	いいえ	NVARCHAR2(256)	NULL	サブスクリプションのステータス。AC クラス HNODE の SUBSCRIBER_STATUS プロパティのステータス コンポーネントに対応します。

名前	主キー	データタイプ	NULL オプション	コメント
LASTSTATUSTIME	いいえ	TIMESTAMP(6)	NULL	ステータスの最終更新時刻です。AC クラス HNODE の SUBSCRIBER_STATUS プロパティの最終ステータス時刻コンポーネントに対応します。

PASSWDRULES テーブルの列

次の表で、PASSWDRULES テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID
GROUPID	はい	NVARCHAR2(256)	NOT NULL	レコードのグループ ID（名）
GROUPTYPE	はい	NVARCHAR2(80)	NOT NULL	グループのクラス（GROUP、XGROUP など）。AC グループ OID の CNAME に対応します。
ISSEOS	はい	NUMBER(1,0)	NOT NULL	この passwdrules レコードが SEOS テーブル内のレコードに関連付けられているどうかを示します。このレコードが GROUPINFO レコードでなく SEOS レコードに関連付けられている場合のみ、ISSEOS は 1 になります。ISSEOS が 1 のとき、GROUPID および GROUPTYPE は空です。
MINLEN	いいえ	NUMBER	NULL	最小長
MAXREP	いいえ	NUMBER	NULL	同一文字の最大繰り返し数
MUSTSMALL	いいえ	NUMBER	NULL	小文字を含める必要があります。

名前	主キー	データタイプ	NULL オプション	コメント
MUSTCAPITAL	いいえ	NUMBER	NULL	大文字を含める必要があります。
MUSTNUM	いいえ	NUMBER	NULL	数字を含める必要があります。
MUSTOTH	いいえ	NUMBER	NULL	その他の文字を含める必要があります。
MUSTALFA	いいえ	NUMBER	NULL	指定された文字数以上の英字を含める必要があります。
MUSTALFAN	いいえ	NUMBER	NULL	指定された文字数以上の英数字を含める必要があります。
SUBNAME	いいえ	NUMBER	NULL	ユーザ名の一部を使用することはできません。
SUBOLD	いいえ	NUMBER	NULL	旧パスワードの一部を使用することはできません。
SUBSTRLEN	いいえ	NUMBER	NULL	パスワード内の繰り返し部分文字の最大長
SUBSTRREP	いいえ	NUMBER	NULL	部分文字の最大繰り返し数
PASSWDLIFE	いいえ	NUMBER	NULL	パスワード変更までのデフォルトの日数
GRACELOGINS	いいえ	NUMBER	NULL	パスワードの失効日以降の猶予ログイン回数
USERBLOCKMIN	いいえ	NUMBER	NULL	ユーザのパスワードをブロックする分数
WRONGPASS	いいえ	NUMBER	NULL	EXPIRE に設定されるまでの、間違ったパスワードの試行回数
HISTORY	いいえ	NUMBER	NULL	履歴のサイズ
MINTIME	いいえ	NUMBER	NULL	変更間の最小時間（日数）
MAXLEN	いいえ	NUMBER	NULL	最大長
DICTFORMAT	いいえ	NUMBER	NULL	辞書形式を選択します

名前	主キー	データタイプ	NULL オプション	コメント
BIDIRECTIONAL	いいえ	NUMBER	NULL	双方向パスワード暗号化を有効または無効にします。双方向パスワード暗号化が有効の場合、パスワードは新しくなるたび暗号化され、解読してクリア テキストに戻すことができます。この暗号化により、新しいパスワードと古いパスワードを幅広く比較できるようになります(パスワード履歴)。双方向暗号化が無効である場合、一方向パスワード履歴暗号化がアクティブなり、古いパスワードの復号化はできません。

POLICY テーブルの列

次の表で、POLICY テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
RESCLASS	はい	NVARCHAR2(80)	NOT NULL	アクセス許可が適用されるエンティティのリソース クラス。リソースの AC OID の CNAME に対応します。
RULEKEY	はい	NVARCHAR2(256)	NOT NULL	CA ACF2 : アクセス許可が見つかったルールのルール セット キー。CA Top Secret : リソースの Owned Resource マスク。 リソースの AC OID の ONAME に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
NAME	はい	NVARCHAR2(256)	NULL	ポリシーの論理名。AC クラス POLICY の AC プロパティ POLICY_BASE_NAME に対応します。
VERSION	はい	NUMBER	NULL	ポリシー バージョンを示す整数。ポリシー バージョンは 1 から始まる連続した整数値です。AC クラス POLICY の AC プロパティ POLICY_VERSION に対応します。
FINALIZE	いいえ	NUMBER(1,0)	NULL	ポリシーがファイナライズされ、デプロイ可能かどうかを示します。AC クラス POLICY の AC プロパティ FINALIZE に対応します。
EXTENDED_SIGNATURE	いいえ	NVARCHAR2(256)	NULL	FIPS 140-2 準拠 SHA1 ポリシー シグネチャ。AC クラス POLICY の EXTENDED_SIGNATURE プロパティに対応します。
SIGNATURE	いいえ	NVARCHAR2(256)	NULL	ポリシー シグネチャ。AC クラス POLICY の SIGNATURE プロパティに対応します。

POLICY_DEVIATION テーブルの列

次の表で、POLICY_DEVIATION テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
NODE_RESCLASS	はい	NVARCHAR2(80)	NOT NULL	アクセス許可が適用されるエンティティのリソース クラス。

名前	主キー	データタイプ	NULL オプション	コメント
NODE_RULEKEY	はい	NVARCHAR2(256)	NOT NULL	CA ACF2：アクセス許可が見つかったルールのルール セット キー。CA Top Secret：リソースの Owned Resource マスク。AC：リソース オブジェクト名
DEVIATION_INDEX	はい	NUMBER	NOT NULL	ポリシーごとに 0 から始まる偏差行シーケンス番号。DEVCALC 出力内の最新の POLICYSTART タグに関連する、この偏差行の行番号に対応します。
DEVIATED_CLASS	いいえ	NVARCHAR2(256)	NULL	deviated クラス DEVCALC 出力内の DIFF 行の 2 番目のトークンに対応します。NULL 値は DEVCALC 出力内の値（*）に対応します。
DEVIATED_OBJECT	いいえ	NVARCHAR2(256)	NULL	deviated オブジェクト DEVCALC 出力内の DIFF 行の 3 番目のトークンに対応します。NULL 値は DEVCALC 出力内の値（*）に対応します。
DEVIATED_PROPERTY	いいえ	NVARCHAR2(256)	NULL	deviated プロパティ DEVCALC 出力内の DIFF 行の 4 番目のトークンに対応します。NULL 値は DEVCALC 出力内の値（*）に対応します。
DEVIATED_VALUE	いいえ	NVARCHAR2(256)	NULL	deviated 値 DEVCALC 出力内の DIFF 行の 5 番目のトークンに対応します。NULL 値は DEVCALC 出力内の値（*）に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
DEVIATION_DATA	いいえ	CLOB	NULL	タイプが明らかになっている(すなわち、「UNKNOWN_%」と異なる)偏差行の場合、この値は DEVCALC 出力内の DIFF 行の 1 番目のトークンに対応します(たとえば、「DIFF」)。 ほかの偏差行の場合、このフィールドには DEVCALC 行全体がそのまま含まれます。
DEVIATION_TYPE	いいえ	NVARCHAR2(256)	NULL	形式 A_B で表される偏差のタイプ。A および B の値は次のとおりです。 A = EXPECTED、UNEXPECTED、または UNKNOWN B = CLASS、OBJECT、PROPERTY、VALUE、または GENERIC

POLICY_GROUP テーブルの列

次の表で、POLICY_GROUP テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
RESCLASS	はい	NVARCHAR2(80)	NULL	アクセス許可が適用されるエンティティのリソース クラス。リソースの AC OID の CNAME に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
RULEKEY	はい	NVARCHAR2(256)	NULL	CA ACF2 : アクセス許可が見つかったルールのルール セット キー。CA Top Secret : リソースの Owned Resource マスク。 リソースの AC OID の ONAME に対応します。
LATEST_FIN_RULEKEY	いいえ	NVARCHAR2(256)	NULL	CA ACF2 : アクセス許可が見つかったルールのルール セット キー。CA Top Secret : リソースの Owned Resource マスク。GPOLICY クラスの OID AC プロパティの LATEST_FINALIZED_VERSION の ONAME に対応します。
LATEST_FIN_RESCLASS	いいえ	NVARCHAR2(80)	NULL	アクセス許可が適用されるエンティティのリソース クラス。GPOLICY クラスの OID AC プロパティの LATEST_FINALIZED_VERSION の CNAME に対応します。
LATEST_RESCLASS	いいえ	NVARCHAR2(80)	NULL	アクセス許可が適用されるエンティティのリソース クラス。GPOLICY クラスの OID AC プロパティの LATEST_VERSION の CNAME に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
LATEST_RULEKEY	いいえ	NVARCHAR2(256)	NULL	CA ACF2 : アクセス許可が見つかったルールのルール セット キー。CA Top Secret : リソースの Owned Resource マスク。GPOLICY クラスの OID AC プロパティの LATEST_VERSION の ONAME に対応します。

POLICY_GROUP_DEPENDENCY テーブルの列

次の表で、POLICY_GROUP_DEPENDENCY テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
DEP_ON_RESCLASS	はい	NVARCHAR2(80)	NOT NULL	アクセス許可が適用されるエンティティのリソース クラス。リソースの AC OID の CNAME に対応します。
RESCLASS	はい	NVARCHAR2(80)	NOT NULL	アクセス許可が適用されるエンティティのリソース クラス。リソースの AC OID の CNAME に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
DEP_ON_RULEKEY	はい	NVARCHAR2(256)	NOT NULL	CA ACF2 : アクセス許可が見つかったルールのルール セット キー。CA Top Secret : リソースの Owned Resource マスク。リソースの AC OID の ONAME に対応します。
RULEKEY	はい	NVARCHAR2(256)	NOT NULL	CA ACF2 : アクセス許可が見つかったルールのルール セット キー。CA Top Secret : リソースの Owned Resource マスク。リソースの AC OID の ONAME に対応します。

POLICY_GROUP_NODE_ASSIGNMENT テーブルの列

次の表で、POLICY_GROUP_NODE_ASSIGNMENT テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
POLICYGRP_RESCLASS	はい	NVARCHAR2(80)	NOT NULL	アクセス許可が適用されるエンティティのリソース クラス。リソースの AC OID の CNAME に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
POLICYGRP_RULEKEY	はい	NVARCHAR2(256)	NOT NULL	CA ACF2 : アクセス許可が見つかったルールのルール セット キー。CA Top Secret : リソースの Owned Resource マスク。リソースの AC OID の ONAME に対応します。
NODE_RESCLASS	はい	NVARCHAR2(80)	NOT NULL	アクセス許可が適用されるエンティティのリソース クラス。リソースの AC OID の CNAME に対応します。このフィールドが「HNODE」の場合、ノード割り当てです。このフィールドが「GHNODE」の場合、ノード グループ割り当てです。
NODE_RULEKEY	はい	NVARCHAR2(256)	NOT NULL	CA ACF2 : アクセス許可が見つかったルールのルール セット キー。CA Top Secret : リソースの Owned Resource マスク。AC : リソース オブジェクト名

POLICY_RULESET テーブルの列

次の表で、POLICY_RULESET テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子

名前	主キー	データタイプ	NULL オプション	コメント
POLICY_RESCLASS	はい	NVARCHAR2(80)	NOT NULL	アクセス許可が適用されるエンティティのリソース クラス。リソースの AC OID の CNAME に対応します。
POLICY_RULEKEY	はい	NVARCHAR2(256)	NOT NULL	CA ACF2: アクセス許可が見つかったルールのルール セット キー。CA Top Secret: リソースの Owned Resource マスク。 リソースの AC OID の ONAME に対応します。
RULESET_RESCLASS	はい	NVARCHAR2(80)	NOT NULL	アクセス許可が適用されるエンティティのリソース クラス。リソースの AC OID の CNAME に対応します。
RULESET_RULEKEY	はい	NVARCHAR2(256)	NOT NULL	CA ACF2: アクセス許可が見つかったルールのルール セット キー。CA Top Secret: リソースの Owned Resource マスク。 リソースの AC OID の ONAME に対応します。

POLICY_STATUS テーブルの列

次の表で、POLICY_STATUS テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子

名前	主キー	データタイプ	NULL オプション	コメント
NODE_RESCLASS	はい	NVARCHAR2(80)	NOT NULL	アクセス許可が適用されるエンティティのリソース クラス。リソースの AC OID の CNAME に対応します。
NODE_RULEKEY	はい	NVARCHAR2(256)	NOT NULL	CA ACF2 : アクセス許可が見つかったルールのルール セット キー。CA Top Secret : リソースの Owned Resource マスク。リソースの AC OID の ONAME に対応します。
POLICY_RESCLASS	はい	NVARCHAR2(80)	NOT NULL	アクセス許可が適用されるエンティティのリソース クラス。リソースの AC OID の CNAME に対応します。
POLICY_RULEKEY	はい	NVARCHAR2(256)	NOT NULL	CA ACF2 : アクセス許可が見つかったルールのルール セット キー。CA Top Secret : リソースの Owned Resource マスク。リソースの AC OID の ONAME に対応します。
UPDATORTYPE	はい	NVARCHAR2(80)	NULL	このユーザのクラス（USER、XUSER）
UPDATORID	はい	NVARCHAR2(256)	NULL	このオブジェクトのシステム上での識別子。
STATUS	いいえ	NVARCHAR2(256)	NULL	ポリシー ステータス（APPROVED、REJECTED、PROCESSING）
DEVSTATE	いいえ	NVARCHAR2(20)	NULL	偏差ステータス（UNSET、YES、NO）
LASTDEVTIME	いいえ	TIMESTAMP(6)	NULL	偏差の最終計算日時
LASTSTATUSTIME	いいえ	TIMESTAMP(6)	NULL	前回ステータスが設定された日時

名前	主キー	データタイプ	NULL オプション	コメント
UPDATORNAME	いいえ	NVARCHAR2(256)	NULL	ポリシー更新者名。AC クラス POLICY の POLICY_STATUS メンバ、UpdatorName に対応します。
UPDATORID	いいえ	NVARCHAR2(256)	NULL	更新者オブジェクト名。AC クラス POLICY の POLICY_STATUS プロパティの Updator メンバ、ONAME コンポーネントに対応します。
UPDATORTYPE	いいえ	NVARCHAR2(256)	NULL	更新者オブジェクト名。AC クラス POLICY の POLICY_STATUS プロパティの Updator メンバ、CNAME コンポーネントに対応します。

POLICYMODELINFO テーブルの列

次の表で、POLICYMODELINFO テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
INITIAL_POLICY_OFFSET	いいえ	NUMBER	NULL	ローカル ノードの場合、sepmd -L selang コマンドによって提供される初期ポリシー オフセットに対応します。

名前	主キー	データタイプ	NULL オプション	コメント
LAST_POLICY_OFFSET	いいえ	NUMBER	NULL	ローカル ノードの場合、sepmd -L selang コマンドによって提供される最終ポリシー オフセットに対応します。

RAUDIT テーブルの列

次の表で、RAUDIT テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
RESCLASS	はい	NVARCHAR2(80)	NOT NULL	アクセス許可が適用されるエンティティのリソース クラス。
RULEKEY	はい	NVARCHAR2(256)	NOT NULL	CA ACF2: アクセス許可が見つかったルールのルール セット キー。CA Top Secret: リソースの Owned Resource マスク。AC: リソース オブジェクト名
AUDITSUCCESS	はい	NUMBER(1,0)	NULL	リソースに対して許可されたアクセスを記録します
AUDITFAILURE	はい	NUMBER(1,0)	NULL	検出された不正アクセスの試みがログに記録されます
DEBUG	いいえ	NUMBER(1,0)	NULL	デバッグ モード以降のログ
TRUST	いいえ	NUMBER(1,0)	NULL	trust イベントを監査します

RESAC テーブルの列

次の表で、RESAC テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
RESCLASS	はい	NVARCHAR2(80)	NOT NULL	アクセス許可が適用されるエンティティのリソース クラス。リソースの AC OID の CNAME に対応します。
RULEKEY	はい	NVARCHAR2(256)	NOT NULL	CA ACF2 : アクセス許可が見つかったルールのルール セット キー。CA Top Secret : リソースの Owned Resource マスク。 リソースの AC OID の ONAME に対応します。
DESCRIPTION	いいえ	NVARCHAR2(256)	NULL	レコードの説明/コメント。関連する AC リソース クラスの AC プロパティ COMMENT に対応します。
CALENDAR	いいえ	NVARCHAR2(256)	NULL	Unicenter TNG で時間帯制限を表す Unicenter TNG カレンダ オブジェクトを指定します。AC は、これらのオブジェクトのリストを管理目的のみに使用し、オブジェクトを保護しません。関連する AC リソース クラスの AC プロパティ CALENDAR に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
NOTIFY	いいえ	NVARCHAR2(256)	NULL	リソース レコードが示すリソースへのアクセスが実行されるたびに、通知メッセージを送信するように指示します。ユーザ名またはユーザの電子メール アドレスを入力します。また、別名が指定されている場合は、メール グループの電子メール アドレスも入力できます。関連する AC リソース クラスの AC プロパティ NOTIFY に対応します。
SECLABEL	いいえ	NVARCHAR2(256)	NULL	セキュリティ ラベルは、特定のセキュリティ レベルと 0 個以上のセキュリティ カテゴリとの関係を表します。関連する AC リソース クラスの AC プロパティ SECLABEL に対応します。
SECLEVEL	いいえ	NUMBER	NULL	セキュリティ レベル。関連する AC リソース クラスの AC プロパティ SECLEVEL に対応します。
CRETIME	いいえ	TIMESTAMP(6)	NULL	作成日時。関連する AC リソース クラスの AC プロパティ CREATE_TIME に対応します。
WARNING	いいえ	NUMBER(1,0)	NULL	アクセサがリソースにアクセスできる権限を持たない場合でも、リソースへのアクセスを AC が許可するように指定します。ただし、監査ログに警告メッセージが書き込まれます。関連する AC リソース クラスの AC プロパティ WARNING に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
UNTRUST	いいえ	NUMBER(1,0)	NULL	プログラムが trusted かどうかを指定します。このプロパティを設定すると、どのユーザもプログラムを実行できません。このプロパティが設定されていない場合は、プログラムのデータベースに指定されているほかのプロパティを使用して、ユーザがプログラムの実行を許可されているかどうかが確認されます。trusted プログラムに何らかの変更を加えると、このプロパティが自動的に設定されます。 PROGRAM、SECFILE、HOST などの、関連する AC リソース クラスの AC プロパティ UNTRUST に対応します。
ETHINFO	いいえ	NVARCHAR2(256)	NULL	ホストのイーサネット情報。AC リソース クラス HOST の AC プロパティ ETHINFO に対応します。
NETMATCH	いいえ	NVARCHAR2(256)	NULL	一致する IP アドレス。AC リソース クラス HOSTNET の AC プロパティ INMASKMATCH の NetworkMatch コンポーネントに対応します。
NETMASK	いいえ	NVARCHAR2(256)	NULL	IP アドレス マスク。AC リソース クラス HOSTNET の AC プロパティ INMASKMATCH のマスク コンポーネントに対応します。

名前	主キー	データタイプ	NULL オプション	コメント
AAUDIT	いいえ	NVARCHAR2(256)	NULL	eTrust AC による監査の対象になっているアクティビティの種類を表示します。AC リソース クラス ADMIN の AC プロパティ AAUDIT に対応します。
UNTRUSTREASON	いいえ	NVARCHAR2(256)	NULL	UNIX の dbdump でのみ使用されます。AC リソース クラス PROGRAM、SECFILE の AC プロパティ UNTRUSTREASON に対応します。
ACCSWHO	いいえ	NUMBER(20,0)	NULL	アクセス オブジェクト名。レコードに最後にアクセスした管理者です。AC リソース クラス PROGRAM の AC プロパティ ACCSWHO に対応します。UNIX の場合、UID（数値）を含みます。Windows の場合、ユーザ名を含みます。
ACCSTIME	いいえ	TIMESTAMP(6)	NULL	アクセス オブジェクト日時（UNIX のみ）。レコードに最後にアクセスした日時です。AC リソース クラス PROGRAM の AC プロパティ ACCSTIME に対応します。
BLOCKRUN	いいえ	NUMBER(1,0)	NULL	実行をブロック。AC リソース クラス PROGRAM の AC プロパティ BLOCKRUN に対応します。
UNIXUID	いいえ	NVARCHAR2(256)	NULL	UNIX UID。AC リソース クラス SPECIALPGM の AC プロパティ UNIXUID に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
INTERACTIVE	いいえ	NUMBER(1,0)	NULL	対話式。sesudo を使用して実行しようとしているアプリケーションが、サービス アプリケーションではなく対話式 Windows アプリケーション（notepad.exe や cmd.exe など）である場合は、このスイッチがマークされている必要があります。sesudo クライアント コマンドを使用して対話式アプリケーションを実行しようとした場合に、そのアプリケーションが「INTERACTIVE」がマークされていないと、アプリケーションはバックグラウンドで実行され、対話を行うことができません。AC リソース クラス SUDO の AC プロパティ INTERACTIVE に対応します。
TARGUSRCNAME	いいえ	NVARCHAR2(80)	NULL	SUDO クラスがコマンドを実行するために借用する権限が与えられているユーザの名前を指定します。デフォルトは administrator です（SUDO クラス）。AC リソース クラス SUDO の AC プロパティ TARGUSR の CNAME に対応します（UNIX のみ）。
TARGUSRONAME	いいえ	NVARCHAR2(256)	NULL	AC リソース クラス SUDO の AC プロパティ TARGUSR の ONAME に対応します（UNIX のみ）。

名前	主キー	データタイプ	NULL オプション	コメント
PASSWDREQ	いいえ	NUMBER(1,0)	NULL	パスワードが必要。sesudo コマンドが、実行前にターゲット ユーザにパスワードを要求するかどうかを示します。AC リソース クラス SUDO の AC プロパティ PASSWDREQ に対応します（UNIX のみ）。
FILEPATH	いいえ	NVARCHAR2(256)	NULL	AC リソース クラス KMODULE の AC プロパティ FILEPATH に対応します。

RESINFO テーブルの列

次の表で、RESINFO テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
RESCLASS	はい	NVARCHAR2(80)	NOT NULL	アクセス許可が適用されるエンティティのリソース クラス。リソースの AC OID の CNAME に対応します。
RULEKEY	はい	NVARCHAR2(256)	NOT NULL	CA ACF2: アクセス許可が見つかったルールのルール セット キー。CA Top Secret: リソースの Owned Resource マスク。 リソースの AC OID の ONAME に対応します。
PREFIX	いいえ	NVARCHAR2(40)	NULL	CA ACF2 のみ: ルール セットのプレフィックス フィールド

名前	主キー	データタイプ	NULL オプション	コメント
OWNERCNAME	いいえ	NVARCHAR2(80)	NULL	このリソースの所有者のクラスです。リソース レコードの所有者には、リソースに対する無制限のアクセス権が与えられます。ただし、前提として、所有者のセキュリティ レベル、セキュリティ ラベル、およびセキュリティ カテゴリに、リソースへのアクセスを許可する適切な権限が設定されている必要があります。リソースの所有者には、リソース レコードを更新および削除する権限が常に与えられます。「GROUP」または「XGROUP」の場合、関連するレコードは GROUPINFO テーブル内にあります。「USER」または「XUSER」の場合、関連するレコードは USERINFO テーブル内にあります。関連する AC リソース クラスの OWNER プロパティの CNAME に対応します。
OWNERONAME	いいえ	NVARCHAR2(256)	NULL	リソースの所有者のオブジェクト名です。関連する AC リソース クラスの OWNER プロパティの ONAME に対応します。
OWNRTYPE	いいえ	CHAR(1)	NULL	リソースの所有者がユーザ (U) であるかロール (R) であるかを示します。関連する AC リソース クラスの OWNER プロパティの CNAME の最初の文字に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
RESOWNER	いいえ	NVARCHAR2(256)	NULL	CA ACF2 : ルール セットの $RESOWNER の値。CA Top Secret : SMS RESOWNER
RULEOWNER	いいえ	NVARCHAR2(256)	NULL	CA ACF2 のみ。ルール セットの $OWNER の値
ADMINBYCNAME	いいえ	NVARCHAR2(80)	NULL	CA ACF2 および AC : このルール セットに最後に変更を加えた管理者のクラス。 「GROUP」または「XGROUP」の場合、関連するレコードは GROUPINFO テーブル内にあります。「USER」または「XUSER」の場合、関連するレコードは USERINFO テーブル内にあります。 関連する AC リソース クラスの UPDATE_WHO プロパティの CNAME に対応します。
ADMINBYONAME	いいえ	NVARCHAR2(256)	NULL	このルール セットに最後に変更を加えた管理者のオブジェクト名。関連する AC リソース クラスの UPDATE_WHO プロパティの ONAME に対応します。
ADMINDATE	いいえ	TIMESTAMP(6)	NULL	CA ACF2 および AC。ルール セットの最終変更日付。関連する AC リソース クラスの AC プロパティ UPDATE_TIME に対応します。
USERDATA	いいえ	NVARCHAR2(256)	NULL	CA ACF2 のみ。ルール セットの $USERDATA の値

名前	主キー	データタイプ	NULL オプション	コメント
ON_BEHALF_OF	いいえ	NVARCHAR2(256)	NULL	有効なユーザ ID。DEPLOYMENT、GDEPLOYMENT、HNODE、GHNODE、POLICY、GPOLICY、RULEKEY など複数の AC クラスの AC プロパティ ON_BEHALF_OF に対応します。

RULESET テーブルの列

次の表で、RULESET テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
RESCLASS	はい	NVARCHAR2(80)	NOT NULL	アクセス許可が適用されるエンティティのリソース クラス。リソースの AC OID の CNAME に対応します。
RULEKEY	はい	NVARCHAR2(256)	NOT NULL	CA ACF2: アクセス許可が見つかったルールのルール セット キー。CA TOP SECRET: リソースの Owned Resource マスク。 リソースの AC OID の ONAME に対応します。
FINALIZE	いいえ	NUMBER(1,0)	NULL	ルールセットがファイナライズされ、デプロイ可能かどうかを示します。AC クラス RULESET の AC プロパティ FINALIZE に対応します。
EXTENDED_SIGNATURE	いいえ	NVARCHAR2(256)	NULL	FIPS 140-2 準拠 SHA1 ポリシー シグネチャ。AC クラス RULESET の EXTENDED_SIGNATURE プロパティに対応します。

名前	主キー	データタイプ	NULL オプション	コメント
SIGNATURE	いいえ	NVARCHAR2(256)	NULL	ルールセット シグネチャ。AC クラス RULESET の SIGNATURE プロパティに対応します。

RULESET_COMMAND テーブルの列

次の表で、RULESET_COMMAND テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
RULESET_RESCLASS	はい	NVARCHAR2(80)	NOT NULL	アクセス許可が適用されるエンティティのリソース クラス。リソースの AC OID の CNAME に対応します。
RULESET_RULEKEY	はい	NVARCHAR2(256)	NOT NULL	CA ACF2 : アクセス許可が見つかったルールのルール セット キー。CA Top Secret : リソースの Owned Resource マスク。 リソースの AC OID の ONAME に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
COMMANDIDX	はい	NUMBER	NOT NULL	ルールセット コマンドが順番に表示されます。この列では、一連のコマンド内でのコマンドの位置を示します。AC クラス RULESET の AC プロパティ RULESET_DO/UNDOCMDS の command-index コンポーネントに対応します（詳細については COMMANDTYPE 列を参照）。
COMMANDTYPE	はい	NVARCHAR2(20)	NOT NULL	コマンドの種類は do と undo です。種類が「do」の場合、レコードは AC クラス RULESET の AC プロパティ RULESET_DOCMDS 内のコマンドに対応します。種類が「undo」の場合、対応するプロパティは RULESET_UNDOCMDS になります。
COMMANDSTR	はい	NVARCHAR2(256)	NULL	コマンド ストリング。AC クラス RULESET の AC プロパティ RULESET_DO/UNDOCMDS 内の command-string コンポーネントに対応します（詳細については、COMMANDTYPE の列を参照）。

SEOS テーブルの列

次の表で、SEOS テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
LASTSTARTUP	いいえ	TIMESTAMP(6)	NULL	ホストの最終起動時刻。AC クラス SEOS の AC プロパティ STARTTIME に対応します。
LASTSHUTDOWN	いいえ	TIMESTAMP(6)	NULL	ホストの最終シャットダウン時刻。AC クラス SEOS の AC プロパティ ENDTIME に対応します。
UPDATEDBY	いいえ	NVARCHAR2(256)	NULL	最後に更新したオブジェクト名。AC クラス SEOS の AC プロパティ UPDATE_WHO の ONAME に対応します。
UPDATETIME	いいえ	TIMESTAMP(6)	NULL	最終更新時刻。AC クラス SEOS の AC プロパティ UPDATE_TIME に対応します。
INACTIVEDAYS	いいえ	NUMBER	NULL	非アクティブ日数。AC クラス SEOS の AC プロパティ INACT に対応します。
ACCUMACL	いいえ	NUMBER(1,0)	NULL	ACL および PACL を累積します。AC クラス SEOS の AC プロパティ ACCPACL に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
ACCUMGRPRIGHTS	いいえ	NUMBER(1,0)	NULL	グループ権限を累積します。AC クラス SEOS の AC プロパティ GRACCR に対応します。
ADMINPWDCHANGE	いいえ	NUMBER(1,0)	NULL	管理者パスワードの変更。AC クラス SEOS の AC プロパティ CNG_ADMIN_PWD に対応します。
OWNPWDCHANGE	いいえ	NUMBER(1,0)	NULL	パスワードの変更。AC クラス SEOS の AC プロパティ CNG_OWN_PWD に対応します。
ISDMA	いいえ	NUMBER(1,0)	NULL	DMA ホストであるかどうかを示します。AC クラス SEOS の AC プロパティ ISDMA に対応します。
ISDMS	いいえ	NUMBER(1,0)	NULL	DMS ホストであるかどうかを示します。AC クラス SEOS の AC プロパティ ISDMS に対応します。
ISDH	いいえ	NUMBER(1,0)	NULL	分散ホスト(DH)。AC クラス SEOS の AC プロパティ ISDH に対応します。
DMS	いいえ	NVARCHAR2(256)	NULL	DMS ホスト名。AC クラス SEOS の AC プロパティ DMS に対応します。
CADMIN	いいえ	NUMBER(1,0)	NULL	クラスのアクティブ化: ADMIN。 AC クラス SEOS の AC プロパティ ADMIN に対応します。
CAPPL	いいえ	NUMBER(1,0)	NULL	クラスのアクティブ化: APPL。AC クラス SEOS の AC プロパティ APPL に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
CAUTHHOST	いいえ	NUMBER(1,0)	NULL	クラスのアクティブ化: AUTHHOST。 AC クラス SEOS の AC プロパティ AUTHHOST に対応します。
CCALENDAR	いいえ	NUMBER(1,0)	NULL	クラスのアクティブ化: CALENDAR。AC クラス SEOS の AC プロパティ CALENDAR に対応します。
CCATEGORY	いいえ	NUMBER(1,0)	NULL	クラスのアクティブ化: CATEGORY。AC クラス SEOS の AC プロパティ CATEGORY に対応します。
CCONNECT	いいえ	NUMBER(1,0)	NULL	クラスのアクティブ化: CONNECT。AC クラス SEOS の AC プロパティ CONNECT に対応します。
CDEPLOYMENT	いいえ	NUMBER(1,0)	NULL	クラスのアクティブ化: DEPLOYMENT。AC クラス SEOS の AC プロパティ DEPLOYMENT に対応します。
CDICTIONARY	いいえ	NUMBER(1,0)	NULL	クラスのアクティブ化: DICTIONARY。AC クラス SEOS の AC プロパティ DICTIONARY に対応します。
CDOMAIN	いいえ	NUMBER(1,0)	NULL	クラスのアクティブ化: DOMAIN。AC クラス SEOS の AC プロパティ DOMAIN に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
CFILE	いいえ	NUMBER(1,0)	NULL	クラスのアクティブ化: FILE。AC クラス SEOS の AC プロパティ FILE に対応します。
CHNODE	いいえ	NUMBER(1,0)	NULL	クラスのアクティブ化: HNODE。AC クラス SEOS の AC プロパティ HNODE に対応します。
CHOLIDAY	いいえ	NUMBER(1,0)	NULL	クラスのアクティブ化: HOLIDAY。AC クラス SEOS の AC プロパティ HOLIDAY に対応します。
CHOST	いいえ	NUMBER(1,0)	NULL	クラスのアクティブ化: HOST。AC クラス SEOS の AC プロパティ HOST に対応します。
CKMODULE	いいえ	NUMBER(1,0)	NULL	クラスのアクティブ化: KMODULE。AC クラス SEOS の AC プロパティ KMODULE に対応します。
CMFTERMINAL	いいえ	NUMBER(1,0)	NULL	クラスのアクティブ化: MFTERMINAL。AC クラス SEOS の AC プロパティ MFTERMINAL に対応します。
CPASSWORD	いいえ	NUMBER(1,0)	NULL	クラスのアクティブ化: PASSWORD。AC クラス SEOS の AC プロパティ PASSWORD に対応します。
CPOLICY	いいえ	NUMBER(1,0)	NULL	クラスのアクティブ化: POLICY。AC クラス SEOS の AC プロパティ POLICY に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
CPROGRAM	いいえ	NUMBER(1,0)	NULL	クラスのアクティブ化: PROGRAM。AC クラス SEOS の AC プロパティ PROGRAM に対応します。
CPROCESS	いいえ	NUMBER(1,0)	NULL	クラスのアクティブ化: PROCESS。AC クラス SEOS の AC プロパティ PROCESS に対応します。
CPWPOLICY	いいえ	NUMBER(1,0)	NULL	クラスのアクティブ化: PWPOLICY。AC クラス SEOS の AC プロパティ PWPOLICY に対応します。
CREGKEY	いいえ	NUMBER(1,0)	NULL	クラスのアクティブ化: REGKEY。AC クラス SEOS の AC プロパティ REGKEY に対応します。
CREGVAL	いいえ	NUMBER(1,0)	NULL	クラスのアクティブ化: REGVAL。AC クラス SEOS の AC プロパティ REGVAL に対応します。
CRULESET	いいえ	NUMBER(1,0)	NULL	クラスのアクティブ化: RULESET。AC クラス SEOS の AC プロパティ RULESET に対応します。
CSECLABEL	いいえ	NUMBER(1,0)	NULL	クラスのアクティブ化: SECLABEL。AC クラス SEOS の AC プロパティ SECLABEL に対応します。
CSECLEVEL	いいえ	NUMBER(1,0)	NULL	クラスのアクティブ化: SECLEVEL。AC クラス SEOS の AC プロパティ SECLEVEL に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
CSPECIALPGM	いいえ	NUMBER(1,0)	NULL	クラスのアクティブ化: SPECIALPGM。AC クラス SEOS の AC プロパティ SPECIALPGM に対応します。
CSUDO	いいえ	NUMBER(1,0)	NULL	クラスのアクティブ化: SUDO。AC クラス SEOS の AC プロパティ SUDO に対応します。
CSURROGATE	いいえ	NUMBER(1,0)	NULL	クラスのアクティブ化: SURROGATE。AC クラス SEOS の AC プロパティ SURROGATE に対応します。
CTCP	いいえ	NUMBER(1,0)	NULL	クラスのアクティブ化: TCP。AC クラス SEOS の AC プロパティ TCP に対応します。
CTERMINAL	いいえ	NUMBER(1,0)	NULL	クラスのアクティブ化: TERMINAL。AC クラス SEOS の AC プロパティ TERMINAL に対応します。
CUSER_DIR	いいえ	NUMBER(1,0)	NULL	クラスのアクティブ化: USER_DIR。AC クラス SEOS の AC プロパティ USER_DIR に対応します。
CWEBSERVICE	いいえ	NUMBER(1,0)	NULL	クラスのアクティブ化: WEBSERVICE。AC クラス SEOS の AC プロパティ WEBSERVICE に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
CWINSERVICE	いいえ	NUMBER(1,0)	NULL	Windows のみ: クラスのアクティブ化: WINSERVICE。AC クラス SEOS の AC プロパティ WINSERVICE に対応します。
CDAYTIMERES	いいえ	NUMBER(1,0)	NULL	UNIX のみ: 時間制限をチェックするかどうか。AC クラス SEOS の AC プロパティ DAYTIMERES に対応します。
CLOGINAPPL	いいえ	NUMBER(1,0)	NULL	UNIX のみ。AC クラス SEOS の AC プロパティ LOGINAPPL に対応します。
MAXLOGINS	いいえ	NUMBER	NULL	有効なログインの最大数。AC クラス SEOS の AC プロパティ MAXLOGINS に対応します。
PROHIBITED	いいえ	NVARCHAR2(256)	NULL	AC クラス SEOS の AC プロパティ PROHIBITED に対応します。
ACID	いいえ	NVARCHAR2(256)	NULL	一意の AC ホスト ID。AC クラス SEOS の ACID プロパティに対応します。同じ ACID が含まれる NODE テーブル内でノードを識別するのに使用されます。

SEOSSYSCALL テーブルの列

次の表で、SEOSSYSCALL テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
INTERCEPTEDSYSCALLS	いいえ	NUMBER(20,0)	NULL	インターセプトされた syscall の数
NONBLOCKINGSYSCALLS	いいえ	NUMBER(1,0)	NULL	インターセプトされた「危険な」syscall の数
ISOVERFLOW	いいえ	NUMBER(20,0)	NULL	割り当てられたバッファが小さすぎる場合は 1
THRESHOLDTIME	いいえ	NUMBER(20,0)	NULL	syscall の「危険な」時間（秒）
ALWAYSEXITSCRIPT	いいえ	NUMBER(1,0)	NULL	SEOS_unload_int.always が存在する場合は 1
OPTIONALEXITSCRIPT	いいえ	NUMBER(1,0)	NULL	SEOS_unload_int.opt が存在する場合は 1
USETRIPACCEPT	いいえ	NUMBER(1,0)	NULL	use_tripAccept トークンが yes の場合は 1
TRIPACCEPT	いいえ	NUMBER(1,0)	NULL	bin/tripAccept が存在する場合は 1
NOVELLZMD	いいえ	NUMBER(1,0)	NULL	/etc/init.d/novell-zmd が存在する場合は 1
XM	いいえ	NUMBER(1,0)	NULL	/usr/sbin/xm が存在する場合は 1
NSCD	いいえ	NUMBER(1,0)	NULL	/etc/init.d/nscd が存在する場合は 1

SNAPSHOTINFO テーブルの列

次の表で、SNAPSHOTINFO テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
DUMPSTARTTIME	いいえ	TIMESTAMP(6)	NULL	スナップショット開始時刻
DUMPENDTIME	いいえ	TIMESTAMP(6)	NULL	スナップショット終了時刻
STATUS	いいえ	CHAR(1)	NULL	スナップショット ステータス
SNAPSHOTTIME	いいえ	TIMESTAMP(6)	NULL	
SNAPSHOTTYPE	いいえ	NVARCHAR2(256)	NULL	
SNAPSHOTNAME	いいえ	NVARCHAR2(256)	NULL	
OS	いいえ	NVARCHAR2(100)	NULL	
ACVERSION	いいえ	NVARCHAR2(50)	NULL	
ACVERSIONNUM1	いいえ	NUMBER(20,0)	NULL	
ACVERSIONNUM2	いいえ	NUMBER(20,0)	NULL	
ACVERSIONNUM3	いいえ	NUMBER(20,0)	NULL	
ACVERSIONNUM4	いいえ	NUMBER(20,0)	NULL	

SPECIALPGMTYPE テーブルの列

次の表で、SPECIALPGMTYPE テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID

名前	主キー	データタイプ	NULL オプション	コメント
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
RESCLASS	はい	NVARCHAR2(80)	NOT NULL	アクセス許可が適用されるエンティティのリソース クラス。
RULEKEY	はい	NVARCHAR2(256)	NOT NULL	CA ACF2 : アクセス許可が見つかったルールのルール セット キー。CA Top Secret : リソースの Owned Resource マスク。AC : リソース オブジェクト名
TMAIL	いいえ	NUMBER(1,0)	NULL	
TBACKUP	いいえ	NUMBER(1,0)	NULL	
TXDM	いいえ	NUMBER(1,0)	NULL	
TDCM	いいえ	NUMBER(1,0)	NULL	
TPBF	いいえ	NUMBER(1,0)	NULL	
TPBN	いいえ	NUMBER(1,0)	NULL	
TPROPAGATE	いいえ	NUMBER(1,0)	NULL	（r12.0 SP1）
TSTOP	いいえ	NUMBER(1,0)	NULL	
TSURR	いいえ	NUMBER(1,0)	NULL	
TREG	いいえ	NUMBER(1,0)	NULL	
TRESTRICTED	いいえ	NUMBER(1,0)	NULL	

SYSCALL テーブルの列

次の表で、SYSCALL テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID

名前	主キー	データタイプ	NULL オプション	コメント
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
PID	はい	NUMBER(20,0)	NOT NULL	キー: プロセス pid
PARENTPID	いいえ	NUMBER(20,0)	NULL	親プロセス ID
USERID	いいえ	NUMBER(20,0)	NULL	本当のユーザ ID
GROUPID	いいえ	NUMBER(20,0)	NULL	グループ ID
INTERCEPTEDPGM	いいえ	NVARCHAR2(256)	NULL	プログラム名
INTERCEPTEDTIME	いいえ	NUMBER(20,0)	NULL	syscall の一生
SYSCALLNUM	いいえ	NUMBER(20,0)	NULL	システム コール番号
ISBLOCKING	いいえ	NUMBER(1,0)	NULL	syscall が危険な場合は 1

SYSCALLUSERSPECIALPGM テーブルの列

次の表で、SYSCALLUSERSPECIALPGM テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
SAFEPGM	はい	NVARCHAR2(256)	NOT NULL	

UACC テーブルの列

次の表で、UACC テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
RESCLASS	はい	NVARCHAR2(80)	NOT NULL	アクセス許可が適用されるエンティティのリソース クラス。
RULEKEY	はい	NVARCHAR2(256)	NOT NULL	CA ACF2: アクセス許可が見つかったルールのルールセット キー。CA Top Secret: リソースの Owned Resource マスク。AC: リソース オブジェクト名
AREAD	いいえ	NUMBER(1,0)	NULL	
AWRITE	いいえ	NUMBER(1,0)	NULL	
AMODIFY	いいえ	NUMBER(1,0)	NULL	
ACREATE	いいえ	NUMBER(1,0)	NULL	
AERASE	いいえ	NUMBER(1,0)	NULL	
AFILESCAN	いいえ	NUMBER(1,0)	NULL	
ALANGINT	いいえ	NUMBER(1,0)	NULL	
AEXEC	いいえ	NUMBER(1,0)	NULL	
ACHOWN	いいえ	NUMBER(1,0)	NULL	
ACHGRP	いいえ	NUMBER(1,0)	NULL	
ACHMOD	いいえ	NUMBER(1,0)	NULL	
AUTIMES	いいえ	NUMBER(1,0)	NULL	

名前	主キー	データタイプ	NULL オプション	コメント
ASEC	いいえ	NUMBER(1,0)	NULL	
AKILL	いいえ	NUMBER(1,0)	NULL	
ACONNECT	いいえ	NUMBER(1,0)	NULL	
ARENAME	いいえ	NUMBER(1,0)	NULL	
APASSWORD	いいえ	NUMBER(1,0)	NULL	
AAUTHORIZED	いいえ	CHAR(18)	NULL	
AXAUDIT	いいえ	NUMBER(1,0)	NULL	
ACHDIR	いいえ	NUMBER(1,0)	NULL	
ACRSUBK	いいえ	NUMBER(1,0)	NULL	
ANOTIFY	いいえ	NUMBER(1,0)	NULL	
AENUM	いいえ	NUMBER(1,0)	NULL	
AQUERY	いいえ	NUMBER(1,0)	NULL	
ARCTRL	いいえ	NUMBER(1,0)	NULL	
ACRLINK	いいえ	NUMBER(1,0)	NULL	
APRINT	いいえ	NUMBER(1,0)	NULL	
AMANAGE	いいえ	NUMBER(1,0)	NULL	
AMAXALLOWED	いいえ	NUMBER(1,0)	NULL	
ASTOP	いいえ	NUMBER(1,0)	NULL	
APAUSE	いいえ	NUMBER(1,0)	NULL	
ACONTROL	いいえ	NUMBER(1,0)	NULL	
ACHOG	いいえ	NUMBER(1,0)	NULL	
ARESUME	いいえ	NUMBER(1,0)	NULL	

USERAC テーブルの列

次の表で、USERAC テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
USERID	はい	NVARCHAR2(256)	NOT NULL	レコードのユーザ ID（名）USER/XUSER オブジェクトの AC OID に対応します。
USERTYPE	はい	NVARCHAR2(80)	NOT NULL	このユーザの AC クラス（USER、XUSER）
DESCRIPTION	いいえ	NVARCHAR2(256)	NULL	このユーザの説明/コメント。USER/XUSER クラスの AC プロパティ COMMENT に対応します。
PROFILE	いいえ	NVARCHAR2(256)	NULL	ユーザのプロファイルへのパスを指定する文字列です。この文字列には、ローカルの絶対パスまたは UNC パスを含めることができます。USER/XUSER クラスの AC プロパティ PROFILE の ONAME に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
GRACELOGIN	いいえ	NUMBER	NULL	パスワードの有効期限が切れた後の猶予ログイン回数です。指定された猶予ログイン回数を超えるとユーザはシステムへのアクセスを拒否されるため、システム管理者に連絡して新しいパスワードを取得する必要があります。USER/XUSER クラスの AC プロパティ GRACELOGIN に対応します。
MAXLOGINS	いいえ	NUMBER	NULL	ユーザが同時にログインできる端末台数の最大値を設定します。値 0(ゼロ)は、同時に任意の数の端末からログインできることを意味します。USER/XUSER クラスの AC プロパティ MAXLOGINS に対応します。
INACTIVE	いいえ	NUMBER	NULL	ユーザのステータスが非アクティブに変更されるまでの経過日数を指定します。指定した日数に達すると、ユーザはログインできなくなります。USER/XUSER クラスの AC プロパティ INACTIVE に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
SUSPENDDATE	いいえ	DATE	NULL	ユーザ レコードを無効にします。ただし、データベースには定義を残します。ユーザは一時停止されたユーザ アカウントを使用してシステムにログインすることはできません。USER/XUSER クラスの AC プロパティ SUSPEND_DATE に対応します。
SUSPENDWHOCNAME	いいえ	NVARCHAR2(80)	NULL	一時停止日をアクティブにした管理者です。USER/XUSER クラスの AC プロパティ SUSPEND_WHO の CNAME に対応します。
SUSPENDWHOONAME	いいえ	NVARCHAR2(256)	NULL	このオブジェクトのシステム上での識別子。USER/XUSER クラスの AC プロパティ SUSPEND_WHO の ONAME に対応します。
RESUMEDATE	いいえ	DATE	NULL	suspend パラメータを指定して無効にしたユーザ レコードを有効にします。USER/XUSER クラスの AC プロパティ RESUME_DATE に対応します。
LUTERMINAL	いいえ	NVARCHAR2(256)	NULL	端末からの最終更新。USER/XUSER クラスの AC プロパティ LAST_ACC_TERM に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
PASSWDINT	いいえ	NUMBER	NULL	パスワードの設定または変更後、ユーザに対して新しいパスワードの入力を促すメッセージを表示するまでの経過日数を設定します。USER/XUSER クラスの AC プロパティ PASSWD_INT に対応します。
PASSWDLAC	いいえ	TIMESTAMP(6)	NULL	管理者が最後にパスワードを更新した日時です。USER/XUSER クラスの AC プロパティ PASSWD_L_A_C に対応します。
PASSWDLC	いいえ	TIMESTAMP(6)	NULL	ユーザが最後にパスワードを更新した日時です。USER/XUSER クラスの AC プロパティ PASSWD_L_C に対応します。
PASSWDACW	いいえ	NVARCHAR2(256)	NULL	このレコードのユーザ パスワードを最後に変更した ADMIN ユーザです。USER/XUSER クラスの AC プロパティ PASSWD_A_C_W に対応します。
MINTIME	いいえ	NUMBER	NULL	ユーザがパスワードを再度変更できるまでの最短経過日数を指定します。USER/XUSER クラスの AC プロパティ MIN_TIME に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
POLICYMODEL	いいえ	NVARCHAR2(256)	NULL	ユーザが sepass ユーティリティを使用してパスワードを変更した場合、新しいパスワードが指定された Policy Model（pmdbName）に伝達されるように指定します。レジストリの HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥eTrustAccessControl¥eTrustAccessControl サブキー の parent_pmd 値または passwd_pmd 値に定義されている Policy Model には、パスワードは送信されません。 USER/XUSER クラスの AC プロパティ POLICYMODEL に対応します。
SESSIONGROUP	いいえ	NVARCHAR2(256)	NULL	Single Sign-On で使用されます。このプロパティにより、SSO セッション グループがユーザに割り当てられます。SESSION_GROUP プロパティは、最大 16 文字の文字列です。USER/XUSER クラスの AC プロパティ SESSION_GROUP に対応します。
LOGINSTATUS	いいえ	NVARCHAR2(256)	NULL	ログイン ステータス
PWDNEXTCHGINDAYS	いいえ	NUMBER	NULL	パスワードが次回変更されるまでの日数
APPLISTTIME	いいえ	TIMESTAMP(6)	NULL	USER/XUSER クラスの AC プロパティ APPLIST_TIME に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
AUTHNMTHD	いいえ	NVARCHAR2(256)	NULL	認証方法。USER/XUSER クラスの AC プロパティ AUTHNMTHD に対応します。
BADPASSWD	いいえ	NUMBER	NULL	無効なパスワードの試行回数。USER/XUSER クラスの AC プロパティ BADPASSWD に対応します。
CALENDAR	いいえ	NVARCHAR2(256)	NULL	Unicenter TNG で時間帯制限を表す Unicenter TNG カレンダ オブジェクトを指定します。AC は、これらのオブジェクトのリストを管理目的のみに使用し、オブジェクトを保護しません。USER/XUSER クラスの AC プロパティ CALENDAR に対応します。
UPDTIME	いいえ	TIMESTAMP(6)	NULL	レコードが最後に変更された日時です。USER/XUSER クラスの AC プロパティ UPDTIME に対応します。
LOCATION	いいえ	NVARCHAR2(256)	NULL	ユーザのロケーション。USER/XUSER クラスの AC プロパティ LOCATION に対応します。
EMAIL	いいえ	NVARCHAR2(256)	NULL	ユーザの電子メール アドレス。USER/XUSER クラスの AC プロパティ EMAIL に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
ORGANIZATION	いいえ	NVARCHAR2(256)	NULL	ユーザの組織名。USER/XUSER クラスの AC プロパティ ORGANIZATION に対応します。
ORGUNIT	いいえ	NVARCHAR2(256)	NULL	ユーザの組織単位。USER/XUSER クラスの AC プロパティ ORG_UNIT に対応します。
PHONE	いいえ	NVARCHAR2(256)	NULL	ユーザの電話番号。USER/XUSER クラスの AC プロパティ PHONE に対応します。
COUNTRY	いいえ	NVARCHAR2(256)	NULL	ユーザの国名を指定します。この文字列は、X.500 ネーミング スキーマの一部です。この情報が eTrust AC による権限付与に使用されることはありません。USER/XUSER クラスの AC プロパティ COUNTRY に対応します。
LOCALAPPS	いいえ	NUMBER(1,0)	NULL	USER/XUSER クラスの AC プロパティ LOCALAPPS に対応します。
LOGSHIFT	いいえ	NUMBER(1,0)	NULL	シフト時間枠外にログインを許可するかどうかを示します。このイベントに関する監査レコードが、AC によって監査ログに書き込まれます。USER/XUSER クラスの AC プロパティ LOGSHIFT に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
NOTIFY	いいえ	NVARCHAR2(256)	NULL	ユーザがログインするたびに、そのユーザに通知が送信されます。ユーザ名またはユーザの電子メール アドレスを入力します。また、別名が指定されている場合は、メール グループの電子メール アドレスも入力できます。通知メッセージを受け取るユーザは、頻繁にログインして、各メッセージに示された不正なアクセスの試みに対処する必要があります。USER/XUSER クラスの AC プロパティ NOTIFY に対応します。
OIDCRDDATA	いいえ	NVARCHAR2(256)	NULL	CA Single Sign-On および CA Web Access Control で使用されます。USER/XUSER クラスの AC プロパティ OIDCRDDATA に対応します。
PWDAUTOGEN	いいえ	NUMBER(1,0)	NULL	アプリケーション パスワードをポリシー サーバで自動的に生成するかどうかを指定します。USER/XUSER クラスの AC プロパティ PWD_AUTOGEN に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
PWDSYNC	いいえ	NUMBER(1,0)	NULL	アプリケーション パスワードをユーザのほかのアプリケーションのパスワードと同一にするかどうかを指定します。USER/XUSER クラスの AC プロパティ PWD_SYNC に対応します。
SCRIPTVARS	いいえ	NVARCHAR2(256)	NULL	CA Single Sign-On および CA Web Access Control で使用されます。アプリケーションごとに保存されるアプリケーション スクリプトの変数値を含む変数リストです。USER/XUSER クラスの AC プロパティ SCRIPT_VARS に対応します。
SECLEVEL	いいえ	NUMBER	NULL	ユーザ レコードに割り当てられたセキュリティ レベル。USER/XUSER クラスの AC プロパティ SECLEVEL に対応します。
SECLABEL	いいえ	NVARCHAR2(256)	NULL	USER/XUSER クラスの AC プロパティ SECLABEL の ONAME に対応します。
SHIFT	いいえ	NVARCHAR2(256)	NULL	CA Single Sign-On および CA Web Access Control で使用されます。USER/XUSER クラスの AC プロパティ SHIFT の ONAME に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
UALIAS	いいえ	NVARCHAR2(256)	NULL	1 つ以上の認証ホストに定義されている特定ユーザのすべての別名です。CA Single Sign-On および CA Web Access Control で使用されます。USER/XUSER クラスの AC プロパティ UALIAS に対応します。
NOCHGPWD	いいえ	NUMBER(1,0)	NULL	UNIX のみ: パスワード変更禁止。AC クラス USER の AC プロパティ NOCHNGPASS に対応します。
OWNERONAME	いいえ	NVARCHAR2(256)	NULL	所有者オブジェクト名。USER/XUSER クラスの AC プロパティ OWNER の ONAME に対応します。
OWNERCNAME	いいえ	NVARCHAR2(80)	NULL	所有者クラス名。GROUP または XGROUP の場合、所有者レコードは GROUPINFO テーブル内にあります。USER または XUSER の場合、所有者レコードは USERINFO テーブル内にあります。USER/XUSER クラスの AC プロパティ OWNER の CNAME に対応します。

USERACAUDIT テーブルの列

次の表で、USERACAUDIT テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
USERID	はい	NVARCHAR2(256)	NOT NULL	レコードのユーザ ID（名）
USERTYPE	はい	NVARCHAR2(80)	NOT NULL	このユーザのクラス（USER、XUSER）
SUCCESS	いいえ	NUMBER(1,0)	NULL	CA Access Control は成功したアクセスをログに記録します。
FAILURE	いいえ	NUMBER(1,0)	NULL	失敗したアクセスの試みがログに記録されます。
LOGONSUCCESS	いいえ	NUMBER(1,0)	NULL	CA Access Control は成功したログインをログに記録します。
LOGONFAILURE	いいえ	NUMBER(1,0)	NULL	CA Access Control は失敗したログインの試みをログに記録します。
DEBUG	いいえ	NUMBER(1,0)	NULL	監査デバッグ イベント
TRACE	いいえ	NUMBER(1,0)	NULL	監査トレース イベント

USERACMODE テーブルの列

次の表で、USERACMODE テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	Yes	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID

名前	主キー	データタイプ	NULL オプション	コメント
HOSTID	Yes	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
USERID	Yes	NVARCHAR2(256)	NOT NULL	レコードのユーザ ID（名）
USERTYPE	Yes	NVARCHAR2(80)	NOT NULL	このユーザのクラス（USER、XUSER）
MREGULAR	No	NUMBER(1,0)	NULL	
MAUDITOR	No	NUMBER(1,0)	NULL	
MOPERATIONS	No	NUMBER(1,0)	NULL	
MPWOFFICER	No	NUMBER(1,0)	NULL	
MENABLED	No	NUMBER(1,0)	NULL	
MIGNHOL	No	NUMBER(1,0)	NULL	
MSERVER	No	NUMBER(1,0)	NULL	
MADMIN	No	NUMBER(1,0)	NULL	
MLOGICAL	No	NUMBER(1,0)	NULL	

USERGRP テーブルの列

次の表で、USERGRP テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
USERID	はい	NVARCHAR2(256)	NOT NULL	レコードのユーザ ID（名）

名前	主キー	データタイプ	NULL オプション	コメント
USERTYPE	はい	NVARCHAR2(80)	NOT NULL	このユーザのクラス（USER、XUSER）
GROUPID	はい	NVARCHAR2(256)	NOT NULL	レコードのグループ ID（名）AC グループ OID の ONAME に対応します。
GROUPTYPE	はい	NVARCHAR2(80)	NOT NULL	グループのクラス（GROUP、XGROUP など）。AC グループ OID の CNAME に対応します。
CONNECTIONDATE	いいえ	TIMESTAMP(6)	NULL	接続日付
OWNERCNAME	いいえ	NVARCHAR2(80)	NULL	所有者クラス名。GROUP または XGROUP の場合、所有者レコードは GROUPINFO テーブル内にあります。USER または XUSER の場合、所有者レコードは USERINFO テーブル内にあります。
OWNERONAME	いいえ	NVARCHAR2(256)	NULL	
MREGULAR	いいえ	NUMBER(1,0)	NULL	
MAUDITOR	いいえ	NUMBER(1,0)	NULL	
MOPERATIONS	いいえ	NUMBER(1,0)	NULL	
MPWOFFICER	いいえ	NUMBER(1,0)	NULL	
MENABLED	いいえ	NUMBER(1,0)	NULL	
MIGNHOL	いいえ	NUMBER(1,0)	NULL	
MSERVER	いいえ	NUMBER(1,0)	NULL	
MADMIN	いいえ	NUMBER(1,0)	NULL	

USERINFO テーブルの列

次の表で、USERINFO テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
USERID	はい	NVARCHAR2(256)	NOT NULL	このオブジェクトのシステム上での識別子。
USERTYPE	はい	NVARCHAR2(80)	NOT NULL	このユーザのクラス（USER、XUSER）
NAME	いいえ	NVARCHAR2(256)	NULL	セキュリティ データベースで定義されたユーザのフルネーム。この列は USER/XUSER クラスの AC プロパティ FULL_NAME に対応します。
DEFGROUP	いいえ	NVARCHAR2(256)	NULL	USS でのユーザのデフォルト グループ。 CA Top Secret では DFLTGRP フィールド、CA ACF2 では GROUP フィールドになります。
CRETIME	いいえ	TIMESTAMP(6)	NULL	セキュリティ データベースでユーザが作成された日時。この列は USER/XUSER クラスの AC プロパティ CREATE_TIME に対応します。

名前	主キー	データタイプ	NULL オプション	コメント
LUTIME	いいえ	TIMESTAMP(6)	NULL	ユーザが最後にシステムにログインした日時。この列は USER/XUSER クラスの AC プロパティ LAST_ACC_TIME に対応します。
ACTDATE	いいえ	DATE	NULL	CA ACF2 のみ。ユーザ アカウントが有効化された日付
EXPDATE	いいえ	DATE	NULL	ユーザ アカウントが失効する日付。この列は USER/XUSER クラスの AC プロパティ EXPIRE_DATE に対応します。
TIMEZONE	いいえ	CHAR(3)	NULL	ACID の実際のタイムゾーンを CPU のタイムゾーンからの相対値で指定します。値は -12 から +12 の間で指定します。
APPIND	いいえ	CHAR(1)	NULL	アプリケーション インジケータ。アプリケーション インジケータは、レコードがどのアプリケーションに属するかを示します。TSS/ACF2 DB スキーマ内の文字の ID と一致します。この値は常に「A」であることが必要です。
CONSOLE	いいえ	CHAR(1)	NULL	CA ACF2 : TSO コンソール機能にアクセスできます。 CA Top Secret : ユーザが TSS MODIFY コマンドを発行できます。
サスペンド	いいえ	CHAR(1)	NULL	ユーザのシステム アクセスを禁止します。

名前	主キー	データタイプ	NULL オプション	コメント
TRACE	いいえ	CHAR(1)	NULL	すべてのユーザ アクティビティを記録する有効な診断トレース(システム エントリ、リソース アクセス、アクセス違反など)。
LDS	いいえ	CHAR(1)	NULL	LDAP 同期可能なユーザ
EIMRECID	いいえ	CHAR(8)	NULL	レコード識別子
LDSRECID	いいえ	CHAR(8)	NULL	レコード識別子
PROXYRECID	いいえ	CHAR(8)	NULL	レコード識別子
SRCRECID	いいえ	CHAR(8)	NULL	ユーザの SOURCE レコード名の指定に使用します。
SNAME	いいえ	NVARCHAR2(64)	NULL	Lotus Notes z/OS UNIX のユーザ ID を CA Top Secret または CA ACF2 のユーザ ID に対応付ける際に使用されます。
UNAME	いいえ	NVARCHAR2(246)	NULL	Novell Directory Services のユーザ ID を CA Top Secret または CA ACF2 のユーザ ID に対応付ける際に使用されます。
SECURITYID	いいえ	NVARCHAR2(256)	NULL	このユーザ エントリに対するベンダ固有のセキュリティ ID。この列は XUSER クラスの AC プロパティ SECURITY_ID に対応します。

USERLIST テーブルの列

次の表で、USERLIST テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。
GROUPID	はい	NVARCHAR2(256)	NOT NULL	レコードのグループ ID（名）
GROUPTYPE	はい	NVARCHAR2(80)	NOT NULL	グループのクラス（GROUP、XGROUP など）。AC グループ OID の CNAME に対応します。
USERTYPE	はい	NVARCHAR2(80)	NOT NULL	ユーザのクラス名
USERID	はい	NVARCHAR2(256)	NOT NULL	ユーザのオブジェクト名

USERREVACL テーブルの列

次の表で、USERREVACL テーブルの列の属性について説明します。

名前	主キー	データタイプ	NULL オプション	コメント
SNAPSHOTID	はい	NUMBER(20,0)	NOT NULL	レコードのスナップショット ID
HOSTID	はい	NVARCHAR2(512)	NOT NULL	レコードのホスト ID。レコードが存在するシステムのシステム識別子
USERID	はい	NVARCHAR2(256)	NOT NULL	このオブジェクトのシステム上での識別子。USER/XUSER オブジェクトの AC OID に対応します。
USERTYPE	はい	NVARCHAR2(80)	NOT NULL	このユーザのクラス（USER、XUSER）
RESCNAME	はい	NVARCHAR2(80)	NOT NULL	リソース クラス名
RESONAME	はい	NVARCHAR2(256)	NOT NULL	リソース オブジェクト名

名前	主キー	データタイプ	NULL オプション	コメント
CONCNAME	はい	NVARCHAR2(80)	NOT NULL	条件クラス名（すなわち、PROGRAM、HOST、CALENDAR）。文字列が空でない場合、RESINFO テーブルに条件オブジェクトが存在することを示しています。空の場合、「無条件」であることを示しています。
CONONAME	はい	NVARCHAR2(256)	NOT NULL	条件オブジェクト名
AREAD	いいえ	NUMBER(1,0)	NULL	
AWRITE	いいえ	NUMBER(1,0)	NULL	
AMODIFY	いいえ	NUMBER(1,0)	NULL	
ACREATE	いいえ	NUMBER(1,0)	NULL	
AERASE	いいえ	NUMBER(1,0)	NULL	
AFILESCAN	いいえ	NUMBER(1,0)	NULL	
ALANGINT	いいえ	NUMBER(1,0)	NULL	
AEXEC	いいえ	NUMBER(1,0)	NULL	
ACHOWN	いいえ	NUMBER(1,0)	NULL	
ACHGRP	いいえ	NUMBER(1,0)	NULL	
ACHMOD	いいえ	NUMBER(1,0)	NULL	
AUTIMES	いいえ	NUMBER(1,0)	NULL	
ASEC	いいえ	NUMBER(1,0)	NULL	
AKILL	いいえ	NUMBER(1,0)	NULL	
ACONNECT	いいえ	NUMBER(1,0)	NULL	
ARENAME	いいえ	NUMBER(1,0)	NULL	
APASSWORD	いいえ	NUMBER(1,0)	NULL	
AAUTHORIZED	いいえ	NUMBER(1,0)	NULL	
AXAUDIT	いいえ	NUMBER(1,0)	NULL	

名前	主キー	データタイプ	NULL オプション	コメント
ACHDIR	いいえ	NUMBER(1,0)	NULL	
ACRSUBK	いいえ	NUMBER(1,0)	NULL	
ANOTIFY	いいえ	NUMBER(1,0)	NULL	
AENUM	いいえ	NUMBER(1,0)	NULL	
AQUERY	いいえ	NUMBER(1,0)	NULL	
ARCTRL	いいえ	NUMBER(1,0)	NULL	
ACRLINK	いいえ	NUMBER(1,0)	NULL	
APRINT	いいえ	NUMBER(1,0)	NULL	
AMANAGE	いいえ	NUMBER(1,0)	NULL	
AMAXALLOWED	いいえ	NUMBER(1,0)	NULL	
ASTOP	いいえ	NUMBER(1,0)	NULL	
APAUSE	いいえ	NUMBER(1,0)	NULL	
ACONTROL	いいえ	NUMBER(1,0)	NULL	
ACHOG	いいえ	NUMBER(1,0)	NULL	
ARESUME	いいえ	NUMBER(1,0)	NULL	
DREAD	いいえ	NUMBER(1,0)	NULL	
DWRITE	いいえ	NUMBER(1,0)	NULL	
DMODIFY	いいえ	NUMBER(1,0)	NULL	
DCREATE	いいえ	NUMBER(1,0)	NULL	
DERASE	いいえ	NUMBER(1,0)	NULL	
DFILESCAN	いいえ	NUMBER(1,0)	NULL	
DLANGINT	いいえ	NUMBER(1,0)	NULL	
DEXEC	いいえ	NUMBER(1,0)	NULL	
DCHOWN	いいえ	NUMBER(1,0)	NULL	
DCHGRP	いいえ	NUMBER(1,0)	NULL	
DCHMOD	いいえ	NUMBER(1,0)	NULL	

名前	主キー	データタイプ	NULL オプション	コメント
DUTIMES	いいえ	NUMBER(1,0)	NULL	
DSEC	いいえ	NUMBER(1,0)	NULL	
DKILL	いいえ	NUMBER(1,0)	NULL	
DCONNECT	いいえ	NUMBER(1,0)	NULL	
DRENAME	いいえ	NUMBER(1,0)	NULL	
DPASSWORD	いいえ	NUMBER(1,0)	NULL	
DAUTHORIZED	いいえ	NUMBER(1,0)	NULL	
DXAUDIT	いいえ	NUMBER(1,0)	NULL	
DCHDIR	いいえ	NUMBER(1,0)	NULL	
DCRSUBK	いいえ	NUMBER(1,0)	NULL	
DNOTIFY	いいえ	NUMBER(1,0)	NULL	
DENUM	いいえ	NUMBER(1,0)	NULL	
DQUERY	いいえ	NUMBER(1,0)	NULL	
DRCTRL	いいえ	NUMBER(1,0)	NULL	
DCRLINK	いいえ	NUMBER(1,0)	NULL	
DPRINT	いいえ	NUMBER(1,0)	NULL	
DMANAGE	いいえ	NUMBER(1,0)	NULL	
DMAXALLOWED	いいえ	NUMBER(1,0)	NULL	
DSTOP	いいえ	NUMBER(1,0)	NULL	
DPAUSE	いいえ	NUMBER(1,0)	NULL	
DCONTROL	いいえ	NUMBER(1,0)	NULL	
DCHOG	いいえ	NUMBER(1,0)	NULL	
DRESUME	いいえ	NUMBER(1,0)	NULL	

関係

FK 名	コメント
CONFIG_ENTRY_CON	エントリを含みます。
DEPTASK_RESULTMSG_CON	メッセージ"を含みます。
USERGRP_GROUP_CON	ユーザのグループです。
USERLIST_FK	ユーザを含みます。
PASSWDRULES_FK	パスワード ルールを含みます。
MEMBEROF_FK	グループを含みます。
GROUPMEMBER_FK	メンバを含みます(グループタイプ)。
GROUPREVACL_FK	ACL の影響を受けます。
GROUPAUDIT_FK	監査を含みます。
SNAPSHOTINFO_FK	スナップショットを含みます。
NODE_ALIAS_FK	
NODE_SUBSCRIPTION_PUBLISHER	
NODE_EFFECTIVE_POLICY_CON	ポリシーの影響を受けます。
NODE_SUBSCRIPTION_SUBSCRIBER	
NODE_POLICY_STATUS_CON	ポリシーのステータスを含みます。
NODE_DEPTASKGRP_CON	タスク グループの演算子です。
NODE_ADDRESS_FK	
NODE_NODE_DEVIATION_CON	偏差を含みます。
NODE_DEPTASK_CON	タスクにより処理されます。
POLICY_POLICY_STATUS_CON	ノードのステータスを含みます。
LATESTFIN_POLICYGRP_CON	最新のファイナライズされたポリシー グループです。
POLICY_EFFECTIVE_POLICY_CON	ノードに影響します。
POLICY_POLICY_DEVIATION_CON	
POLICY_RULEST_POLICY_CON	ルールセットを含みます。

FK 名	コメント
LATEST_POLICYGRP_CON	グループ内の最新のポリシーです。
POLICY_DEPTASK_CON	タスクによりデプロイされます。
POLICYGRP_DEPTASK_CON	タスクによりデプロイされます。
POLICYGRP_DEPTASKGRP_CON	タスク グループの演算子です。
POLICY_GROUP_DEP_ON_CON	ポリシー グループに依存します。
POLICY_GROUP_DEP_CON	依存ポリシー グループを含みます。
PMDSUBC_CON	
POLICYGRP_NODASS_POL_CON	ノードの割り当てを含みます。
POLICY_GROUP_CON	スーパークラスです。
POLICY_CON	スーパークラスです。
RULESET_CON	スーパークラスです。
POLICYGRP_NODASS_NOD_CON	ポリシー グループに割り当てられたリソース（NODE/GNODE）です。
NODE_CON	スーパークラスです。
HOLDATE_CON	スーパークラスです。
RESINFO_GRPREVACL_COND_CON	条件に参加します。
RESINFO_HOST_CON	CACL ホストです。
USER_RESOURCE_ACL_CON	ユーザ用の ACL を含みます。
UACC_CON	デフォルト アクセスを含みます。
SPECIALPGMTYPE_CON	スーパークラスです。
GROUP_RESOURCE_ACL_CON	グループの ACL を含みます。
GROUPS_GROUP_CON	コンテナのメンバです。
RESAC_CON	CA Access Control プロパティにより拡張されます。
RAUDIT_CON	スーパークラスです。
MEMBERS_PARENT_CON	メンバを含みます。
INSERVRNGE_CON	スーパークラスです。
INETACL_CON	スーパークラスです。

FK 名	コメント
MEMBERS_CHILD_CON	メンバのコンテナです。
RESINFO_DEPTASKGRP_CON	スーパークラスです。
RESINFO_DEPTASK_CON	スーパークラスです。
RESINFO_USERREVACL_COND_CON	条件（制約なし）に参加します。
RESINFO_HOST_CON	CACL ホストです。
GROUPS_MEMBER_CON	コンテナを含みます。
LOGINAPPL_CON	
INSERVRNGE_CON	スーパークラスです。
NODEGRP_DEPTASK_CON	タスクのターゲット グループ（ノード グループ）です。
ACL_CON	ACL により保護されます。
USER_RESOURCE_ACL_CON	ユーザ用の ACL を含みます。
RULESET_RULESET_POLICY_CON	ポリシー内に取り込まれます。
RULESET_COMMAND_CON	コマンド内に取り込まれます。
SEOS_DH_FK	
SNAPSHOTINFO_CON	ユーザを含みます。
SNAPSHOT_CONFIG_CON	config を含みます。
SEOS_CON	オプションを含みます。
RESINFO_CON	リソースを含みます。
POLICYMODEL_CON	
CATEGORY_CON	カテゴリを含みます。
DAYTIME_CON	daytime 設定を含みます。
GROUPINFO_CON	グループを含みます。
USERACMODE_FK	CA Access Control モードを含みます。
USERACAUDIT_FK	CA Access Control 監査を含みます。
USERGRP_FK	グループに所属します。
USERREVACL_FK	ACL の影響を受けます。

FK 名	コメント
USERINFO_SUSPEND_USERAC_CON	ユーザによって一時停止されます。
USER_DEPTASK_CHECKER_CON	このタスクのチェッカです。
USER_DEPTASK_MAKER_CON	タスクのメーカーです。
USERAC_CON	CA Access Control プロパティにより拡張されます。

CONFIG_ENTRY_CON 関係の親テーブル

CONFIG は CONFIG_ENTRY_CON の親テーブルです。

CONFIG_ENTRY_CON 関係の子テーブル

CONFIG_ENTRY は CONFIG_ENTRY_CON の子テーブルです。

CONFIG_ENTRY_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
CONFIGNAME	CONFIGNAME

DEPTASK_RESULTMSG_CON 関係の親テーブル

DEPLOYMENT_TASK は、DEPTASK_RESULTMSG_CON の親テーブルです。

DEPTASK_RESULTMSG_CON 関係の子テーブル

DEPLOYMENT_RESULT_MESSAGE は、DEPTASK_RESULT_MSG_CON の子テーブルです。

DEPTASK_RESULTMSG_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

GROUPMEMBER_FK 関係の親テーブル

GROUPINFO は、GROUPMEMBER_FK の親テーブルです。

GROUPMEMBER_FK 関係の子テーブル

GROUPMEMBER は、GROUPMEMBER_FK の子テーブルです。

GROUPMEMBER_FK 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
GROUPID	GROUPID
GROUPTYPE	GROUPTYPE

GROUPREVACL_FK 関係の親テーブル

GROUPINFO は、GROUPREVACL_FK の親テーブルです。

GROUPREVACL_FK 関係の子テーブル

GROUPREVACL は、GROUPREVACL_FK の子テーブルです。

GROUPREVACL_FK 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
GROUPID	GROUPID
GROUPTYPE	GROUPTYPE

USERGRP_GROUP_CON 関係の親テーブル

GROUPINFO は、USERGRP_GROUP_CON の親テーブルです。

USERGRP_GROUP_CON 関係の子テーブル

USERGRP は、USERGRP_GROUP_CON の子テーブルです。

USERGRP_GROUP_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
GROUPID	GROUPID
GROUPTYPE	GROUPTYPE

MEMBEROF_FK 関係の親テーブル

GROUPINFO は、MEMBEROF_FK の親テーブルです。

MEMBEROF_FK 関係の子テーブル

MEMBEROF は、MEMBEROF_FK の子テーブルです。

MEMBEROF_FK 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
GROUPID	GROUPID
GROUPTYPE	GROUPTYPE

PASSWDRULES_FK 関係の親テーブル

GROUPINFO は、PASSWDRULES_FK の親テーブルです。

PASSWDRULES_FK 関係の子テーブル

PASSWDRULES は、PASSWDRULES_FK の子テーブルです。

PASSWDRULES_FK 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
GROUPID	GROUPID
GROUPTYPE	GROUPTYPE

USERLIST_FK 関係の親テーブル

GROUPINFO は、USERLIST_FK の親テーブルです。

USERLIST_FK 関係の子テーブル

USERLIST は、USERLIST_FK の子テーブルです。

USERLIST_FK 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
GROUPID	GROUPID
GROUPTYPE	GROUPTYPE

GROUPAUDIT_FK 関係の親テーブル

GROUPINFO は、GROUPAUDIT_FK の親テーブルです。

GROUPAUDIT_FK 関係の子テーブル

GROUPAUDIT は、GROUPAUDIT_FK の子テーブルです。

GROUPAUDIT_FK 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
GROUPID	GROUPID
GROUPTYPE	GROUPTYPE

SNAPSHOTINFO_FK 関係の親テーブル

HOSTINFO は、SNAPSHOTINFO_FK 親テーブルです。

SNAPSHOTINFO_FK 関係の子テーブル

SNAPSHOTINFO は、SNAPSHOTINFO_FK の子テーブルです。

SNAPSHOTINFO_FK 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
HOSTID	HOSTID

NODE_ALIAS_FK 関係の親テーブル

NODE は、NODE_ALIAS_FK の親テーブルです。

NODE_ALIAS_FK 関係の子テーブル

NODE_ALIAS は、NODE_NODE_ALIAS_FK の子テーブルです。

NODE_ALIAS_FK 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

NODE_SUBSCRIPTION_PUBLISHER 関係の親テーブル

NODE は、NODE_SUBSCRIPTION_PUBLISHER の親テーブルです。

NODE_SUBSCRIPTION_PUBLISHER 関係の子テーブル

NODE_SUBSCRIPTION_STATUS は、NODE_SUBSCRIPTION_PUBLISHER の子テーブルです。

NODE_SUBSCRIPTION_PUBLISHER 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	PUBLISHERCNAME
RULEKEY	PUBLISHERONAME

NODE_EFFECTIVE_POLICY_CON 関係の親テーブル

NODE は、NODE_EFFECTIVE_POLICY_CON の親テーブルです。

NODE_EFFECTIVE_POLICY_CON 関係の子テーブル

EFFECTIVE_POLICY は、NODE_EFFECTIVE_POLICY_CON の子テーブルです。

NODE_EFFECTIVE_POLICY_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

NODE_SUBSCRIPTION_SUBSCRIBER 関係の親テーブル

NODE は、NODE_SUBSCRIPTION_SUBSCRIBERER の親テーブルです。

NODE_SUBSCRIPTION_SUBSCRIBER 関係の子テーブル

NODE_SUBSCRIPTION_STATUS は、NODE_SUBSCRIPTION_SUBSCRIBER の子テーブルです。

NODE_SUBSCRIPTION_SUBSCRIBER 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	SUBSCRIBERCNAME
RULEKEY	SUBSCRIBERONAME

NODE_POLICY_STATUS_CON 関係の親テーブル

NODE は、NODE_POLICY_STATUS_CON の親テーブルです。

NODE_POLICY_STATUS_CON 関係の子テーブル

POLICY_STATUS は、NODE_POLICY_STATUS_CON の子テーブルです。

NODE_POLICY_STATUS_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	NODE_RESCLASS
RULEKEY	NODE_RULEKEY

NODE_DEPTASKGRP_CON 関係の親テーブル

NODE は、NODE_DEPTASKGRP_CON の親テーブルです。

NODE_DEPTASKGRP_CON 関係の子テーブル

DEPLOYMENT_TASK_GROUP は、NODE_DEPTASKGRP_CON の子テーブルです。

NODE_DEPTASKGRP_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	NODE_RESCLASS
RULEKEY	NODE_RULEKEY

NODE_ADDRESS_FK 関係の親テーブル

NODE は、NODE_ADDRESS_FK の親テーブルです。

NODE_ADDRESS_FK 関係の子テーブル

NODE_ADDRESS は、NODE_ADDDRESS_FK の子テーブルです。

NODE_ADDRESS_FK 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

NODE_NODE_DEVIATION_CON 関係の親テーブル

NODE は、NODE_NODE_DEVIATION_CON の親テーブルです。

NODE_NODE_DEVIATION_CON 関係の子テーブル

NODE_DEVIATION は、NODE_NODE_DEVIATION_CON の子テーブルです。

NODE_NODE_DEVIATION_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	NODE_RESCLASS
RULEKEY	NODE_RULEKEY

NODE_DEPTASK_CON 関係の親テーブル

NODE は、NODE_DEPTASK_CON の親テーブルです。

NODE_DEPTASK_CON 関係の子テーブル

DEPLOYMENT_TASK は、NODE_DEPTASK_CON の子テーブルです。

NODE_DEPTASK_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	NODE_RESCLASS
RULEKEY	NODE_RULEKEY

POLICY_POLICY_STATUS_CON 関係の親テーブル

POLICY は、POLICY_POLICY_STATUS_CON の親テーブルです。

POLICY_POLICY_STATUS_CON 関係の子テーブル

POLICY_STATUS は、POLICY_POLICY_STATUS_CON の子テーブルです。

POLICY_POLICY_STATUS_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	POLICY_RESCLASS
RULEKEY	POLICY_RULEKEY

LATESTFIN_POLICYGRP_CON 関係の親テーブル

POLICY は、LATESTFIN_POLICYGRP_CON の親テーブルです。

LATESTFIN_POLICYGRP_CON 関係の子テーブル

POLICY_GROUP は、LATESTFIN_POLICYGRP_CON の子テーブルです。

LATESTFIN_POLICYGRP_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	LATEST_FIN_RESCLASS
RULEKEY	LATEST_FIN_RULEKEY

POLICY_EFFECTIVE_POLICY_CON 関係の親テーブル

POLICY は、POLICY_EFFECTIVE_POLICY_CON の親テーブルです。

POLICY_EFFECTIVE_POLICY_CON 関係の子テーブル

POLICY_EFFECTIVE は、POLICY_EFFECTIVE_POLICY_CON の子テーブルです。

POLICY_EFFECTIVE_POLICY_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	POLICY_RESCLASS
RULEKEY	POLICY_RULEKEY

POLICY_POLICY_DEVIATION_CON 関係の親テーブル

POLICY は、POLICY_POLICY_DEVIATION_CON の親テーブルです。

POLICY_POLICY_DEVIATION_CON 関係の子テーブル

POLICY_DEVIATION は、POLICY_POLICY_DEVIATION_CON の子テーブルです。

POLICY_POLICY_DEVIATION_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	POLICY_RESCLASS
RULEKEY	POLICY_RULEKEY

POLICY_RULESET_POLICY_CON 関係の親テーブル

POLICY は、POLICY_RULESET_POLICY_CON の親テーブルです。

POLICY_RULESET_POLICY_CON 関係の子テーブル

POLICY_RULESET は、POLICY_RULESET_POLICY_CON の子テーブルです。

POLICY_RULESET_POLICY_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	POLICY_RESCLASS
RULEKEY	POLICY_RULEKEY

LATEST_POLICYGRP_CON 関係の親テーブル

POLICY は、LATEST_POLICYGRP_CON の親テーブルです。

LATEST_POLICYGRP_CON 関係の子テーブル

POLICY_GROUP は、LATEST_POLICYGRP_CON の子テーブルです。

LATEST_POLICYGRP_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	LATEST_RESCLASS
RULEKEY	LATEST_RULEKEY

POLICY_DEPTASK_CON 関係の親テーブル

POLICY は、POLICY_DEPTASK_CON の親テーブルです。

POLICY_DEPTASK_CON 関係の子テーブル

DEPLOYMENT_TASK は、POLICY_DEPTASK_CON の子テーブルです。

POLICY_DEPTASK_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	POLICY_RESCLASS
RULEKEY	POLICY_RULEKEY

POLICYGRP_DEPTASK_CON 関係の親テーブル

POLICY_GROUP は、POLICYGRP_DEPTASK_CON の親テーブルです。

POLICYGRP_DEPTASK_CON 関係の子テーブル

DEPLOYMENT_TASK は、POLICYGRP_DEPTASK_CON の子テーブルです。

POLICYGRP_DEPTASK_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	POLICYGRP_RESCLASS
RULEKEY	POLICYGRP_RULEKEY

POLICYGRP_DEPTASKGRP_CON 関係の親テーブル

POLICY_GROUP は、POLICYGRP_DEPTASKGRP_CON の親テーブルです。

POLICYGRP_DEPTASKGRP_CON 関係の子テーブル

DEPLOYMENT_TASK_GROUP は、POLICYGRP_DEPTASKGRP_CON の子テーブルです。

POLICYGRP_DEPTASKGRP_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	POLICYGRP_RESCLASS
RULEKEY	POLICYGRP_RULEKEY

POLICY_GROUP_DEP_ON_CON 関係の親テーブル

POLICY_GROUP は、POLICY_GROUP_DEP_ON_CON の親テーブルです。

POLICY_GROUP_DEP_ON_CON 関係の子テーブル

POLICY_GROUP_DEPENDENCY は、POLICY_GROUP_DEP_ON_CON の子テーブルです。

POLICY_GROUP_DEP_ON_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	DEP_ON_RESCLASS

親列名	子列名
RULEKEY	DEP_ON_RULEKEY

POLICY_GROUP_DEP_CON 関係の親テーブル

POLICY_GROUP は、POLICY_GROUP_DEP_CON の親テーブルです。

POLICY_GROUP_DEP_CON 関係の子テーブル

POLICY_GROUP_DEPENDENCY は、POLICY_GROUP_DEP_CON の子テーブルです。

POLICY_GROUP_DEP_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

PMD_SUBSC_CON 関係の親テーブル

POLICYMODELINFO は、PMD_SUBSC_CON の親テーブルです。

PMD_SUBSC_CON 関係の子テーブル

LOCAL_PMD_SUBSCRIBER は、PMD_SUBSC_CON の子テーブルです。

PMD_SUBSC_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

POLICYGRP_NODASS_POL_CON 関係の親テーブル

RESINFO は、POLICYGRP_NODASS_POL_CON の親テーブルです。

POLICYGRP_NODASS_POL_CON 関係の子テーブル

POLICY_GROUP_NODE_ASSIGNMENT は、POLICYGRP_NODASS_POL_CON の子テーブルです。

POLICYGRP_NODASS_POL_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	NODE_RESCLASS
RULEKEY	NODE_RULEKEY

POLICY_GROUP_CON 関係の親テーブル

RESINFO は、POLICY_GROUP_CON の親テーブルです。

POLICY_GROUP_CON 関係の子テーブル

POLICY_GROUP は、POLICY_GROUP_CON の子テーブルです。

POLICY_GROUP_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

POLICY_CON 関係の親テーブル

RESINFO は、POLICY_CON の親テーブルです。

POLICY_CON 関係の子テーブル

POLICY は、POLICY_CON の子テーブルです。

POLICY_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

RULESET_CON 関係の親テーブル

RESINFO は、RULESET_CON の親テーブルです。

RULESET_CON 関係の子テーブル

RULESET は、RULESET_CON の子テーブルです。

RULESET_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

POLICYGRP_NODASS_NOD_CON 関係の親テーブル

RESINFO は、POLICYGRP_NODASS_NOD_CON の親テーブルです。

POLICYGRP_NODASS_NOD_CON 関係の子テーブル

POLICY_GROUP_NODE_ASSIGNMENT は、POLICYGRP_NODASS_NOD_CON の子テーブルです。

POLICYGRP_NODASS_NOD_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	POLICYGRP_RESCLASS
RULEKEY	POLICYGRP_RULEKEY

NODE_CON 関係の親テーブル

RESINFO は、NODE_CON の親テーブルです。

NODE_CON 関係の子テーブル

NODE は、NODE_CON の子テーブルです。

NODE_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

GROUP_RESOURCE_ACL_CON 関係の親テーブル

RESINFO は、GROUP_RESOURCE_ACL_CON の親テーブルです。

GROUP_RESOURCE_ACL_CON 関係の子テーブル

GROUPREVACL は、GROUP_RESOURCE_ACL_CON の子テーブルです。

GROUP_RESOURCE_ACL_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
RESCLASS	RESCNAME
RULEKEY	RESONAME
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

RESINFO_USERREVACL_COND_CON 関係の親テーブル

RESINFO は、RESINFO_USERREVACL_COND_CON の親テーブルです。

RESINFO_USERREVACL_COND_CON 関係の子テーブル

USERREVACL は、RESINFO_USERREVACL_COND_CON の子テーブルです。

RESINFO_USERREVACL_COND_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
RESCLASS	CONCNAME
RULEKEY	CONONAME
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

UACC_CON 関係の親テーブル

RESINFO は、UACC_CON の親テーブルです。

UACC_CON 関係の子テーブル

UACC は、UACC_CON の子テーブルです。

UACC_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

SPECIALPGMTYPE_CON 関係の親テーブル

RESINFO は、SPECIALPGMTYPE_CON の親テーブルです。

SPECIALPGMTYPE_CON 関係の子テーブル

SPECIALPGMTYPE は、SPECIALPGMTYPE_CON の子テーブルです。

SPECIALPGMTYPE_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

RESAC_CON 関係の親テーブル

RESINFO は、RESAC_CON の親テーブルです。

RESAC_CON 関係の子テーブル

RESAC は、RESAC_CON の子テーブルです。

RESAC_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

RAUDIT_CON 関係の親テーブル

RESINFO は、RAUDIT_CON の親テーブルです。

RAUDIT_CON 関係の子テーブル

RAUDIT は、RAUDIT_CON の子テーブルです。

RAUDIT_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

MEMBERS_PARENT_CON 関係の親テーブル

RESINFO は、MEMBERS_PARENT_CON の親テーブルです。

MEMBERS_PARENT_CON 関係の子テーブル

MEMBERS は、MEMBERS_PARENT_CON の子テーブルです。

MEMBERS_PARENT_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

RESINFO_DEPTASKGRP_CON 関係の親テーブル

RESINFO は、RESINFO_DEPTASKGRP_CON の親テーブルです。

RESINFO_DEPTASKGRP_CON 関係の子テーブル

DEPLOYMENT_TASK_GROUP は、RESINFO_DEPTASKGRP_CON の子テーブルです。

RESINFO_DEPTASKGRP_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

RESINFO_DEPTASK_CON 関係の親テーブル

RESINFO は、RESINFO_DEPTASK_CON の親テーブルです。

RESINFO_DEPTASK_CON 関係の子テーブル

DEPLOYMENT_TASK は、RESINFO_DEPTASK_CON の子テーブルです。

LOGINAPPL_CON 関係の親テーブル

RESINFO は、LOGINAPPL_CON の親テーブルです。

LOGINAPPL_CON 関係の子テーブル

LOGINAPPL は、LOGINAPPL_CON の子テーブルです。

LOGINAPPL_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

INSERVRNGE_CON 関係の親テーブル

RESINFO は、INSERVRNGE_CON の親テーブルです。

INSERVRNGE_CON 関係の子テーブル

INSERVRNGE は、INSERVRNGE_CON の子テーブルです。

INSERVRNGE_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

NODEGRP_DEPTASKGRP_CON 関係の親テーブル

RESINFO は、NODEGRP_DEPTASKGRP_CON の親テーブルです。

NODEGRP_DEPTASKGRP_CON 関係の子テーブル

DEPLOYMENT_TASK_GROUP は、NODEGRP_DEPTASKGRP_CON の子テーブルです。

NODEGRP_DEPTASKGRP_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	NODEGRP_RESCLASS
RULEKEY	NODEGRP_RULEKEY

RESINFO_GRPREVACL_COND_CON 関係の親テーブル

RESINFO は、RESINFO_GRPREVACL_COND_CON の親テーブルです。

RESINFO_GRPREVACL_COND_CON 関係の子テーブル

GROUPREVACL は、RESINFO_GRPREVACL_COND_CON の子テーブルです。

RESINFO_GRPREVACL_COND_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
RESCLASS	CONCNAME
RULEKEY	CONONAME
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

RESINFO_HOST_CON 関係の親テーブル

RESINFO は、RESINFO_HOST_CON の親テーブルです。

RESINFO_HOST_CON 関係の子テーブル

ACL は、RESINFO_HOST_CON の子テーブルです。

RESINFO_HOST_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
RESCLASS	HOSTCNAME
RULEKEY	HOSTONAME
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

GROUPS_GROUP_CON 関係の親テーブル

RESINFO は、GROUPS_GROUP_CON の親テーブルです。

GROUPS_GROUP_CON 関係の子テーブル

GROUPS は、GROUPS_GROUP_CON の子テーブルです。

GROUPS_GROUP_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
RESCLASS	CNAME
RULEKEY	ONAME
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

INETACL_CON 関係の親テーブル

RESINFO は、INETACL_CON の親テーブルです。

INETACL_CON 関係の子テーブル

INETACL は、INETACL_CON の子テーブルです。

INETACL_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

HOLDATE_CON 関係の親テーブル

RESINFO は、HOLDATE_CON の親テーブルです。

HOLDATE_CON 関係の子テーブル

HOLDATE は、HOLDATE_CON の子テーブルです。

HOLDATE_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

GROUPS_MEMBER_CON 関係の親テーブル

RESINFO は、GROUPS_MEMBER_CON の親テーブルです。

GROUPS_MEMBER_CON 関係の子テーブル

GROUPS は、GROUPS_MEMBER_CON の子テーブルです。

GROUPS_MEMBER_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

ACL_CON 関係の親テーブル

RESINFO は、ACL_CON の親テーブルです。

ACL_CON 関係の子テーブル

ACL は、ACL_CON の子テーブルです。

ACL_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RESCLASS
RULEKEY	RULEKEY

MEMBERS_CHILD_CON 関係の親テーブル

RESINFO は、MEMBER_CHILD_CON の親テーブルです。

MEMBERS_CHILD_CON 関係の子テーブル

MEMBER は、MEMBERS_CHILD_CON の子テーブルです。

MEMBERS_CHILD_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
RESCLASS	CNAME
RULEKEY	ONAME
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

USER_RESOURCE_ACL_CON 関係の親テーブル

USER は、RESINFO_RESOURCE_ACL_CON の親テーブルです。

USER_RESOURCE_ACL_CON 関係の子テーブル

RESOURCE は、USER_USERREVACL_ACL_CON の子テーブルです。

USER_RESOURCE_ACL_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
RESCLASS	RESCNAME
RULEKEY	RESONAME
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

RULESET_RULESET_POLICY_CON 関係の親テーブル

RULESET は、RULESET_RULESET_POLICY_CON の親テーブルです。

RULESET_RULESET_POLICY_CON 関係の子テーブル

RULESET_RULESET は、POLICY_RULESET_POLICY_CON の子テーブルです。

RULESET_RULESET_POLICY_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RULESET_RESCLASS
RULEKEY	RULESET_RULEKEY

RULESET_COMMAND_CON 関係の親テーブル

RULESET は、RULESET_COMMAND_CON の親テーブルです。

RULESET_COMMAND_CON 関係の子テーブル

RULESET_COMMAND は、RULESET_COMMAND_CON の子テーブルです。

RULESET_COMMAND_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
RESCLASS	RULESET_RESCLASS
RULEKEY	RULESET_RULEKEY

SEOS_DH_FK 関係の親テーブル

SEOS は、SEOS_DH_FK の親テーブルです。

SEOS_DH_FK 関係の子テーブル

DISTRIBUTION_HOST は、SEOS_DH_FK の子テーブルです。

SEOS_DH_FK 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

DAYTIME_CON 関係の親テーブル

SNAPSHOTINFO は、DAYTIME_CON の親テーブルです。

DAYTIME_CON 関係の子テーブル

DAYTIME は、CATEGORY_CON の子テーブルです。

DAYTIME_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

SEOS_CON 関係の親テーブル

SNAPSHOTINFO は、SEOS_CON の親テーブルです。

SEOS_CON 関係の子テーブル

SEOS は、SEOS_CON の子テーブルです。

SEOS_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

SEOSSYSCALL_CON 関係の親テーブル

SNAPSHOTINFO は、SEOSSYSCALL_CON の親テーブルです。

SEOSSYSCALL_CON 関係の子テーブル

SEOSSYSCALL は、SEOSSYSCALL_CON の子テーブルです。

SEOSSYSCALL_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

SNAPSHOT_CONFIG_CON 関係の親テーブル

SNAPSHOTINFO は、SNAPSHOT_CONFIG_CON の親テーブルです。

SNAPSHOT_CONFIG_CON 関係の子テーブル

CONFIG は、SNAPSHOT_CONFIG_CON の子テーブルです。

SNAPSHOT_CONFIG_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

SYSCALL_CON 関係の親テーブル

SEOSSYSCALL は、SYSCALL_CONFIG_CON の親テーブルです。

SYSCALL_CON 関係の子テーブル

SYSCALL は、SYSCALL_CON の子テーブルです。

SYSCALL_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

SYSCALLUSERSPECIALPGM 関係の親テーブル

SEOSSYSCALL は、SYSCALLUSERSPECIALPGM の親テーブルです。

SYSCALLUSERSPECIALPGM 関係の子テーブル

SYSCALLUSERSPECIALPGM は、SYSCALLUSERSPECIALPGM の子テーブルです。

SYSCALLUSERSPECIALPGM 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

CATEGORY_CON 関係の親テーブル

SNAPSHOTINFO は、CATEGORY_CON の親テーブルです。

CATEGORY_CON 関係の子テーブル

CATEGORY は、CATEGORY_CON の子テーブルです。

CATEGORY_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

GROUPINFO_CON 関係の親テーブル

SNAPSHOTINFO は、GROUPINFO_CON の親テーブルです。

GROUPINFO_CON 関係の子テーブル

GROUPINFO は、CATEGORY_CON の子テーブルです。

GROUPINFO_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

SNAPSHOTINFO_CON 関係の親テーブル

SNAPSHOTINFO は、SNAPSHOTINFO_CON の親テーブルです。

SNAPSHOTINFO_CON 関係の子テーブル

USERINFO は、SNAPSHOTINFO_CON の子テーブルです。

SNAPSHOTINFO_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

RESINFO_CON 関係の親テーブル

SNAPSHOTINFO は、RESINFO_CON の親テーブルです。

RESINFO_CON 関係の子テーブル

RESINFO は、RESINFO_CON の子テーブルです。

RESINFO_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

POLICYMODEL_CON 関係の親テーブル

SNAPSHOTINFO は、POLICYMODEL_CON の親テーブルです。

POLICYMODEL_CON 関係の子テーブル

POLICYMODELINFO は、POLICYMODEL_CON の子テーブルです。

POLICYMODEL_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

USERACAUDIT_FK 関係の親テーブル

USERAC は、USERACAUDIT_FK の親テーブルです。

USERACAUDIT_FK 関係の子テーブル

USERACAUDIT は、USERACAUDIT_FK の子テーブルです。

USERACAUDIT_FK 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
USERID	USERID
USERTYPE	USERTYPE

USERACMODE_FK 関係の親テーブル

USERAC は、USERACMODE_FK の親テーブルです。

USERACMODE_FK 関係の子テーブル

USERACMODE は、USERACMODE_FK の子テーブルです。

USERACMODE_FK 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
USERID	USERID
USERTYPE	USERTYPE

USERGRP_FK 関係の親テーブル

USERAC は、USERGRP_FK の親テーブルです。

USERGRP_FK 関係の子テーブル

USERGRP は、USERGRP_FK の子テーブルです。

USERGRP_FK 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
USERID	USERID
USERTYPE	USERTYPE

USERINFO_SUSPEND_USERAC_CON 関係の親テーブル

USERINFO は、USERINFO_SUSPEND_USERAC_CON の親テーブルです。

USERINFO_SUSPEND_USERAC_CON 関係の子テーブル

USERAC は、USERINFO_SUSPEND_USERAC_CON の子テーブルです。

USERINFO_SUSPEND_USERAC_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
USERTYPE	SUSPENDWHOCNAME
USERID	SUSPENDWHOONAME
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID

USER_DEPTASK_CHECKER_CON 関係の親テーブル

USER は、USERINFO_DEPTASK_CHECKER_CON の親テーブルです。

USER_DEPTASK_CHECKER_CON 関係の子テーブル

DEPLOYMENT_TASK は、USER_DEPTASK_CHECKER_CON の子テーブルです。

USER_DEPTASK_CHECKER_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
USERID	CHECKERID
USERTYPE	CHECKERTYPE

USER_DEPTASK_MAKER_CON 関係の親テーブル

USERINFO は、USER_DEPTASK_CON の親テーブルです。

USER_DEPTASK_MAKER_CON 関係の子テーブル

DEPLOYMENT_TASK は、USER_DEPTASK_CON の子テーブルです。

USER_DEPTASK_MAKER_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
USERID	MAKERID
USERTYPE	MAKERTYPE

USERREVACL_FK 関係の親テーブル

USERINFO は、USERREVACL_FK の親テーブルです。

USERREVACL_FK 関係の子テーブル

USERREVACL は、USERREVACL_FK の子テーブルです。

USERREVACL_FK 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
USERID	USERID
USERTYPE	USERTYPE

USERAC_CON 関係の親テーブル

USERINFO は、USERAC_CON の親テーブルです。

USERAC_CON 関係の子テーブル

USERAC は、USERAC_CON の子テーブルです。

USERAC_CON 関係の移行された列

次の表で、親テーブルの列と子テーブルの列との関係について説明します。

親列名	子列名
SNAPSHOTID	SNAPSHOTID
HOSTID	HOSTID
USERID	USERID
USERTYPE	USERTYPE