*e*Trust® Access Control for Windows

リファレンス ガイド

r8 SP1

CA 製品の参照

このマニュアルが参照している CA の製品は以下のとおりです。

- eTrust® Access Control (eTrust AC)
- eTrust® Single Sign-On (eTrust SSO)
- eTrust® Web Access Control (eTrust Web AC)
- eTrust® CA-Top Secret®
- eTrust® CA-ACF2®
- eTrust® Audit
- Unicenter® TNG
- Unicenter® Network and Systems Management (Unicenter NSM)
- Unicenter® Software Delivery

テクニカル サポートの連絡先

オンライン 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.caj.co.jp/support/）を参照してください。

目次

第 1 章: selang - eTrust AC のコマンド言語

eTrust Access Control は、eTrust Access Control のコマンド言語である *selang* というコマンド シェルを使用して管理します。この章では、selang のコマンドの入力方法、カテゴリ別のコマンドの一覧、および selang コマンド言語に関するその他の一般情報について説明します。

この後の章では、selang のコマンドについて詳しく説明します。selang は複数の***環境***で実行できるため、環境別に章を分けて selang のコマンドについて説明します。複数の環境で共通のコマンドもありますが、その場合でも、コマンドのパラメータおよび引数は異なる場合があります。そのため、新しい環境で作業を始めるときは、必ず構文を確認してください。

このセクションには、以下のトピックが含まれます。

コマンドの表記規則

eTrust Access Control のドキュメントでは、コマンド構文やユーザ入力の説明の際に、いくつかの特殊な表記法を使用しています。

表記	意味
等幅フォント	コードまたはプログラムの出力
斜体	情報を入力するためのプレースホルダ
太字	表示されているとおりに入力する必要のある要素
角かっこ ([]) で囲まれた文字列	省略可能な項目
中かっこ ({}) 内でパイプ (|) で区切られた選択項目	選択すべき項目を 1 つだけ含む選択項目のセット
行の最後にあるスペースと円記号 (¥)	次の行にコマンドが続く

注:

- 太字は、強調の意味にも使用されています。 次に例を示します。

  パスワードをモニタに貼り付けたままに**しないでください**。

- 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、行末のスペースとそれに続く円記号(¥)は、そのコマンドが次の行に続いていることを示します。

  注: 円記号は実際のコマンド構文では不要なため、コピーしないでください。

- いずれか 1 つのみ選択する項目は、パイプ(|)で区切られています。 選択項目のセットは中かっこ({})で囲まれています。いずれかの項目を入力する場合、この中かっこは**入力しません**。 たとえば、以下の例では、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*}

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:

- 太字で示されたコマンド名(ruler)は表示されているとおりに入力します。
- 斜体で示された *className* オプションは、クラス名(USER など)のプレースホルダです。
- 後半の角かっこの部分を指定しなくても、コマンドは実行できます。
- 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。

selang コマンド シェル

Windows から selang コマンド シェルを呼び出すには、cmd.exe を実行し、*eTrustACDir*¥bin ディレクトリに移動します(*eTrustACDir* は、eTrust Access Control をインストールしたディレクトリです。また、デフォルトのディレクトリは、*system_directory*¥Program Files¥CA¥eTrustAccessControl です)。その後、以下のコマンドを入力します。

```
selang
```

以下のプロンプトが表示されます。

```
eTrustAC>
```

このプロンプトが表示されたら、selang のコマンドを入力できます。複数のコマンドを入力する場合は、セミコロン(;)で区切ります。1 つのコマンドを複数の行にまたがって入力する必要がある場合は、行末に円記号(¥)を入力して、以下の行に残りを入力します。

コマンド ライン インターフェースではなく GUI を使用する場合も、ポリシー マネージャを使用して eTrust Access Control データベースおよび Windows データベースにアクセスして更新を行うことができます。詳細については、「**導入ガイド**」および「**管理者ガイド**」を参照してください。

異なる環境での作業

selang を使用すると、ローカル eTrust Access Control データベースだけでなく、ネイティブ Windows データベース、ローカル Policy Model データベース(PMDB)、または eTrust Access Control がインストールされているリモート ホスト(Windows または UNIX/Linux)上のデータベースを変更できます。環境を切り替えるには、「env」(environment)コマンドを使用します。このコマンドはすべての環境で使用できます。

ローカル PMDB を変更するには、以下のコマンドを入力します。

```
env pmd
```

プロンプトが以下のように変わります。

```
eTrustAC(pmd)>
```

これ以降、selang のコマンドはすべて、PMDB に対して実行されます。

ローカル Windows データベースを変更するには、以下のコマンドを入力します。

```
env nt
```

以下のプロンプトが表示されます。

```
eTrustAC(nt)>
```

これ以降、selang のコマンドで Windows データベースを変更できます。eTrust Access Control 環境に戻るには、以下のコマンドを入力します。

```
env eTrust
```

元のプロンプトが表示されます。

```
eTrustAC>
```

これ以降、selang のコマンドはすべて、Windows データベースではなく、eTrust Access Control データベースに対して実行されます。

注: 環境を切り替えるときに、切り替え先の環境のプレフィクスのみを入力することもできます。たとえば、eTrust 環境に切り替えるには、以下のいずれかのコマンドを入力します。

- `env e`
- `env et`

PMD 環境に変更するには、以下のいずれかのコマンドを入力します。

- env p
- env pm

selang コマンド シェルは、一般的な UNIX/Linux コマンドもサポートしているので、UNIX/Linux マシンに接続している場合は、eTrust Access Control 内から UNIX/Linux 環境を管理することができます。UNIX/Linux コマンドを有効にするには、以下のコマンドを入力します。

```
env unix
```

詳細については、「eTrust Access Control for UNIX and Linux リファレンス ガイド」の「UNIX/Linux 環境の selang のコマンド」を参照してください。

デフォルトでは、selang コマンド シェルは、ローカル eTrust Access Control および PMDB に対して実行されます。別の端末上のデータベースに対してコマンドを実行する場合は、selang のコマンドを入力する前に hosts コマンドを指定します。詳細については、「eTrust 環境のクラスとプロパティ」の章の hosts コマンドの説明を参照してください。

注: env を使用して、コマンドのネイティブ プロパティを入力すると、そのコマンドがネイティブ環境と現在の環境の両方に入力されます。

ファンクション キー

selang コマンド シェルでは、さまざまなショートカットを使用して効率よく作業できます。selang のコマンドを入力するときに使用できるファンクション キーとその説明を以下の表に示します。

上方向キー

1 つ前のコマンドをバッファから取り出します。このキーを押すたびに、バッファ内の上位にあるコマンドが順次呼び出されます。バッファには、作業中のセッションで入力されたすべてのコマンドが格納されています。

下方向キー

バッファ内の下位のコマンドに移動します。このキーは、上方向キーと同様に使用します。

左方向キー

コマンド ライン上でカーソルを左に移動します。Insert キーのモード(挿入または上書き)を切り替えます。

右方向キー

コマンド ライン上でカーソルを右に移動します。

F1

1 つ前のコマンドを 1 文字ずつ挿入します。

F2

ウィンドウに「入力文字の前までコピー:」というメッセージが表示されます。1 つ前のコマンドに含まれる文字を入力すると、コマンドでその文字が最初に出現するまでの部分が自動的に入力されます。コマンド内に同じ文字が複数ある場合は、F2 キーをもう一度押すと、コマンドでその文字が 2 回目に出現するまでの部分が自動的に入力されます。

取り消すには Backspace キーを押します。

F3

1 つ前のコマンドを入力します(上方向キーと同じ)。

F4

1 つ前のコマンドを編集します。ウィンドウに「入力文字の前まで削除:」というメッセージが表示されます。

取り消すには Backspace キーを押します。

F5

1 つ前のコマンドを入力します（上方向キーと同じ）。

F6

コマンド ラインに Ctrl+Z（^Z）を入力します。これにより、Enter キーを押して次の行に続けてコマンドを入力できるようになります。

F7

コマンド履歴を示すウィンドウを表示します。上下の方向キーで、前に入力した任意のコマンドを選択できます。

取り消すには Esc キーを押します。

F8

上方向キーと同様に 1 つ前のコマンドを入力します。ただし、カーソルはコマンドラインの最後ではなく先頭に表示されます。

F9

ウィンドウに「コマンド番号を入力：」というメッセージが表示されます。F7 キーで表示したコマンドの一覧にある数字を入力すると、その数字に対応するコマンドが挿入されます。

取り消すには Esc キーを押します。

ヘルプ

対話形式の selang のコマンド環境では、いつでもヘルプを表示できます。

selang のオンライン ヘルプを表示するには、「?」、「help」、「h」、「h *topic*」または「help *topic*」と入力します（*topic* には、selang のコマンド、または selang コマンド シェルに関連するその他のトピックを指定します）。

selang のオンライン ヘルプ テキストが画面に表示されます。トピックを指定した場合は、指定したトピックについて説明するヘルプ テキストが表示されます。トピックを指定しないと、ヘルプの目次が表示されます。

注: コマンド ラインのテキストを削除せずに、コマンド ラインに入力したコマンドのヘルプ テキストを表示するには、Ctrl キーを押しながら 2 を押します。

help コマンドの詳細については、この章の「その他のコマンド」の help コマンドの説明を参照してください。

権限

selang のコマンドを使用して eTrust データベースまたはネイティブ オペレーティング システム(ネイティブ OS)データベースのレコードを変更するには、適切な権限が必要です。ほとんどのコマンドの場合、実行するには以下のいずれかの条件を満たしている必要があります。

- リソースの所有者であること。
- ADMIN 属性が割り当てられていること。
- GROUP-ADMIN 属性で管理者権限を与えられたグループの有効範囲内に、目的のリソース レコードが含まれていること。
- ADMIN クラスのレコードの ACL に、CREATE アクセス権限または MODIFY アクセス権限が設定されていること。
- ネイティブ Windows 環境の管理のみが許可されている場合は、Windows データベースの eTrust Access Control Admins グループのメンバであること。

これらの一般原則の例外については、コマンドの説明に注記してあります。

selang の構文規則

selang の各コマンドは、eTrust Access Control データベースに対して特定のアクションを実行します。selang のコマンド構文は、以下のとおりです。

commandname *parameters*

eTrust Access Control では、実行するコマンドはコマンド名によって識別されます。通常は、コマンドの後に 1 つまたは複数のパラメータを指定します。パラメータは、コマンドの実行に必要な追加情報を eTrust Access Control に渡します。

selang のパラメータ構文は、以下のとおりです。

parameterName[(arguments)]

eTrust Access Control では、パラメータはパラメータ名によって識別されます。多くのパラメータでは、パラメータの処理に必要な情報を eTrust Access Control に渡す引数を指定する必要があります。複数の引数を指定できるパラメータもあります。複数の引数を指定する場合は、カンマまたはスペースで引数を区切ります。パラメータの引数そのものがパラメータになる場合もあります。

文字列で引数を定義する場合にレコード プロパティを削除するには、空のかっこ「()」を使用してプロパティを入力します。場合によっては、引数としてアスタリスク(*)を使用できます。アスタリスクは、その引数が取る可能性のあるすべての値を表すことができます。アスタリスクを使用する前または後のコマンドで同じ引数に特定の値を指定した場合、その特定の値の指定は**無効になりません**。また、引数がファイル名の場合は、ファイル名パターンの一部としてワイルドカードを使用できます。ワイルドカードは、「*」(0 個以上の文字を表す)と「?」 (1 個の文字を表す)です。

selang コマンド言語は、コマンドとパラメータのプレフィクスをサポートしています。入力する必要があるのは、コマンドまたはパラメータを一意に指定するための文字のみ(つまり、プレフィクス)です。コマンド名またはパラメータ名をすべて入力する必要はありません。

たとえば、showusr コマンドを入力するには「showu」と入力します。このように入力するだけで、eTrust Access Control では showusr コマンドとして認識されます。また、すべてのコマンドには 1 つまたは複数の文字で構成された省略形があります。たとえば、showusr コマンドの場合は、「su」と入力するだけで済みます。

UNIX/Linux 環境では、ユーザが指定する情報は大文字と小文字が区別され、両方の文字を使用できます。たとえば、ユーザ ID が user53 のユーザのフルネームを「Mike Jones」と指定できます。Windows 環境では、情報の大文字と小文字の区別は認識されませんが、***その情報は保存されます***。UNIX/Linux ワークステーションから Windows のリモート ホストを管理する場合、UNIX/Linux では***保存された状態***のユーザ指定情報が検索されます。たとえば、eTrust Access Control ローカル データベースを管理する場合、Windows 環境では「Mike Jones」として識別されるユーザの名前を「mike jones」と入力することができます。ただし、このデータベースをリモート UNIX/Linux マシンから管理する場合は、ユーザ名を「Mike Jones」と入力する必要があります。

カテゴリ別の selang のコマンド

このセクションでは、以下のカテゴリ別に selang のすべてのコマンドの一覧を示します。

- ユーザを管理するためのコマンド
- グループを管理するためのコマンド
- リソースを管理するためのコマンド
- その他のコマンド

複数のカテゴリに重複して分類されているコマンドもあります。コマンドを使用する環境も示してあります。ネイティブ環境は、接続するホストのオペレーティング システムに応じて、NT または UNIX/Linux のいずれかの環境の規則と一致するため、省略してあります。

ユーザ コマンド

authorize

eTrust および NT 環境で有効です。

特定のリソースへのアクセス権限を特定のユーザに設定します。

authorize-

eTrust および NT 環境で有効です。

特定のリソースへのアクセス権限を特定のユーザから削除します。

checkpwd

eTrust および NT 環境で有効です。

ユーザの新しいパスワードをチェックして、変更はせずに、パスワード ルールに従っていることを確認します。

chusr

eTrust、NT、および UNIX/Linux 環境で有効です。

eTrust Access Control データベースまたはネイティブ OS データベースの既存のユーザ設定を変更します。

editusr

eTrust、NT、および UNIX/Linux 環境で有効です。

eTrust Access Control データベースまたはネイティブ OS データベースに新しいユーザを追加するか、いずれかのデータベースの既存のユーザを変更します。

join

eTrust、NT、および UNIX/Linux 環境で有効です。

ユーザをグループに追加します。

join-

eTrust、NT、および UNIX/Linux 環境で有効です。

ユーザをグループから削除します。

newusr

eTrust、NT、および UNIX/Linux 環境で有効です。

eTrust Access Control データベースまたはネイティブ OS データベースに新しいユーザを追加します。

rename

eTrust および NT 環境で有効です。

データベースのオブジェクト名を変更します。eTrust Access Control では、名前が 255 文字を超えるリソースを管理できません。そのため、オブジェクト名の最大文字数は 255 文字です。この制限は、ネイティブ環境にも適用されます。

rmusr

eTrust、NT、および UNIX/Linux 環境で有効です。

eTrust Access Control データベースまたはネイティブ OS データベースからユーザを削除します。

showusr

eTrust、NT、および UNIX/Linux 環境で有効です。

eTrust Access Control データベースまたはネイティブ OS データベースのユーザレコードのプロパティを一覧表示します。

xaudit

NT 環境で有効です。

監査基準を設定して、アクセス イベントの記録を開始します。

xaudit-

NT 環境で有効です。

監査基準を削除して、アクセス イベントの記録を停止します。

グループ コマンド

authorize

eTrust および NT 環境で有効です。

特定のリソースへのアクセス権限を特定のグループに設定します。

authorize-

eTrust および NT 環境で有効です。

特定のリソースへのアクセス権限を特定のグループから削除します。

chgrp

eTrust、NT、および UNIX/Linux 環境で有効です。

eTrust Access Control データベースまたはネイティブ OS データベースの既存のグループ設定を変更します。

editgrp

eTrust、NT、および UNIX/Linux 環境で有効です。

eTrust Access Control データベースまたはネイティブ OS データベースに新しいグループを追加するか、いずれかのデータベースの既存のグループを変更します。

join

eTrust、NT、および UNIX/Linux 環境で有効です。

ユーザをグループに追加します。

join-

eTrust、NT、および UNIX/Linux 環境で有効です。

ユーザをグループから削除します。

newgrp

eTrust、NT、および UNIX/Linux 環境で有効です。

eTrust Access Control データベースまたはネイティブ OS データベースに新しいグループを追加します。

rmgrp

eTrust、NT、および UNIX/Linux 環境で有効です。

eTrust Access Control データベースまたはネイティブ OS データベースからグループを削除します。

showgrp

eTrust、NT、および UNIX/Linux 環境で有効です。

eTrust Access Control データベースまたはネイティブ OS データベースのグループ レコードのプロパティを一覧表示します。

xaudit

NT 環境で有効です。

監査基準を設定して、アクセス イベントの記録を開始します。

xaudit-

NT 環境で有効です。

監査基準を削除して、アクセス イベントの記録を停止します。

リソース コマンド

authorize

eTrust および NT 環境で有効です。

特定のリソースへのアクセス権限を特定のアクセサに設定します。

authorize-

eTrust および NT 環境で有効です。

特定のリソースへのアクセス権限を特定のアクセサから削除します。

chfile

eTrust、NT、および UNIX/Linux 環境で有効です。

eTrust Access Control データベースまたはネイティブ OS データベースのファイル レコードの定義を変更します。

chres

eTrust、NT、および UNIX/Linux 環境で有効です。

eTrust Access Control データベースまたはネイティブ OS データベースの既存の リソース設定を変更します。

editfile

eTrust および NT 環境で有効です。

新しいファイル レコードを追加するか(eTrust 環境のみ)、既存のファイル レコードを変更します。

editres

eTrust、NT、および UNIX/Linux 環境で有効です。

eTrust Access Control データベースまたはネイティブ OS データベースに新しいリソース レコードを追加するか、いずれかのデータベースの既存のリソース レコードを変更します。

newfile

eTrust 環境で有効です。

データベースに新しいファイル レコードを追加します。

newres

eTrust、NT、および UNIX/Linux 環境で有効です。

eTrust Access Control データベースまたはネイティブ OS データベースに新しいリソース レコードを追加します。

rename

eTrust および NT 環境で有効です。

データベースのオブジェクト名を変更します。eTrust Access Control では、名前が 255 文字を超えるリソースを管理できません。そのため、オブジェクト名の最大文字数は 255 文字です。この制限は、ネイティブ環境にも適用されます。

rmfile

eTrust 環境で有効です。

eTrust Access Control データベースからファイル リソース レコードを削除します。

rmres

eTrust および NT 環境で有効です。

eTrust Access Control データベースまたは Windows データベースからリソースレコードを削除します。

showfile

eTrust、NT、および UNIX/Linux 環境で有効です。

eTrust Access Control データベースまたはネイティブ OS データベースのファイルレコードのプロパティを一覧表示します。

showres

eTrust、NT、および UNIX/Linux 環境で有効です。

eTrust Access Control データベースまたはネイティブ OS データベースのリソースレコードのプロパティを一覧表示します。

xaudit

NT 環境で有効です。

監査基準を設定して、アクセス イベントの記録を開始します。

xaudit-

NT 環境で有効です。

監査基準を削除して、アクセス イベントの記録を停止します。

高度なポリシー管理コマンド

deploy

特定のポリシーの RULESET オブジェクトに保存されている selang の展開コマンドを実行します。

deploy- | undeploy

特定のポリシーの RULESET オブジェクトに保存されている selang のポリシー展開解除コマンドを実行します。

get devcalc

ポリシーの偏差計算結果を取得します。

start devcalc

ポリシー偏差計算を開始します。

その他のコマンド

env

eTrust、NT、UNIX/Linux、および pmd リモート管理環境で有効です。

selang コマンドを実行するセキュリティ環境を設定します。

find

eTrust、NT、および UNIX/Linux 環境で有効です。

特定の環境に定義されているクラスを一覧表示します。1 つのクラスのレコードを一覧表示します。

help

eTrust、NT、UNIX/Linux、および pmd リモート管理環境で有効です。

ヘルプ画面を表示します。

history

eTrust、NT、UNIX/Linux、および pmd リモート管理環境で有効です。

セッションでこれまでに発行したコマンドを表示します。

hosts

eTrust、NT、UNIX/Linux、および pmd リモート管理環境で有効です。

selang のコマンドの送信先ホストを表示するか、これ以降に実行するすべてのコマンドの送信先ホストを示します。

list

eTrust、NT、および UNIX/Linux 環境で有効です。

1 つのクラスのレコードを一覧表示します。このコマンドは find コマンドと同じです。

ruler

eTrust 環境で有効です。

特定のコマンドを実行するたびに表示されるプロパティを設定します。

search

eTrust、NT、および UNIX/Linux 環境で有効です。

1 つのクラスのレコードを一覧表示します。このコマンドは find コマンドと同じです。

setoptions

eTrust 環境で有効です。

データベースの動作を制御するグローバル オプションを設定または表示します。

source

eTrust 環境で有効です。

特定のファイル内のコマンドを実行します。

第 2 章: eTrust 環境の selang のコマンド

このセクションには、以下のトピックが含まれます。

eTrust 環境での作業

この章では、eTrust 環境で使用できる selang のすべてのコマンド シェルをアルファベット順に示します。eTrust 環境では、selang のコマンドを使用し、ローカル Windows ホストに対して、ユーザやグループの追加、削除、変更、および一覧表示を行います。selang の他の環境についての一般情報、ヘルプの表示方法、コマンド構文、およびコマンドの全体的な構成については、「selang – eTrust AC のコマンド言語」の章を参照してください。

eTrust のコマンド リファレンス

このセクションでは、eTrust 環境で使用できるすべての selang のコマンドをアルファベット順に示します。

authorize

authorize は、特定のリソースへのアクセスを許可されているユーザおよびグループのリストを管理するコマンドです。authorize コマンドを使用すると、ユーザまたはグループのリストを以下のように変更できます。

- 特定の eTrust Access Control ユーザまたはグループのリソースへのアクセスを許可します。
- 特定の eTrust Access Control ユーザまたはグループのリソースへのアクセスをブロックします。
- 特定のユーザまたはグループのリソースへのアクセス権限レベルを変更します。

authorize- は、標準アクセス制御リストからアクセサを削除することによって、リソースへのアクセス権限を取り消すコマンドです。このコマンドを実行すると、特定のリソースに対するアクセサのアクセス権限はデフォルトのアクセス権限のみになります。

authorize コマンドおよび authorize- コマンドの形式は、クラスのセットによって異なります。クラスは以下のようなグループに分類されます。

- HOST、GHOST、HOSTNET、および HOSTNP
- TCP
- 残りのすべてのクラス

アクセス制御リストには、以下の 7 種類があります。

- ACL - 標準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限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 - 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依存します。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。
- INET-ACL - インターネット アクセス制御リスト
- 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 TNG カレンダに依存するリソース ACL です。
- AZNACL - 権限 ACL。リソースの説明に基づいてリソースへのアクセスを許可する ACL です。

以下の表に記載されていないクラスにはアクセス制御リストがないため、authorize コマンドでは制御できません。

クラス	ACL/NACL	CALACL	PACL	INET-ACL	CACL	AZNACL
ADMIN	X	X	X			
APPL	X	X				X
AUTHHOST	X	X				X
CONNECT	X	X	X			
CONTAINER	X	X	X			
DOMAIN	X	X	X			
FILE	X	X	X			
GAPPL	X	X				X
GAUTHHOST	X	X				X
GFILE	X	X	X			
GHOST				X		
GSUDO	X	X				
GTERMINAL	X	X				
HOLIDAY	X	X				
HOST				X		
HOSTNET				X		
HOSTNP				X		
LOGINAPPL	X	X				
MFTERMINAL	X	X	X			
PROCESS	X	X	X			
PROGRAM	X	X				
REGKEY	X	X	X			
SUDO	X	X	X			
SURROGATE	X	X	X			
TCP	X	X	X		X	
TERMINAL	X	X	X			
UACC	X	X				
USER_DIR	X					X

```
{authorize | auth} class-name record-name
                [uid({user-name...|*})]
                [gid(group-name...)]
                [access(access-value)]
                [via(pgm(program-names...))]
                                [calendar(calendar-name)]
                [nt]
        または
        {authorize- | auth-} class-name record-name {uid | gid}(name...) [nt]
        または
        {authorize | auth} class-name record-name
                [uid({user-name...|*})]
                [gid(group-name...)]
                [access(access-value) | deniedaccess(access-value)]
                [calendar(calendar-name)]
        または
        {authorize- | auth-} class-name record-name {uid | gid}(name...)
                [calendar(calendar-name)]
                [access-]
                [deniedaccess-]
        または
        {authorize | auth} class-name station-name
               service(service-name | service-number | service-number-range)
                [access(read|none)]
        または
        {authorize- | auth-} class-name station-name
               service(service-name | service-number | service-range)
        または
        {authorize | auth} TCP tcp-service-name
                [host(host-name...)]
                [ghost(ghost-name...)]
                [hostnp(hostnp-name...)]
                [hostnet(hostnet-name...)]
                [uid({user-name...|*})]
                [gid(group-name...)]
                [access(read | none | write)]
        または
        {authorize- | auth-} TCP tcp-service-name
                [host(host-name...)]
                [ghost(ghost-name...)]
                [hostnp(hostnp-name...)]
                [hostnet(hostnet-name...)]
                [uid({user-name...|*})]
                [gid(group-name...)]
        または
        {authorize | auth} WAC-class-name resource-name
                [user_attr(user-attribute)]
                [attr_va(attribute-val)]
                {user_dir(user-directory)}
```

{access(WAC-access)}
{response_yes(granted-response)}

class-name

record-name が所属するクラスの名前です。

注: *class-name* には、以下のいずれかの Windows リソースを指定できます。

- FILE
- PRINTER
- SHARE
- DISK
- COM
- REGKEY

record-name

アクセス制御リストを変更するリソース レコードの名前です。指定できるリソース レコードは 1 つのみです。

station-name

指定したクラスに属するレコードの名前です。

- HOST - 1 台の端末の名前
- GHOST - GHOST コマンドでデータベースに定義されたホスト グループの名前
- HOSTNET - IP アドレスのマスク値と一致値で定義されたホスト グループの名前
- HOSTNP - 名前パターンによって定義されたホスト グループの名前

解決できないホストについては、IP アドレスの範囲を入力します。

uid(*user-name*)

リソースへのアクセス権限を設定する対象の eTrust Access Control ユーザを示します。

user-name は、1 人または複数の eTrust Access Control ユーザのユーザ名です。複数のユーザを指定する場合は、各ユーザ名をスペースまたはカンマで区切ります。eTrust Access Control に定義されているすべてのユーザを指定する場合は、*user-name* にアスタリスク(*)を入力します。

gid(*group-name*)

リソースへのアクセス権限を設定する対象の 1 つまたは複数の eTrust Access Control グループを示します。

group-name は、1 つまたは複数の eTrust Access Control グループです。複数のグループを入力する場合は、名前をスペースまたはカンマで区切ります。

access(*access-value*)

uid パラメータまたは gid パラメータに指定したアクセサに対して設定する、リソースへのアクセス権限を示します。*via* パラメータを指定しない場合、アクセス権限はリソースの標準アクセス制御リスト内に設定されます。*via* パラメータを指定した場合、アクセス権限はリソースの条件付きアクセス制御リスト内に設定されます。

access-value パラメータはアクセス権限です。その値は、レコードが属するクラスによって異なります。

- ADMIN クラスの場合、有効な値は all、create、delete、join、modify、none、password、および read です。
- FILE クラスに対する有効な値は create、delete、execute、none、read、rename、sec、update、utime、および write です。
- HOLIDAY クラスの場合、有効な値は all、read、および none です。値 read が指定されている場合、指定した休日にログインすることをユーザに許可します。アクセス権限を指定しない場合、デフォルトは none になります。
- PROGRAM クラス、SUDO クラス、および GSUDO クラスの場合、有効な値は all、none、および execute になります。
- TCP クラスの場合、有効な値は all、none、read、および write です。値 read が指定されている場合、リモート ホストまたはホスト グループからのアクセスを許可します。値 write が指定されている場合、ユーザまたはグループが特定のホストまたはホスト グループにアクセスすることを許可します。
- TERMINAL クラスおよび GTERMINAL クラスに対する有効な値は、all、none、read、および write です。値 read が指定されている場合、ユーザまたはグループが端末にログインすることを許可します。値 write が指定されている場合、ユーザまたはグループが端末を管理することを許可します。
- その他すべてのクラスの場合、有効な値は all、none、および read です(値 *all* は、特定クラスの *none* 以外のアクセス値のグループ全体を表します)。
- access パラメータを省略すると、UACC クラスのリソース クラスを表すレコードの UACC プロパティに指定された暗黙的なアクセス権が割り当てられます。

deniedaccess(*access-value*)

uid パラメータまたは gid パラメータに指定したアクセサに対して設定する、リソースへのアクセス禁止を指定します。

拒否できる *accessvalue* は、all、create、delete、join、modify、none、password、および read です。

注: *accessValue* は authorize コマンドのみで使用できます。authorize- コマンドでは使用できません。

calendar(*calendar-name*)

Unicenter TNG で時刻制限を表す Unicenter TNG カレンダ オブジェクトを示します。eTrust Access Control では、これらのオブジェクトのリストは管理目的のみに使用され、オブジェクトは保護されません。

calendar-name は、CALENDAR クラスに定義された 1 つまたは複数の Unicenter TNG カレンダ レコードの名前です。複数のカレンダを割り当てる場合は、各カレンダ名をスペースまたはカンマで区切ります。

via_pgm(*program-names*)

条件付きアクセス ルールを設定します。指定したアクセス権は、指定されたプログラムまたはシェル スクリプトからリソースにアクセスした場合にのみ適用されます。シェル スクリプトの 1 行目は、#!¥bin¥sh とする必要があります。値 *program-names* に、PROGRAM クラスで定義されていないプログラムまたはシェル スクリプトを指定すると、そのプログラムまたはシェル スクリプトを保護する PROGRAM クラスのレコードが自動的に作成されます。

包括的な PACL は、PACL の拡張機能です。PACL のプログラム名でワイルドカード文字を指定すると、ワイルドカード文字によって作成されたマスクに一致するプログラムは、PACL で保護されているファイルにアクセスできます。プログラムが複数のマスクと一致する場合は、最大文字数のマスクが優先されます。

nt

Windows のシステム ACL に値を追加します。このパラメータは FILE クラスに対してのみ有効です。

ghost(*ghost-name*)

リソースへのアクセス権を設定する対象の eTrust Access Control ホスト グループを示します。

ghost-name は 1 つまたは複数の eTrust Access Control ホスト グループの名前です。複数のホスト グループを入力する場合は、名前をスペースまたはカンマで区切ります。

host(*host-name*)

リソースへのアクセス権を設定する対象の eTrust Access Control ホストを示します。

host-name は 1 つまたは複数の eTrust Access Control ホストの名前です。複数のホストを入力する場合は、名前をスペースまたはカンマで区切ります。

hostnet(*hostnet-name*)

リソースへのアクセス権限を設定する対象の eTrust Access Control hostnet オブジェクトを示します。

hostnet-name は 1 つまたは複数の eTrust Access Control hostnet オブジェクトの名前です。複数の hostnet オブジェクトを入力する場合は、名前をスペースまたはカンマで区切ります。

hostnp(*hostnp-name*)

リソースへのアクセス権限を設定する対象の eTrust Access Control hostnp オブジェクトを示します。

hostnp-name は、1 つまたは複数の eTrust Access Control hostnp オブジェクトの名前です。複数の hostnp オブジェクトを入力する場合は、名前をスペースまたはカンマで区切ります。

service(*service-name*/*service-number*/*service-number-range*/*service-range*)

station-name で指定された端末に提供されるローカル ホストのサービスを示します。

service-name はサービスの名前です。

service-number はサービス番号です。この番号は、符号なし短整数(0 ～ 65535)である必要があります。

service-number-range と *service-range* はサービス番号の範囲です。

TCP *tcp-service-name*

アクセス権限を設定する対象の eTrust Access Control TCP オブジェクトを示します。

tcp-service-name は TCP サービス レコードの名前です。

注:

- eTrust Access Control では、リソースに対するユーザのアクセス権限をチェックする際に、関連するすべてのリストが使用されます。

  注: アクセス権限チェックに使用されるリストの詳細については、「**管理者ガイド**」を参照してください。

- authorize コマンドでは一度に 1 つのリストのみを操作できます。複数のリストを変更する場合は、authorize コマンドを繰り返して発行する必要があります。
- 1 つの権限ルールで複数のユーザおよびグループに対する複数のアクセス権限を定義することはできません。その場合には、ルールを分割する必要があります。

例

ADMIN 属性を持つユーザ *admin* がユーザ Joe に、機密ファイル d:¥projects¥projectA¥secrets にアクセスする許可を与えるとします。

- ユーザ *admin* には ADMIN 属性が割り当てられています。
- eTrust Access Control にユーザ Joe が定義されています。
- FILE クラスのレコード *¥projects¥projectA¥secrets* がファイル d:¥projects¥projectA¥secrets を表しています。

```
authorize FILE d:¥projects¥projectA¥secrets uid(Joe) access(execute)
```

ユーザ「*admin*」が、RESEARCH グループのすべてのユーザからファイル d:¥products¥new への読み取りアクセス権限を削除するとします。

- ユーザ *admin* に ADMIN 属性が割り当てられています。
- グループ RESEARCH とファイル d:¥products¥new が Windows データベースに定義されています。

```
authorize- FILE d:¥products¥new gid(RESEARCH)
```

ユーザ「*admin*」が、ユーザ Joe から機密ファイル d:¥projects¥projectA¥secrets に対する execute アクセス権限を削除するとします。

- ユーザ *admin* に ADMIN 属性が割り当てられています。
- ユーザ Joe およびファイル d:¥projects¥projectA¥secrets が Windows データベースに定義されています。

```
authorize- FILE d:¥projects¥projectA¥secrets uid(Joe)
```

check

このコマンドによって、ユーザに特定のリソースへのアクセス権があるかどうかを確認できます。

注:

- このコマンドは、リソースの ACL およびデフォルトのアクセス プロパティに基づいてアクセス権をチェックします。ただし、このコマンドは PACL に対応していません。つまり、ユーザが特定のプログラムを使用してリソースにアクセスできるかどうかはチェックされません。PACL の詳細については、「**管理者ガイド**」の「概要」の章を参照してください。
- このコマンドは、seos の停止中には使用できません。
- このコマンドを使用する場合は、チェックするクラスがオブジェクトに対する大文字と小文字の区別をサポートするかどうかを考慮する必要があります。本書の第 5 章「seclassadm ユーティリティ」と「eTrust Access Control for UNIX and Linux **ユーティリティ ガイド**」の第 2 章を参照してください。

権限

check コマンドを使用するには、ADMIN 属性を持つ管理者である必要があります。SERVER 属性を持つプロセスもこのコマンドを使用できます。SERVER 属性の詳細については、「**管理者ガイド**」の「実装の計画」の章を参照してください。

```
check className {resourceName | (resourcenames…)} ¥
                        [uid (userName)] ¥
                        [access(authority)]
```

className

resourceName が属するクラスの名前です。

resourceName

リソース レコードの名前です。

access(*authority*)

uid パラメータで指定したアクセサに対し、eTrust Access Control でチェックするアクセス権限を示します。詳細については、*authorize* コマンドを参照してください。

uid(*userName*)

resourceName へのアクセス権限を確認する対象の eTrust Access Control ユーザの名前を示します。複数の *userName* を指定する場合は、各ユーザ名をスペースまたはカンマで区切ります。eTrust Access Control に定義されているすべてのユーザを指定する場合は、 *userName* にアスタリスク(*)を指定します。

例

ユーザ Administrator に FILE クラスのリソースに対するアクセス権限があるかどうかを確認するには、以下の check コマンドを実行します。出力結果は以下のようになります。

```
eTrust selang v8.0 - eTrust command line interpreter

Copyright 2004 Computer Associates International, Inc.

eTrustAC> check FILE c:¥temp¥testfile.txt uid(Administrator) access(w)

(localhost)

Access to FILE c:¥temp¥testfile.txt GRANTED

Access to FILE c:¥temp¥testfile.txt DENIED

Stage:Resource OWNER check

eTrustAC>
```

checklogin

checklogin は、ユーザのログイン権限、パスワード チェックが必要かどうか、および端末へのアクセス権のチェックが必要かどうかを調べるコマンドです。

注: このコマンドは、seos の停止中には使用できません。

権限

checklogin コマンドを使用するには、ADMIN 属性を持つ管理者である必要があります。SERVER 属性を持つプロセスもこのコマンドを使用できます。SERVER 属性の詳細については、「**管理者ガイド**」の「実装の計画」の章を参照してください。

checklogin *userName* [password(*userPassword*)] [terminal(*loginTerminalName*)]

Password(*userPassword*)

パスワード チェックが有効な場合に、eTrust Access Control でオペレーティング システムのパスワードおよびデータベースと照合してチェックするパスワードを示します。

Terminal(*loginTerminalName*)

このパラメータを指定すると、この端末からログインする権限がユーザにあるかどうかがチェックされます。

userName

1 人または複数の eTrust Access Control ユーザのユーザ名です。複数のユーザを入力する場合は、各ユーザ名をスペースまたはカンマで区切ります。eTrust Access Control に定義されているすべてのユーザを指定する場合は、*userName* にアスタリスク(*)を指定します。

例

- ユーザ Frank に端末のリモート ホストからローカル ホストにログインする権限があるかどうかを確認するには、以下の checklogin コマンドを実行します。

  checklogin frank terminal(remotehost)(localhost)

  出力結果は以下のようになります。

  Login by USER frank to host localhost is GRANTED

- ユーザ Frank のパスワードを検証するには、以下の checklogin コマンドを実行します。

  checklogin frank password(111) (localhost)

  出力結果は以下のようになります。

  Given password does not match OS password

  ここで、以下のコマンドを実行します。

```
checklogin frank password(moonshine) (localhost)
```

出力結果は以下のようになります。

```
WARNING:Access Control password check is disabled
Login by USER frank to host localhost is GRANTED
Stage:Resource class global universal access
```

次に、ユーザ Frank のパスワードをデータベースのパスワードと照合して検証するには、以下のコマンドを実行します。

```
so class+(PASSWORD) (localhost)
```

出力結果は以下のようになります。

```
Successfully updated Access Control options
```

ここで、以下のコマンドを実行します。

```
checklogin frank password(moonshine) terminal(tack) (localhost)
```

出力結果は以下のようになります。

```
Login by USER frank to host localhost is GRANTED
Stage:Resource class global universal access
```

checkpwd

このコマンドを使用すると、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ことを確認できます。このチェックを行っても、パスワードは変更されません。

注: このコマンドは、seos の停止中には使用できません。

新しいパスワードのチェックに適用されるパスワード ルールには、以下のようなものがあります。

- 新しいパスワードは、以前に使用したものと一致するものは指定できません。
- 新しいパスワード内にはユーザ名を含めることができません。
- 新しいパスワードには、英数字を最低文字数以上使用する必要があります。
- 新しいパスワード内には、以前のパスワードやその一部として使用されていたものを含めることはできません。
- 新しいパスワードには禁止文字を使用できません。

権限

checkpwd コマンドを使用するには、ADMIN 属性を持つ管理者である必要があります。

checkpwd userName password(newPassword)

userName

新しいパスワードをチェックする eTrust Access Control ユーザの名前を示します。

password(*newPassword*)

チェックするパスワードを示します。

例

新しいパスワードを受け入れるかどうかは、eTrust Access Control パスワード ルールに従って判断されます。

- 新しいパスワードが受け入れられた場合、成功したことを示す以下のメッセージが表示されます。

  Changing *userName*'s password is permitted.

  例:

  Changing *JDoe*'s password is permitted.

- 新しいパスワードが拒否された場合、失敗したことを示す以下のメッセージが表示されます。

  Changing *userName*'s password is denied.
  denied_reason

  denied_reason は、実際にパスワードのチェックが失敗したときに適用されたパスワード ルールです。
  例：

  Changing *JDoe*'s password is denied.
  Too few lowercase letters in password.

注: *denied_reason* には、パスワードのチェックが失敗したときに適用された最初のルールのみが表示されます。たとえば、パスワードが短すぎ、さらにパスワードに含まれる大文字の数が少なすぎる場合、「Password is too short」というメッセージが表示されます。

chfile/editfile/newfile

chfile は FILE クラスの 1 つまたは複数のレコードを変更し、newfile は FILE クラスの 1 つまたは複数のレコードを作成するコマンドです。editfile は FILE クラスの 1 つまたは複数のレコードを作成または変更するコマンドです。

注: まだ存在しないファイルについてもデータベースにレコードを作成できます。存在しないファイルのレコードを作成すると、次のような selang のメッセージが返されます。INFO:*file-name* is not found on the file system.

```
{chfile   | cf} file-name | (file-names...)

または
{editfile | ef} file-name | (file-names...)
または
{newfile | nf} file-name | {file-names…}
                [audit(none | all | success | failure)]
                                    [calendar(calendar-name)]
                [category(category-names...) | category-(category-names...)]
                [comment('installation defined data') | comment-]
                [defaccess(global-access-value)]
                [gen_prop(property-name) [ {gen_flag | gen_op}(flag)]
gen_val(property-values ...)]
                [gowner(group-name)]
                [label(seclabel-name) | label-]
                [level(seclevel-num) | level-]
                [notify(notify-address) | notify-]
                [owner(user-name or group-name)]
                [restrictions(days( day-data ) time(hhmm:hhmm | anytime) ) | restrictions-]
                day-data:{[mon] [tue] [wed] [thu] [fri] [sat] [sun]} | anyday | weekdays
                [warning | warning-]
```

audit[(none|all|success|failure)]

ログに記録するアクセス イベントを示します。chfile コマンドで audit パラメータを使用するには AUDITOR 属性が必要です。

- none - ログ ファイルにはレコードが一切記録されません。
- all - 許可されたアクセスと検出された許可されないアクセス試行の両方がログに記録されます。
- success - リソースへの許可されたアクセスが記録されます。
- failure - 検出された許可されないアクセス試行がログに記録されます。これがデフォルト値です。

calendar(*calendar-name*)

Unicenter TNG で時刻制限を表す Unicenter TNG カレンダ オブジェクトを示します。eTrust Access Control では、これらのオブジェクトのリストは管理目的のみに使用され、オブジェクトは保護されません。

calendarName は、CALENDAR クラスに定義された 1 つまたは複数の Unicenter TNG カレンダ レコードの名前です。複数のカレンダを割り当てる場合は、各カレンダ名をスペースまたはカンマで区切ります。

calendar-(*calendar-name*)

ユーザ レコードから 1 つまたは複数の Unicenter TNG カレンダ レコードを削除します。このパラメータは chusr コマンドまたは editusr コマンドにのみ使用できます。

category(*category-name*)

レコードにセキュリティ カテゴリを割り当てます。

category-name は、CATEGORY クラスに定義された 1 つまたは複数のセキュリティ カテゴリ レコードの名前です。複数の名前を入力する場合は、名前をスペースまたはカンマで区切ります。

category-(*category-name*)

リソース レコードから 1 つまたは複数のセキュリティ カテゴリを削除します。指定したセキュリティ カテゴリは、CATEGORY クラスがアクティブかどうかに関係なく、リソース レコードから削除されます。

このパラメータは chres コマンドまたは editres コマンドにのみ使用できます。

comment('*installation defined data*)

レコードにコメント文字列を追加します。レコードにすでにコメント文字列が追加されている場合、既存の文字列はここで指定した新しい文字列に置き換えられます。

installation defined data は、最大 255 文字の英数字から成る文字列です。文字列に空白が含まれている場合は、文字列全体を一重引用符で囲みます。

comment-

リソース レコードからコメント文字列を削除します。このパラメータは chres コマンドまたは editres コマンドにのみ使用できます。

defaccess(*global-access-value*)

ファイルに対するデフォルトのアクセス権限を示します。デフォルトのアクセス権限とは、ファイルのアクセス制御リストに含まれていないアクセサがファイルへのアクセス要求を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。

global-access-value には、all、chmod、chown、control、create、delete、none、read、rename、sec、update、utime、または write のいずれかの値を指定します。アクセス権限の詳細については、「**管理者ガイド**」を参照してください。

file-name

chfile コマンドの場合、*file-name* は変更するファイル レコードの名前です。1 つ以上のファイル名を指定する**必要があります**。

newfile コマンドの場合、*file-name* は FILE クラスに追加するファイルの名前です。

包括的なファイル名を使用して FILE クラスにレコードを追加する場合、またはレコードを変更する場合は、selang で許可されているワイルドカード表現を使用します。詳細については、「ユーティリティ」の章を参照してください。複数のレコードを定義または変更する場合は、ファイル名のリストを丸かっこで囲み、各ファイル名をスペースまたはカンマで区切ります。

editfile コマンドの場合、レコードがすでに存在するかどうかによって、ファイル名を newfile コマンドまたは chfile コマンドのルールに準拠させる必要があります。

gen_prop(*property-name*)

Active Directory プロパティを示します。

gen_flag | gen_op(*flag*)

gen_val(*property-values*)

Active Directory プロパティに関連付けられた値を示します。

gowner(*group-name*)

レコードの所有者として eTrust Access Control グループ (*group-name*) を割り当てます。ファイル レコードのグループ所有者には、ファイル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、グループ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、ファイル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。ファイルのグループ所有者は、ファイル レコードを常時更新および削除することができます。詳細については、「**管理者ガイド**」を参照してください。

label(*sec/abe/-name*)

レコードにセキュリティ ラベルを割り当てます(*sec/abe/-name* は SECLABEL クラスに定義されているセキュリティ ラベルのレコード名です)。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。リソース レコードに現在セキュリティ ラベルが含まれている場合、現在のセキュリティ ラベルは、ここで指定したセキュリティ ラベルに置き換えられます。セキュリティ ラベルのチェックの実装方法については、「**管理者ガイド**」を参照してください。

label-(*sec/abe/-name*)

ファイル レコードに定義されているセキュリティ ラベルを削除します(*sec/abe/-name* は SECLABEL クラスに定義されているセキュリティ ラベルのレコード名です)。このパラメータは chfile コマンドまたは editfile コマンドにのみ使用できます。

level(*sec/eve/-num*)

リソース レコードにセキュリティ レベルを割り当てます。level には 1 から 255 までの正の整数を指定する必要があります。すでにリソース レコードにセキュリティ レベルが割り当てられている場合は、既存の値が新しい値に置き換えられます。詳細については、「**管理者ガイド**」を参照してください。

level-(*sec/eve/-num*)

eTrust Access Control によるリソースのセキュリティ レベルのチェックを停止します。このパラメータは chfile コマンドまたは editfile コマンドにのみ使用できます。

notify(*notify-address*)

リソース レコードが示すファイルへのアクセスが成功するたびに、*notify-address* で指定されているユーザに通知メッセージを送信するように eTrust Access Control に指示します。

通知は、ログ ルーティング システムがアクティブな場合にのみ行われます。通知メッセージは、ログ ルーティング システムの設定に基づいて、ユーザの画面またはメールボックスに送信されます。

通知メッセージが送信されるたびに、監査ログに監査レコードが書き込まれます。監査レコードのフィルタ処理および表示の詳細については、このマニュアルの「ユーティリティ」の章を参照してください。

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許可されないアクセス試行に対処する必要があります。

notify-address には、ユーザ名、ユーザの電子メール アドレスを指定できます。また、別名が指定されている場合、メール グループの電子メール アドレスも指定できます。

制限: 30 文字。

notify-(*notify-address*)

レコードが示すファイルへのアクセスが許可される際に、誰にも通知を行わないことを示します。このパラメータは chfile コマンドまたは editfile コマンドにのみ使用できます。

owner ({*user-name*|*group-name*})

ファイル レコードの所有者として eTrust Access Control のユーザ(*user-name*)またはグループ(*group-name*)を割り当てます。ファイル レコードの所有者には、ファイル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、ファイル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。ファイルの所有者は、ファイル レコードをいつでも更新または削除することができます。詳細については、「**管理者ガイド**」を参照してください。

restrictions(days (*day-data*) time(*time*))

ユーザがファイルにアクセスできる曜日と時間帯を示します。

days 引数を指定せずに time 引数を指定した場合、レコード内にすでに設定されている曜日制限に対して、指定した時刻制限が適用されます。time 引数を指定せずに days 引数を指定した場合、レコード内にすでに設定されている時刻制限に対して、指定した曜日制限が適用されます。days 引数と time 引数の両方を指定した場合、ユーザは、指定した曜日の指定した時間帯にのみシステムにアクセスできます。

- (*day-data*) は、ユーザがファイルにアクセスできる曜日を示します。days 引数には以下のサブ引数があります。
  - anyday - ユーザはすべての曜日にファイルにアクセスできます。
  - weekdays - ユーザは月曜から金曜までの平日に限りリソースにアクセスできます。
  - Mon、Tue、Wed、Thu、Fri、Sat、Sun - ユーザは指定した曜日にのみリソースにアクセスできます。曜日は任意の順で指定できます。複数の曜日を指定する場合は、各曜日をスペースまたはカンマで区切ります。
- (*time*) は、ユーザがリソースにアクセスできる時間帯を示します。time 引数には以下のサブ引数があります。
  - anytime - ユーザは任意の時間帯にリソースにアクセスできます。
  - startTime:endTime - 指定した時間帯に限りリソースにアクセスできます。startTime と endTime は両方とも、*hhmm* という形式で指定します。*hh* は 24 時間表記の時間(00 ～ 23)、*mm* は分(00 ～ 59)を表します。2400 は有効な time 値ではありません。startTime が endTime より小さく、両方が同じ日の時刻であることが必要です。端末がホストと異なるタイムゾーンにある場合は、端末の開始時間と終了時間をホストのローカル時間に相当する時間に変換し、時間の値を調整してください。たとえば、ホストがニューヨークにあり、端末がロサンゼルスにある場合、端末へのアクセスをロサンゼルス時間の午前 8 時から午後 5 時まで許可するには、「time (1100:2000)」と指定します。

restrictions-(days (*day-data*) time(*time*))

ファイルに対するユーザのアクセス権限を限定するすべての制限を削除します。

warning

ファイルにアクセスできるだけの十分な権限がアクセサにない場合に、ファイルへのアクセスを拒否するのではなく、監査ログに警告メッセージを書き込むよう eTrust Access Control に指示します。

warning-

実行した warning コマンドを終了します。ファイルにアクセスできるだけの十分な権限がアクセサにない場合、警告メッセージは書き込まれず、ユーザはファイルへのアクセスを拒否されます。このパラメータは chfile コマンドまたは editfile コマンドにのみ使用できます。

包括的なファイル保護

包括的なファイル保護により、正規表現で指定したファイル名のパターンに一致するすべてのファイルに対し、特定のアクセス ルールを適用できます。包括的なアクセス ルールとは、名前がワイルドカードを使用したパターンに一致するすべてのファイル リソースを保護するルールです。リソースが複数の包括的なアクセス ルールに一致する場合は、リソースに最も厳密に一致するルールが eTrust Access Control によって選択されます。

包括的なファイル保護を使用すると、ほんのわずかなセキュリティ ルールを定義するだけで、Windows システム内で保護を必要とするほとんどのファイルを保護できます。

ただし、以下のパターンは***使用できません***。

- ¥*
- ¥tmp¥*

¥etc¥*

注: 複数のファイル名を指定した場合は、指定したパラメータに基づいて各ファイル レコードが個別に処理されます。ファイルの処理中にエラーが発生すると、メッセージが表示され、リストの次のファイルから処理が続行されます。

関連項目

この章の authorize コマンド、rmfile コマンド、および showfile コマンドの説明。

例

ADMIN 属性を持つセキュリティ管理者が、Administrators グループのメンバを除くすべてのユーザに対して読み取りアクセス権限のみを与えることで、d:¥winnt¥win.ini ファイルへのアクセスを制限するとします。現在、レコードの ACL にはエントリがありません。

- セキュリティ管理者に ADMIN 属性が割り当てられています。
- ファイル d:¥winnt¥win.ini がデータベースに定義されています。
- 現在、レコードの ACL にはエントリがありません。

```
chfile d:¥winnt¥win.ini defaccess(read) owner(Administrators)
```

chgrp/editgrp/newgrp

chgrp は、eTrust Access Control グループの定義を変更するコマンドです。グループが Windows に対しても定義されている場合は、chgrp コマンドを使用して Windows でのグループの定義を変更できます。chgrp コマンドは一度に複数のグループの定義を変更できます。

editgrp は、newgrp コマンドと同様にデータベースに新しいグループを追加したり、chgrp コマンドと同様に既存の eTrust Access Control グループの定義を変更するコマンドです。

newgrp は、新しいグループのレコードをデータベースに追加することによって、eTrust Access Control に新しいグループを定義するコマンドです。必要に応じて、新しいグループと指定した親の管理者グループまたはメンバ グループとの関係を設定します。

```
{chgrp   | cg} group-name | (group-names ...)
または
{editgrp | eg} group-name | (group-names ...)
または
{newgrp | ng} group-name | (group-names…)
          [audit(none | all | success | failure | loginsuccess | loginfail  | trace) | audit-]
          [comment('installation defined data') | comment- ]
          [expire | expire(mm/dd/yy[yy][@hh:mm]) | expire-]
          [gen_prop(property-name) [ {gen_flag | gen_op}(flag)]
gen_val(property-values ...)]
          [gowner(group-name)]
          [grace(number-of-grace-logins) | grace-]
          [homedir(full-path)]
          [inactive(num-inactive-days) | inactive-]
          [interval(maximum-password-change-interval) | interval-]
          [maxlogins(maximum-number-of-logins) | maxlogins-]
          [mem(group-name) | mem+(group-name) | mem-(group-name)]
          [min_life(minimum-password-change-interval) | min_life-]
          [name('full-name')]
          [owner(user-name or group-name)]
          [parent(group-name) | parent-]
          [password (
[history(numberStoredPasswords) | history-]
[interval(maximumPasswordChangeInterval) | interval-]
[min_life(minimumPasswordChangeInterval) | min_life-]
[rules(
[alpha(minimumAlphaCharacters)]
[alphanum(minimumAlphanumericCharacters)]
[bidirectional | bidirectional-]
[grace(numberOfGraceLogins)]
[min_len(minimumPasswordLength)]
[max_len(maximumPasswordLength)]
[lowercase(minimumLowercaseCharacters)]
[max_rep(maxRepetitiveCharacters)]
```

```
[namechk | namechk-]
[numeric(minimumNumericCharacters)]
[oldpwchk | oldpwchk-]
[special(minimumSpecialCharacters)]
[uppercase(minimumUppercaseCharacters)]
[use_dbdict | use_dbdict-]
        )]
[rules-]
                [pmdb(PolicyModel-name) | pmdb-]
                [restrictions(days( day-data ) time(hhmm:hhmm | anytime) ) |
restrictions-]
                day-data:{[mon] [tue] [wed] [thu] [fri] [sat] [sun]} | anyday | weekdays
                [resume | resume(mm/dd/yy[yy][@hh:mm]) | resume-]
                [shellprog(full-path)]
                [suspend | suspend(mm/dd/yy[yy][@hh:mm]) | suspend-]
                [nt| nt( nt-group-attributes )]
                nt-group-attributes :
                [comment('installation defined data')]
```

注: いくつかのパラメータは、グループがユーザのプロファイル グループとして機能する場合にのみ有効です。これらのパラメータを以下に示します。

audit(*mode*)

このコマンドのトレース監査を有効にします。*mode* には none、all、success、failure、loginsuccess、loginfail、trace、audit- のいずれかを指定します。

audit-

このコマンドのトレース監査を無効にします。

comment('*installation defined data*')

グループ レコードに最大 255 文字の英数字から成るコメント文字列を追加します。文字列に空白が含まれている場合は、文字列全体を一重引用符で囲みます。以前に追加した既存の文字列は、この文字列に置き換えられます。

comment-

グループ レコードからコメント文字列(ある場合)を削除します。このパラメータは chgrp コマンドまたは editgrp コマンドにのみ使用できます。

expire(*date*)

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。この日付を指定しない場合、ユーザが現在ログインしていなければ、ユーザ アカウントはただちに失効します。ユーザがログインしている場合は、ユーザがログアウトした時点で失効します。このパラメータは、プロファイル グループにのみ適用されます。

有効期限の日付と時刻は、以下の形式で指定します。時刻は省略可能です。
*mm/dd/yy [yy][@HH:MM]*年は、下 2 桁または 4 桁のどちらでも指定できます。

注: 失効したユーザ レコードは、resume パラメータに再開日を指定しても有効にできません。失効したユーザ レコードを有効にするには、expire- パラメータを使用します。

expire-

newgrp コマンドの場合は、有効期限のないユーザ アカウントを定義します。chgrp コマンドおよび editgrp コマンドの場合は、ユーザ アカウントから有効期限を削除します。このパラメータは、プロファイル グループにのみ適用されます。

gen_prop(*property-name*)

Active Directory プロパティを示します。

gen_flag|gen_op(*flag*)

gen_val(*property-values*)

Active Directory プロパティに関連付ける値を示します。

gowner(*group-name*)

グループ レコードの所有者として、eTrust Access Control のユーザまたはグループを割り当てます。複数のグループ名を指定する場合は、グループ名を丸かっこで囲み、各グループ名をスペースまたはカンマで区切ります。このパラメータを省略した場合、データベースにグループを追加したユーザがグループ レコードの所有者になります。

grace(*number-of-grace-logins*)

ユーザのアカウントが一時停止になるまでにログインできる最大回数を設定します。猶予ログイン回数には、0 から 255 までの数値を指定する必要があります。猶予ログイン回数に達すると、ユーザは、システムへのアクセスを拒否されます。システム管理者に連絡して、新しいパスワードを選択できるようにする必要があります。grace を 0 に設定すると、ユーザはログインできなくなります。このパラメータはプロファイル グループにのみ適用されます。

group-name

プロパティを追加、変更、または編集するグループの名前を示します。newgrp コマンドの場合、データベースに存在しない一意のグループ名を指定する必要があります。ただし、グループとユーザは同じ名前を共有できます。

grace-

グループの猶予ログイン設定を削除します。このパラメータは chgrp コマンドまたは editgrp コマンドにのみ使用できます。このパラメータは、プロファイル グループにのみ適用されます。

history

保存するパスワードの数を示します。history- を使用して履歴ファイルを削除できます。

homedir(*full-path*)

ユーザのホーム ディレクトリの完全パスを指定します。指定する homedir の末尾をスラッシュにすると、指定したパスに *user-name* が自動的に追加されます。

inactive(num-inactive-days)

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示します。経過日数に達すると、ユーザはログインできなくなります。このパラメータはプロファイル グループにのみ適用されます。

正の整数または 0 を入力します。inactive を 0 に設定した場合は、inactive- パラメータを使用した場合と同じ結果になります。

注: ユーザ レコードには、アクティブでないユーザにはマークは付けられません。アクティブでないユーザを識別するには、Inactive Days 値と Last Accessed Time 値を比較する必要があります。

inactive-

ユーザのステータスを非アクティブからアクティブに変更します。このパラメータは chgrp コマンドまたは editgrp コマンドにのみ使用できます。このパラメータは、プロファイル グループにのみ適用されます。

interval(*maximum-password-change-interval*)

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。正の整数または 0 を入力します。interval に 0 を設定すると、グループに対するパスワード期間のチェックが無効になり、パスワードが失効しません。setoptions コマンドで設定したデフォルト値は使用されません。セキュリティ要件が厳しくないユーザに対してのみ interval を 0 に設定してください。

指定した日数が経過すると、eTrust Access Control は、現在のパスワードが期限切れになったことをユーザに通知します。通知を受けたユーザは、ただちにパスワードを更新するか、猶予ログイン回数に達するまで古いパスワードを引き続き使用することができます。猶予ログイン回数に達すると、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設定する必要があります。このパラメータは、プロファイル グループにのみ適用されます。

interval-

グループに対するパスワード期間の設定を取り消します。この設定を取り消すと、ユーザ レコードの任意の値が使用されます。それ以外の場合は、setoptions コマンドで設定したデフォルト値が使用されます。このパラメータは chgrp コマンドまたは editgrp コマンドにのみ入力できます。このパラメータは、プロファイル グループにのみ適用されます。

maxlogins(*maximum-number-of-logins*)

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、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。このパラメータを指定しない場合は、ユーザ レコードの任意の値が使用されます。それ以外の場合は、グローバルに設定されているログインの最大数が使用されます。このパラメータは、プロファイル グループにのみ適用されます。

注: maxlogins を 1 に設定すると、selang を実行できません。この場合、eTrust Access Control をシャットダウンし、maxlogins 設定を 2 以上の値に変更して、eTrust Access Control を再起動する必要があります。

maxlogins-

グループの最大ログイン数の設定を削除します。このパラメータを指定しない場合は、ユーザ レコードの任意の値が使用されます。それ以外の場合は、グローバルに設定されているログインの最大数が使用されます。このパラメータは chgrp コマンドまたは editgrp コマンドにのみ使用できます。このパラメータは、プロファイル グループにのみ適用されます。

mem(*group-name*) | mem+(*group-name*)

eTrust Access Control のグループにメンバ グループ(または子グループ)を追加します。メンバ グループ (*group-name*)は、あらかじめ eTrust Access Control に定義しておく必要があります。複数のメンバ グループを追加する場合は、各グループ名をカンマで区切ります。グループ名にスペースが含まれている場合は、一重引用符で囲みます。

mem-(*group-name*)

指定のグループからメンバ グループを削除します。メンバ グループ (*group-name*)は、あらかじめ eTrust Access Control に定義しておく必要があります。複数のメンバ グループを削除する場合は、各グループ名をカンマで区切ります。グループ名にスペースが含まれている場合は、一重引用符で囲みます。

min_life(*minimum-password-change-interval*)

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です。このパラメータは、プロファイル グループにのみ適用されます。

min_life-

グループの min_life 設定を削除します。min_life パラメータがユーザ レコードに設定されている場合、min_life- パラメータを指定しないと、ユーザ レコードの値が使用されます。それ以外の場合は、グローバルに設定されている min_life が使用されます。このパラメータは chgrp コマンドまたは editgrp コマンドにのみ使用できます。このパラメータは、プロファイル グループにのみ適用されます。

name('*full-name*')

グループのフル ネームを示します。最大 256 文字の英数字から成る文字列を入力します。文字列に空白が含まれている場合は、文字列を一重引用符で囲みます。

owner(*user-name*|*group-name*)

グループ レコードの所有者として、eTrust Access Control のユーザまたはグループを割り当てます。このパラメータを省略した場合、データベースにグループを追加したユーザが所有者になります。詳細については、「**管理者ガイド**」を参照してください。

parent(*group-name*)

グループ レコードの親グループとして既存の eTrust Access Control グループを割り当てます。グループの親子関係の詳細については、「**管理者ガイド**」を参照してください。

parent-

グループとその親グループの間のリンクを削除します。このパラメータは chgrp コマンドまたは editgrp コマンドにのみ使用できます。

password

指定されたグループにパスワードを割り当てます。

rules

以下のようなパスワードのルールを指定します。

alpha(*minimumAlphaCharacters*)

英字の文字数の最小値です。

alphanum(*minimumAlphanumericCharacters*)

英数字の文字数の最小値です。

bidirectional | bidirectional-

双方向パスワード暗号化の無効化/有効化を切り替えます。双方向パスワード暗号化が有効になっている場合、新しいパスワードはすべて暗号化され、クリア テキストに復号化できるようになります。この暗号化によって、新しいパスワードと古いパスワード(パスワード履歴)を広範囲にわたって比較できます。双方向暗号化を無効にすると、一方向のパスワード履歴暗号化が有効になり、古いパスワードを復号化できなくなります。

注(UNIX/Linux の場合): この機能を使用するには、トークンのパスワード形式を NT に設定する必要があります。

min_len(*minimumPasswordLength*)

パスワードの長さの最小値です。

max_len(*maximumPasswordLength*)

パスワードの長さの最大値です。

lowercase(minimumLowercaseCharacters)

小文字の数の最小値です。

max_rep(*maximumRepetitiveCharacters*)

文字を繰り返し使用できる回数の最大値です。

namechk | namechk-

パスワードと名前を照合します。

numeric(*minimumNumericCharacters*)

数字の数の最小値です。

oldpwchk | oldpwchk-

新しいパスワードと古いパスワードを照合します。

special(*minimumSpecialCharacters*)

特殊文字の文字数の最小値です。

uppercase(*minimumUppercaseCharacters*)

大文字の数の最小値です。

use_dbdict | use_dbdict-

パスワード辞書を設定します。use_dbdict は、トークンを db に設定し、eTrust Access Control データベース内の単語とパスワードを比較します。use_dbdict- は、トークンを file に設定し、UNIX/Linux の場合は seos.ini ファイルで指定されたファイルとパスワードを照合し、Windows の場合は Windows レジストリで指定されたファイルとパスワードを照合します。

password-

このグループのパスワードの入力を不要にします。

pmdb(*PolicyModel-name*)

グループ内のユーザが 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、指定した Policy Model に新しいパスワードを伝達するように指定します。PMDB の完全修飾名を入力します。

パスワードは、seos.ini の[seos]セクションで parent_pmd トークンまたは passwd_pmd トークンに定義されている Policy Model には送信されません。このパラメータは、プロファイル グループにのみ適用されます。

pmdb-

- グループ レコードから pmdb 属性を削除します。このパラメータは chgrp コマンドまたは editgrp コマンドにのみ使用できます。このパラメータは、プロファイル グループにのみ適用されます。

restrictions(days(*day-data*) time(*time-data*))

グループのメンバがシステムにログインできる時間帯を示します。ユーザのログイン中にログインの有効期限が切れた場合でも、ユーザがシステムから強制的にログオフされることはありません。また、ログイン制限は、バッチ ジョブに適用されません。したがって、ユーザはいつでもバックグラウンド プロセスを実行できます。このパラメータは、プロファイル グループにのみ適用されます。

days 引数を指定せずに time 引数を指定した場合、グループ レコード内にすでに設定されている曜日制限に対して、指定した時刻制限が適用されます。time 引数を指定せずに days 引数を指定した場合、グループ レコード内にすでに設定されている時刻に対して、指定した曜日制限が適用されます。days 引数と time 引数の両方を指定した場合、グループのメンバは、指定した曜日の指定した時間帯にのみシステムへのログインを許可されます。

- days(day-data) - ユーザがシステムにログインできる曜日を指定します。days 引数には以下のサブ引数があります。
  - anyday - ユーザは任意の曜日にログインできます。
  - weekdays - ユーザは月曜日から金曜日までの平日にかぎりログインできます。
  - mon tue wed thu fri sat sun - ユーザは指定した曜日にのみログインできます。曜日は任意の順で指定できます。複数の曜日を指定する場合は、各曜日をスペースまたはカンマで区切ります。
  - time(time-data) - ユーザがシステムにログインできる時間帯を指定します。time 引数には以下のサブ引数があります。
  - anytime- - ユーザは特定の曜日の任意の時間帯にログインできます。

- startTime:endTime - ユーザは指定した時間帯のみにログインできます。*startTime* と *endTime* は両方とも、*hhmm* という形式で指定します。*hh* は 24 時間表記の時間(00 ～ 23)、*mm* は分(00 ～ 59)を表します。2400 は有効な time 値ではありません。*endTime* の値が *startTime* の値より小さい場合、その時間帯の終了時間は翌日の時刻とみなされます。それ以外の場合、指定した時間帯は同じ日の時刻であるとみなされます。

  端末がホストと異なるタイム ゾーンにある場合は、端末の開始時間と終了時間をホストのローカル時間に相当する時間に変換し、時間の値を調整してください。たとえば、ホストがニューヨークにあり、端末がロサンゼルスにある場合、ロサンゼルスの端末からのアクセスを午前 8 時から午後 5 時まで許可するには、「time(1100:2000)」と指定します。

restrictions-

システムにログインするユーザの権限を限定するすべての曜日および時間帯の制限をグループ レコードから削除します。restrictions パラメータがユーザ レコードに設定されている場合、restrictions- パラメータを指定しないと、ユーザ レコードの値が使用されます。このパラメータは chgrp コマンドまたは editgrp コマンドにのみ使用できます。このパラメータは、プロファイル グループにのみ適用されます。

resume(*date*)

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。日付と時刻は、次の形式で指定します。時刻は省略可能です。*mm/dd/yy[@HH:MM]*

suspend パラメータと resume パラメータの両方を指定する場合は、必ず再開日を一時停止日より後に設定する必要があります。そうしないと、ユーザが無期限に一時停止することになります。*date* を省略した場合、chgrp コマンドの実行直後にユーザ レコードが再開されます。詳細については、「**管理者ガイド**」を参照してください。このパラメータは、プロファイル グループにのみ適用されます。

resume-

再開日および再開時間(指定されている場合)をグループ レコードから消去します。これにより、ユーザのステータスがアクティブ(有効)から一時停止に変更されます。このパラメータは chgrp コマンドまたは editgrp コマンドにのみ使用できます。このパラメータは、プロファイル グループにのみ適用されます。

shellprog(*full-path*)

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。*full-path* は文字列です。

supgroup(*Group'sSuperiorGroup*)

スーパーグループ(親グループ)を示します。

suspend(*date*)

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。日付と時刻は、次の形式で指定します。時刻は省略可能です。*mm/dd/yy[@HH:MM]*

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。*date* を指定した場合、指定した日にユーザ レコードが一時停止されます。*date* を省略した場合、chgrp コマンドの実行直後にユーザ レコードが一時停止されます。このパラメータは、プロファイル グループにのみ適用されます。

suspend-

一時停止日をユーザ レコードから消去し、ユーザのステータスを無効からアクティブ(有効)に変更します。このパラメータは chgrp コマンドまたは editgrp コマンドにのみ使用できます。このパラメータは、プロファイル グループにのみ適用されます。

nt(*nt-group-attributes*)

chusr コマンドおよび editusr コマンドでこのパラメータを使用する場合、ローカル Windows システムのユーザ定義を変更します。newusr コマンドでこのパラメータを使用する場合、ユーザをローカル Windows システムに追加します。複数の引数を指定する場合は、各引数をスペースで区切ります。

eTrust Access Control 内でローカル Windows システムを操作する方法については、この章の environment コマンドの説明と「Windows 環境の selang のコマンド」の章を参照してください。

comment('*installation defined data*)

レコードにコメント文字列を追加します。レコードにすでにコメント文字列が追加されている場合、既存の文字列はここで指定した新しい文字列に置き換えられます。

installation defined data は、 最大 255 文字の英数字から成る文字列です。文字列に空白が含まれている場合は、文字列全体を一重引用符で囲みます。

unix(*groupidNumber*)

UNIX/Linux のグループ属性を設定します。

- chgrp コマンドで使用する場合、ローカル UNIX/Linux システムのグループ属性を変更します。
- editgrp コマンドで使用する場合、レコードがすでに存在していればグループ属性が変更され、存在していなければグループが追加されます。このパラメータは、プロファイル グループにのみ適用されます。
- newgrp コマンドで使用する場合、グループをローカル UNIX/Linux システムおよびデータベースに追加します。デフォルトの属性を使用してグループを UNIX/Linux に追加するには、unix パラメータを引数なしで指定します。UNIX/Linux の属性を明示的に設定するには、該当する引数を指定します。

groupidNumber は 10 進数です。グループ ID に 0 を指定することはできません。この数値を省略した場合、その時点で最大のグループ ID が検出され、その ID 番号に 1 を加えた値がそのグループの ID として設定されます。一度に複数のグループを追加または変更する場合も、同様の方法でグループ ID の番号が生成されます。seos.ini ファイルのトークン AllowedGidRange を使用して、特定の番号を利用できないようにすることができます。

その他のパラメータの詳細については、「**管理者ガイド**」を参照してください。

userlist(*userName*)

グループにメンバを割り当てます。*userName* は、1 人または複数の UNIX/Linux ユーザのユーザ名です。複数のユーザを割り当てる場合は、各ユーザ名をスペースまたはカンマで区切ります。chgrp コマンドまたは editgrp コマンドで使用する場合、グループにすでに定義されているメンバ リストはすべて、ここで指定したメンバ リストに置き換えられます。

関連項目

この章の rmgrp コマンド、showgrp コマンド、および join コマンドの説明。

例

- ADMIN 属性を持つユーザ Sally が、グループ NewEmployee のレコードに格納されているグループ プロファイルに対して、ホーム ディレクトリとシェル プログラムの指定を削除する操作を実行するとします。

  - ユーザ Sally が NewEmployee のグループ レコードの所有者です。

  ```
  editgrp NewEmployee homedir() shellprog()
  ```

  レコード プロパティが文字列で定義されている場合、プロパティを削除するには、「-」記号または空のかっこ「()」のいずれかを付けてプロパティを入力します。

- ユーザ Bob が、Sales グループの親グループおよび Sales グループを所有するグループを、ACCOUNTS から PAYROLL に変更するとします。

  - ユーザ Bob に ADMIN 属性が割り当てられています。

  ```
  chgrp Sales parent(PAYROLL) owner(PAYROLL)
  ```

- ユーザ admin1 がグループ projectB の親グループを divisionA から divisionB に変更し、新しい所有者としてグループ RESEARCH を指定するとします。

  - ユーザ admin1 に ADMIN 属性が割り当てられています。

  ```
  chgrp projectB parent(divisionB) owner(RESEARCH)
  ```

- ユーザ Admin1 が、グループ ProjectA をグループ RESEARCH の子グループとして追加するとします。ユーザ Admin1 がグループ ProjectA の所有者になります。

  - ユーザ Admin1 に ADMIN 属性が割り当てられています。
  - owner(Admin1)

```
newgrp ProjectA parent(RESEARCH)
```

chres / editres / newres

newres は、eTrust Access Control クラスに新しいリソースを定義するコマンドです。chres は、eTrust Access Control クラスに属する 1 つまたは複数のリソース レコードを変更するコマンドです。editres は、新しいリソースを定義することも、既存のリソースを変更することもできるコマンドです。

eTrust Access Control for Windows では、chres コマンド、editres コマンド、および newres コマンドを使用して、ADMIN、AGENT、AGENT_TYPE、APPL、AUTHHOST、CALENDAR、CATEGORY、CONNECT、CONTAINER、DOMAIN、FILE、GAPPL、GAUTHHOST、GFILE、GHOST、GSUDO、GTERMINAL、HNODE、HOLIDAY、HOST、HOSTNET、HOSTNP、MFTERMINAL、OU、POLICY、PROCESS、PROGRAM、PWPOLICY、REGKEY、RESOURCE-DESC、RESPONSE-TAB、RULESET、SECFILE、SECLABEL、SPECIALPGM、SUDO、SURROGATE、TCP、TERMINAL、UACC、USER-ATTR、USER-DIR クラス、および任意のユーザ定義クラスを管理できます。

注: chres コマンドまたは editres コマンドでは、ユーザまたはグループを変更できません。

各クラスに適用される newres パラメータおよび chres パラメータを以下の表に示します。

クラス	プロパティ											
	audit	calendar	category	comment	defaccess	label	level	notify	owner	restrictions [-]	warning	other
ADMIN	X	X	X	X	X	X	X	X	X	X	X	
AGENT				X					X			
AGENT-TYPE				X					X			
APPL	X	X		X				X	X		X	DAYTIME、HOST
AUTHHOST	X	X	X	X		X	X		X		X	
CALENDAR				X					X			
CATEGORY				X					X			
CONNECT	X	X	X	X	X	X	X	X	X	X	X	
CONTAINER	X	X		X					X		X	MEM

クラス	プロパティ											
	audit	calendar	category	comment	defaccess	label	level	notify	owner	restrictions [-]	warning	other
DOMAIN	X	X	X	X	X	X	X	X	X	X	X	MEM
FILE	X	X	X	X	X	X	X	X	X	X	X	
GAPPL	X			X					X			MEM
GAUTHHOST	X			X					X			MEM
GFILE	X	X		X				X	X		X	MEM
GHOST	X	X		X					X	X	X	MEM
GSUDO		X		X	X				X			MEM
GTERMINAL	X	X		X	X				X	X		MEM
HOLIDAY	X		X	X	X	X	X	X	X	X	X	DATES
HNODE	X	X	X	X	X	X	X	X	X	X	X	SUBSCRIBER [-]、POLICY[-]
HOST	X	X		X					X	X	X	
HOSTNET	X	X		X					X		X	MASK、MATCH
HOSTNP	X	X		X					X	X	X	
MFTERMINAL	X	X	X	X		X	X	X	X		X	DAYTIME
POLICY	X	X	X	X	X	X	X	X	X	X	X	SIGNATURE、RULESET{+¥-}
PROCESS	X	X	X	X	X	X	X	X	X	X	X	
PROGRAM	X	X	X	X	X	X	X	X	X	X	X	TRUST[-]
PWPOLICY				X					X			
REGKEY	X	X		X	X			X	X		X	DAYTIME
RESOURCE-DESC				X					X			
RESPONSE-TAB				X					X			

クラス	プロパティ											
	audit	calendar	category	comment	defaccess	label	level	notify	owner	restrictions [-]	warning	other
RULESET	X	X	X	X	X	X	X	X	X	X	X	SIGNATURE、CMD{+|-}、UNDOCMD{+|-
SECFILE				X					X			TRUST[-]
SECLABEL			X	X			X		X			
SEOS		X	X	X		X	X					
SPECIALPGM				X					X			
SUDO	X	X	X	X	X	X	X	X	X	X	X	
SURROGATE	X	X	X	X	X	X	X	X	X	X	X	
TCP	X		X	X	X	X	X	X	X	X	X	
TERMINAL	X	X	X	X	X	X	X	X	X	X	X	
UACC	X		X	X	X				X			
USER-ATTR									X		X	
USER-DIR	X			X					X			

```
{chres   | cr} class-name resource-name | (resource-names...)
または
{editres | er} class-name resource-name | (resource-names...)
または
{newres | nr} class-name resource-name | (resource-names…)
        [audit(none | all | success | failure)]
        [caption(caption-name) | caption-]
        [category(category-names...) | category-(category-names...)]
        [comment('installation defined data') | comment-]
        [container | container-]
        [dates(mm/dd/[yy[yy]][@hh:mm][-mm/dd/[yy[yy]][@hh:mm]]...) |
        dates-(mm/dd/[yy[yy]][@hh:mm][-mm/dd/[yy[yy]][@hh:mm]]...)]
        [defaccess(global-access-value)]
        [disable| disable-]
        [flags(flags)]
        flags:{[Ctime] [Mtime] [Mode] [Size] [Device] [Inode] [Crc] [Owner] [Group]} | All
| None
        [gacc(access-value)]
        [gen_prop(property-name) [ {gen_flag | gen_op}(flag)]
gen_val(property-values ...)]
        [gowner(group-name)]
        [hidden | hidden-]
        [host(host-name) | host-]
        [iconfile(iconfile-name) | iconfile-]
        [iconid(iconid-number)]
        [item(application-name ...) | item-(application-name ...)]
        [label(seclabel-name) | label-]
        [level(seclevel-num) | level-]
        [login_type( none | otp | pwd | ticket )]
        [mask(inet-address) match(inet-address)]
        [master(application-name) | master-]
        [mem+(member-names ...) | mem-(member-names...) ]
        [notify(notify-address) | notify-]
        [owner(user-name or group-name)]
        [password | password-]
        [postcmd(command-name | ; command-names...) | postcmd-]
        [precmd(command-name | ; command-names...) | precmd-]
        [pwd_autogen | pwd_autogen-]
        [pwd_sync | pwd_sync-]
        [pwpolicy(policy-name)]
        [restrictions(days( day-data ) time(hhmm:hhmm | anytime) ) | restrictions-]
        day-data:{[mon] [tue] [wed] [thu] [fri] [sat] [sun]} | anyday | weekdays
        [script(script-name) | script-]
        [sensitive | sensitive-]
        [targuid(user-name)]
        [trust | trust-]
        [uacc(access-value)]
        [warning | warning-]
        [agent_type]
```

[of_resource]
[resaccess]
[resp_list | resp_list+ | resp_list-]
[db_field]
[field_id]
[predef | predef- | predef+]
[user_dir]
[addcategory]
[auth_method]
[base_path]
[cont_format]
[properties]
[user_format]

class-name

リソースが属するクラスの名前です。eTrust Access Control に定義されているリソース クラスを一覧表示するには、find コマンドを実行します。詳細については、この章の find コマンドの説明を参照してください。

resource-name

変更または追加するリソース レコードの名前です。複数のリソースを変更または追加する場合は、リソース名のリストを丸かっこで囲み、各リソース名をスペースまたはカンマで区切ります。少なくとも 1 つのリソース名を指定する必要があります。

eTrust Access Control では、指定したパラメータに従って、各リソース レコードが個別に処理されます。リソースの処理中にエラーが発生すると、メッセージが表示され、リストの次のリソースから処理が続行されます。

audit (*mode*)

ログに記録するアクセス イベントを示します。以下のいずれかの属性を指定します。

- none - ログ ファイルには一切レコードが記録されません。
- all - 許可されたアクセス試行と許可されないアクセス試行の両方がログに記録されます。
- failure - 許可されないアクセス試行がログに記録されます。これがデフォルト値です。
- success - 許可されたアクセス試行がログに記録されます。

caption(*caption-name*)

ユーザのデスクトップのアプリケーション アイコンの下に表示されるテキストです。

calendar(*calendarName*)

Unicenter TNG で時刻制限を表すカレンダ オブジェクトを示します。eTrust Access Control では、これらのオブジェクトのリストは管理目的のみに使用され、オブジェクトは保護されません。複数のカレンダを割り当てる場合は、各カレンダ名をスペースまたはカンマで区切ります。

calendar-(*calendarName*)

リソース レコードから 1 つまたは複数の Unicenter TNG カレンダ レコードを削除します。このパラメータは chres コマンドまたは editres コマンドにのみ使用できます。

category(category-name)

CATEGORY クラスに定義された 1 つまたは複数のセキュリティ カテゴリ レコードをリソースに割り当てます。複数のセキュリティ カテゴリを割り当てる場合は、各セキュリティ カテゴリ名をスペースまたはカンマで区切ります。

CATEGORY クラスがアクティブでない場合に category パラメータを指定すると、eTrust Access Control では、データベース内のリソースの定義が更新されます。ただし、更新されたカテゴリの割り当ては、CATEGORY クラスが再度アクティブになるまでは有効になりません。セキュリティ カテゴリのチェックの詳細については、「**管理者ガイド**」を参照してください。

category-(*category-names*)

リソース レコードから 1 つまたは複数のセキュリティ カテゴリを削除します。複数のセキュリティ カテゴリを削除する場合は、各セキュリティ カテゴリ名をスペースまたはカンマで区切ります。

指定したセキュリティ カテゴリは、CATEGORY クラスがアクティブかどうかに関係なく、リソース レコードから削除されます。このパラメータは chres コマンドまたは editres コマンドにのみ使用できます。

cmd+(*selang_command_string*)

ポリシーを定義する selang のコマンドのリストを示します。これらのコマンドがポリシーの展開に使用されます。

cmd-

RULESET オブジェクトからポリシー展開コマンドを削除します。

comment('*installation defined data*')

最大 255 文字の英数字から成る文字列をリソース レコードに追加します。文字列に空白が含まれる場合は、文字列全体を一重引用符で囲みます。以前に定義した既存の文字列は、この文字列に置き換えられます。

注: SUDO クラスには、comment プロパティは *data* プロパティと呼ばれ、この文字列は特別な意味を持ちます。SUDO レコードの定義については、「**管理者ガイド**」を参照してください。

comment-

リソース レコードからコメント文字列を削除します。このパラメータは chres コマンドまたは editres コマンドにのみ使用できます。

container(*containerName*)

CONTAINER オブジェクト(包括的なグループ化クラス)を表します。詳細については、「eTrust 環境のクラスとプロパティ」の章の CONTAINER クラスの説明を参照してください。

containerName は、CONTAINER クラスに定義された 1 つまたは複数の CONTAINER クラスのレコードの名前です。複数の CONTAINER クラスのレコードを割り当てる場合は、名前をスペースまたはカンマで区切ります。

container-(*containerName*)

リソース レコードから 1 つまたは複数の CONTAINER クラスのレコードを削除します。このパラメータは chres コマンドまたは editres コマンドにのみ使用できます。

dates(*time-period*)

休日などユーザがログインできない期間を 1 つまたは複数指定します。複数の期間を指定する場合は、各期間をスペースで区切ります。以下の形式を使用します。

mm/dd[/yy[yy]][@hh:mm][-mm/dd]/[/yy[yy]][@hh:mm]

特定の年を指定しない場合、または 1990 年より前の年を指定した場合、期間または休日は毎年適用されるとみなされます。年は、03 または 2003 のように、2 桁または 4 桁で指定できます。

開始時間を指定しない場合、その日の開始時間(午前 0 時)が使用されます。終了時間を指定しない場合、その日の終了時間(午前 0 時)が使用されます。時間および分の形式は *hh:mm* で指定します。*hh* は 24 時間表記の時間(00 から 23)、*mm* は分(00 から 59)を表します。

期間(たとえば、12/25@14:00-12/25@17:00)を指定しないで月と日のみ(12/25)を指定すると、その日 1 日が休日とみなされます。

休日を迎えるタイム ゾーンとは異なるタイム ゾーンでコマンドを発行する場合は、指定する期間をユーザのローカル時間に変換します。たとえば、ロサンゼルスで半日の休日があり、ニューヨークからコマンドを発行する場合、「09/14/03@18:00-09/14/03@20:00」と入力する必要があります。このように指定すると、ロサンゼルスにいるユーザは午後 3 時から午後 5 時までの間ログインできなくなります。

defaccess(*global-access-value*)

リソースに対するデフォルトのアクセス権限を示します。デフォルトのアクセス権限とは、リソースのアクセス制御リストに含まれていないアクセサがリソースへのアクセス要求を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。アクセス権限の値は、リソースが属するクラスによって異なります。

- ADMIN クラスの場合、有効な値は *all*、*create*、*delete*、*join*、*modify*、*none*、*password*、および *read* です。
- FILE クラスの場合、有効な値は *all*、*chdir*、*chmod*、*chown*、*control*、*create*、*delete*、*execute*、*none*、*read*、*rename*、*sec*、*update*、*utime*、および *write* です。
- HOLIDAY クラスの場合、有効な値は *all*、*read*、および *none* です。値 *read* が指定されている場合、指定した休日にログインすることをユーザに許可します。アクセス権限を指定しない場合、デフォルトは *none* になります。
- PROGRAM クラス、SUDO クラス、および GSUDO クラスの場合、有効な値は *all*、*none*、および *execute* になります。
- TCP クラスの場合、有効な値は *all*、*none*、*read*、および *write* です。値 *read* が指定されている場合、リモート ホストまたはホスト グループからのアクセスを許可します。値 *write* が指定されている場合、ユーザまたはグループが特定のホストまたはホスト グループにアクセスすることを許可します。
- TERMINAL クラスおよび GTERMINAL クラスの場合、有効な値は *all*、*none*、*read*、および *write* です。値 *read* が指定されている場合、ユーザまたはグループが端末にログインすることを許可します。値 *write* が指定されている場合、ユーザまたはグループが端末を管理することを許可します。
- その他すべてのクラスの場合、有効な値は *all*、*none*、および *read* です。(値 *all* は、特定クラスの *none* 以外のアクセス値のグループ全体を表します)。

access パラメータを省略すると、eTrust Access Control では UACC クラスのリソース クラスを表すレコードの UACC プロパティに指定された暗黙的なアクセス権限が割り当てられます。

アクセス権限の詳細については、「**管理者ガイド**」を参照してください。

disable

アプリケーションを無効化状態にします。

注: アプリケーションが無効化された状態である場合、ユーザは eTrust Web Access Control を使用してアプリケーションにログインできません。

disable-

無効化フラグを削除します。

flags(*flags*)

リソースを trusted にする方法およびリソースのステータスが trusted であるかどうかをチェックする方法を示します。有効なフラグは、Ctime、Mtime、Mode、Size、Device、Inode、Crc、Owner、Group、SHA1、および All/None です。

gacc(access-value)

gen_prop(property-name)

Active Directory プロパティを示します。

gen_flag|gen_op(*flag*)

gen_val(*property-values*)

Active Directory プロパティに関連付ける値を示します。

gowner(group-name)

リソース レコードの所有者として eTrust Access Control グループを割り当てます。リソース レコードのグループ所有者には、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、グループ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。リソースのグループ所有者には、リソースレコードを更新および削除する許可が常に与えられます。詳細については、「**管理者ガイド**」を参照してください。

hidden

アプリケーションを起動できるユーザに対しても、デスクトップにアプリケーションを表示しないことを示します。

注: 他のアプリケーションにパスワードを提供することを唯一の目的とするマスタアプリケーションを非表示にすることができます。

hidden-

非表示フラグを削除します。

host(*host-name*)

リソースへのアクセス権限を設定する対象の eTrust Access Control ホストを示します。詳細については、このマニュアルの「eTrust 環境のクラスとプロパティ」の章の HOST クラスの説明を参照してください。

host-name は 1 つまたは複数の eTrust Access Control ホストの名前です。複数のホストを入力する場合は、名前をスペースまたはカンマで区切ります。

host-

ホスト フラグを削除します。

iconfile (*iconfile-name*)

ユーザのデスクトップに表示するアプリケーションのアイコンが保存されているファイルのファイル名または完全パスです。ファイル名のみを入力した場合は、以下の順序でファイルが検索されます。

1. カレント ディレクトリ
2. Windows システム ディレクトリ
3. Windows ディレクトリ
4. 環境変数 PATH に示されているディレクトリ。

iconfile-

アイコン ファイルを削除します。

iconid(*iconid-number*)

アイコン ファイル内のアイコンの(必要に応じた)ID 番号です。ICONID を指定しないと、デフォルト アイコンが使用されます。

item(*application-names*)

GAPPL クラスの場合 - グループに属するアプリケーション リストを追加します。

item-(*application-names*)

GAPPL クラスから、そのクラスに属するアプリケーションを削除します。

label(*seclabel-name*)

SECLABEL クラスに定義されているセキュリティ ラベル レコードを割り当てます。

label-

リソース レコードからセキュリティ ラベルを削除します。このパラメータは chres コマンドまたは editres コマンドにのみ使用できます。

level(*seclevel-num*)

リソース レコードにセキュリティ レベルを割り当てます。1 から 255 までの正の整数を入力します。リソース レコードにすでにセキュリティ レベルが割り当てられている場合、既存の値は新しい値に置き換えられます。セキュリティ レベルのチェックの実装方法については、「**管理者ガイド**」を参照してください。

level-

eTrust Access Control によるリソースのセキュリティ レベルのチェックを停止します。このパラメータは chres コマンドまたは editres コマンドにのみ使用できます。

login_type(*type*)

ログイン タイプを none、otp、pwd、または ticket に設定します。

mask(*inet-address*) match(*inet-address*)

mask パラメータおよび *match* パラメータは HOSTNET クラスにのみ適用できます。newres コマンドおよび editres コマンドを使用してクラスにレコードを追加する場合、これらのパラメータが必要です。chres コマンドを使用する場合は省略可能です。

HOSTNET レコードに属するホストを定義するには、*mask* と *match* を一緒に使用します。*mask* とホストの IP アドレスでビット単位の AND が実行された結果が *match* と等しい場合、そのホストは HOSTNET レコードのメンバです。

たとえば、mask(255.255.255.0) および match(192.16.133.0) を指定すると、192.16.133. の後に任意の数字が続く IP アドレスを持つすべてのホストが対象になります。

master(*application-name*)

パスワードを提供するアプリケーションのレコード名です。

master-

指定されたアプリケーションからマスタ アプリケーションを削除します。

mem+(member-names)

リソース グループにメンバを追加します。追加するメンバ リソースは、eTrust Access Control で事前に定義して保護しておく必要があります。複数のメンバを追加する場合は、各リソース名をカンマで区切ります。

mem パラメータは、CONTAINER クラス、GFILE クラス、GSUDO クラス、GTERMINAL クラス、または GHOST クラスのリソース レコードにのみ適用されます。

- CONTAINER クラスは、他のリソース クラスに属するオブジェクトのグループを定義します。
- GFILE クラスには、名前パターンに基づいてアクセス権限を定義するファイルのグループが含まれています。
- GSUDO クラスには、コマンドのグループを定義するリソース レコードが含まれています。
- GTERMINAL クラスには、端末のグループを定義するリソース レコードが含まれています。
- GHOST クラスには、ホストのグループを定義するリソース レコードが含まれています。

mem は、追加または変更する CONTAINER オブジェクト、GFILE レコード、GSUDO レコード、GTERMINAL リソース レコード、GHOST リソース レコードに、それぞれ、さまざまな種類のレコード、FILE リソース レコード、SUDO リソース レコード、TERMINAL リソース レコード、HOST リソース レコードを追加するためのパラメータです。

注: CONTAINER リソースに対し mem パラメータを使用する場合、of_class パラメータも併用する必要があります。

mem-(*member-names*)

リソース グループからメンバ リソースを削除します。複数のメンバ リソースを削除する場合は、各リソース名をスペースまたはカンマで区切ります。このパラメータは chres コマンドまたは editres コマンドにのみ使用できます。

notify(*notify-address*)

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 eTrust Access Control 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。

通知は、ログ ルーティング システムがアクティブな場合にのみ行われます。通知メッセージは、ログ ルーティング システムの設定に基づいて、ユーザの画面またはメールボックスに送信されます。

通知メッセージが送信されるたびに、監査ログに監査レコードが書き込まれます。監査レコードのフィルタ処理および表示の詳細については、「**管理者ガイド**」を参照してください。

通知メッセージの受信者は、頻繁にログインして、各メッセージに示された許可されないアクセス試行に対処する必要があります。

制限: 30 文字。

notify-

リソース レコードが示すリソースへのアクセスが成功した場合、誰にも通知を行わないことを示します。このパラメータは chres コマンドまたは editres コマンドにのみ使用できます。

of_class(*className*)

mem パラメータを使用して CONTAINER クラスに追加するレコードのリソース タイプを示します。

owner(*user-name*|*group-name*)

リソース レコードの所有者として、eTrust Access Control のユーザまたはグループを割り当てます。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許可が常に与えられます。詳細については、「**管理者ガイド**」を参照してください。

password

(UNIX/Linux のみ)。SUDO クラスに使用する場合、sesudo コマンドの実行時に元のユーザのパスワードが必要であることを示します。

password-

（UNIX/Linux のみ）。password パラメータを取り消し、元のユーザのパスワードを指定しなくても sesudo コマンドを実行できるようにします。このパラメータは chres コマンドまたは editres コマンドにのみ使用できます。これまでに password パラメータが使用されていない場合、このパラメータは必要ありません。

policy(name(*<name>*) status(*<status>*) updated_by(*<name>*)) |
policy(name(*<name>*) deviation{+|-})

伝達ツリーにノードのサブスクライバを追加し、そのステータスを示します。あるいは、既存のポリシーを更新し、ポリシーの偏差が存在するかどうかを示します。updated_by プロパティは、ポリシー ステータスの更新時に更新する必要があります。これはポリシー ステータスを変更したユーザの名前を表す文字列です。

ポリシー ステータスには、Transfer、Deployed、Undeployed、Failed、SigFailed、Queued、UndeployFailed、Transfer Failures があります。

policy-[(name(*name#xx*))]

ノードから指定のポリシーを削除します。ポリシーを指定しないと、このノードに展開されているすべてのポリシーが削除されます。

postcmd(*command-names*)

ログオン スクリプトの後に実行されるコマンドです。

postcmd-

postcmd コマンドを削除します。

precmd(*command-names*)

ログオン スクリプトの前に実行されるコマンドです。

precmd-

precmd コマンドを削除します。

pwd_autogen

アプリケーションの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示します。

pwd_autogen-

pwd_autogen フラグを削除します。

pwd_sync

アプリケーションのパスワードをユーザの他のアプリケーション パスワードと同一にできるかどうかを示します。

pwd_sync-

pwd_sync フラグを削除します。

pwpolicy(policy-name)

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です。

restrictions(days(*day-data*) time(*time-data*))

ユーザがファイルにアクセスできる曜日と時間帯を示します。

days 引数を指定せずに time 引数を指定した場合、レコード内にすでに設定されている曜日制限に対して、指定した時刻制限が適用されます。time 引数を指定せずに days 引数を指定した場合、レコード内にすでに設定されている時刻制限に対して、指定した曜日制限が適用されます。days 引数と time 引数の両方を指定した場合、ユーザは、指定した曜日の指定した時間帯にのみシステムにアクセスできます。

- (*day-data*) は、ユーザがファイルにアクセスできる曜日を示します。days 引数には以下のサブ引数があります。
  - anyday - ユーザはすべての曜日にファイルにアクセスできます。
  - weekdays - ユーザは月曜から金曜までの平日に限りリソースにアクセスできます。
  - Mon、Tue、Wed、Thu、Fri、Sat、Sun - ユーザは指定した曜日にのみリソースにアクセスできます。曜日は任意の順で指定できます。複数の曜日を指定する場合は、各曜日をスペースまたはカンマで区切ります。
- (*time-data*) には、ユーザがリソースにアクセスできる時間帯を示します。time 引数には以下のサブ引数があります。
  - anytime - ユーザは任意の時間帯にリソースにアクセスできます。
  - startTime:endTime - 指定した時間帯に限りリソースにアクセスできます。startTime と endTime の両方とも *hhmm* の形式で指定します。*hh* は 24 時間表記の時間（00 から 23）、*mm* は分（00 から 59）を表します。2400 は有効な time 値ではないことに注意してください。startTime が endTime より小さいこと、および両方が同じ日の時刻であることが必要です。端末がホストと異なるタイム ゾーンにある場合は、端末の開始時間と終了時間をホストのローカル時間に相当する時間に変換し、時間の値を調整してください。たとえば、ホストがニューヨークにあり、端末がロサンゼルスにある場合、端末へのアクセスをロサンゼルス時間の午前 8 時から午後 5 時まで許可するには、「time (1100:2000)」と指定します。

restrictions-(days(*day-data*) time(*time-data*))

ファイルに対するユーザのアクセス権限を限定するすべての曜日および時間帯の制限を削除します。

ruleset+(*<name>*)

ポリシーに関連付けるルール セットを示します。

ruleset+(*<name>*)

ポリシーからルール セットを削除します。ルール セットを指定しないと、ポリシーからすべてのルール セットが削除されます。

script(*script-name*)

ユーザがログインしたときに自動的に実行されるファイルの場所を示します。このログイン スクリプトによって作業環境が設定されます。ユーザの作業環境は profile パラメータでも設定されるため、このパラメータの指定は省略可能です。

script-

アプリケーションから script 値を削除します。

sensitive

事前設定された時間が経過した後にユーザがアプリケーションを再度開いた場合に、ユーザの再認証が必要かどうかを示します。

sensitive-

アプリケーションから sensitive フラグを削除します。

signature(*hash_value*)

ハッシュ値を示します。ポリシーに対しては、これはポリシーに関連付けられた RULESET オブジェクトのシグネチャに基づきます。ルール セットに対しては、これはポリシー展開コマンド リストとポリシー削除(展開解除)コマンド リストに基づきます。

subscriber(name(*<sub_name>*) status(*<status>*))

伝達ツリーにノードのサブスクライバを追加し、そのステータスを示します。ステータスには、unknown、available、unavailable、sync があります。

subscriber-(name(*sub_name*)) | sub-

ノードからサブスクライバ データベースを削除します。サブスクライバを指定しないと、すべてのサブスクライバが削除されます。

targuid(*user-name*)

(UNIX/Linux のみ)。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示します。デフォルトでは root ユーザです。

trust

プログラムを trusted プログラムとしてマークを付けます。

trust-

trusted プログラムとしてのフラグを削除します。

uacc(*access-value*)

リソースに対するデフォルトのアクセス権です。eTrust Access Control に定義されていないアクセサ、またはリソースの ACL に登録されていないアクセサに与えるアクセス権を示します。

warning

リソースにアクセスできる権限がアクセサにない場合でも、eTrust Access Control がリソースにアクセスできることを示します。ただし、監査ログに警告メッセージが書き込まれます。

注: 警告モードの場合、eTrust Access Control では、リソース グループに対する警告メッセージは作成されません。

warning-

警告付きのアクセス権を削除します。リソースにアクセスできるだけの十分な権限がアクセサにない場合、ユーザはリソースへのアクセスを拒否されます。警告メッセージは書き込まれません。このパラメータは chres コマンドまたは editres コマンドにのみ使用できます。

agent_type

エージェントのタイプを示します。

of_resource

RESPONSE_TABLE が属するリソース クラスの名前です。

resaccess

RESPONSE_TAB オブジェクトのアクセスです。

resp_list

resaccess に対する応答を示します。

resp_list+

resaccess に対する応答を追加します。

resp_list-

resaccess から応答を削除します。

db_field

userdir データベースに登録されているフィールドの名前です。異なるデータベースには異なる属性を指定できるため、属性フィールドは同期させる必要があります。

field_id

内部でのみ使用されます。ポリシー サーバで管理されるマッピング テーブルの USER_DIR オブジェクト属性の内部番号です。

predef

特定のユーザ属性に対して許可される値のリストを追加します。

predef-

特定のユーザ属性に対して許可される値のリストを削除します。

predef+

特定のユーザ属性に対して許可される値のリストを追加します。

user_dir

USER_ATTR が参照するユーザのディレクトリの名前です。

addcategory

カテゴリを追加します。

auth_method

AUTHHOST オブジェクトの方法 ID です。

base_path

USER_DIR オブジェクトの基本パスです。

cont_format

ポリシー サーバで、認証プロセスの際に入力されたコンテナの相対識別名を操作し、ユーザ データ ストアのコンテナ名に合わせる際に使用されるフォーマット文字列です。

properties

表示する 1 つまたは複数の eTrust Access Control のプロパティの名前を示します。複数のプロパティを指定する場合は、プロパティ名のリストを丸かっこで囲み、各プロパティ名をスペースまたはカンマで区切ります。

user_format

ポリシー サーバで、認証プロセスの際に入力されたユーザ名を操作し、ユーザ データ ストアのユーザ名に合わせる際に使用するフォーマット文字列です。&user_name& フィールドと &user_dir& フィールドにこの値が存在する場合、ポリシー サーバによってそれぞれユーザ名と USER_DIR 名に変更されます。

関連項目

authorize コマンド、rmres コマンド、および showres コマンドの説明。

例

- SHARE レコード shar22 の所有者であるユーザ Bob が、SHARE レコード shar22 のコメント フィールドを削除し、一度に shar22 に接続できるユーザの最大数を 12 に設定するとします。
  - ユーザ Bob は eTrust Access Control ユーザであり、SHARE レコード shar22 の所有者です。

```
chres SHARE shar22 comment- maxusers(12)
```

- ADMIN 属性を持つユーザ *admin1* が、Windows データベースに定義されている NTFS ファイル d:¥tmp¥a.exe の所有者およびデフォルトのアクセス権を変更するとします。
  - ユーザ *admin1* に ADMIN 属性が割り当てられています。
  - ファイル d:¥tmp¥a.exe が Windows データベースに定義されています。

```
editres file d:¥tmp¥a.exe owner(admin1) defaccess(read)
```

- *ADMIN 属性を持つユーザ admin1* が、Software¥Mineval という新しい REGVAL リソース タイプを追加し、それにレジストリ値 4 を設定するとします。その結果生成される新しい値は、デフォルトではレジストリ キー HKEY_LOCAL_MACHINE に定義されます。

  - ユーザ *admin1* に ADMIN 属性が割り当てられています。

  ```
  newres REGVAL HKEY_LOCAL_MACHINE¥Software¥Mineval dword(4)
  ```

chusr / editusr / newusr

chusr は、ユーザ レコードのプロパティを変更するコマンドです。eTrust Access Control では、ユーザが現在システムにログイン中であっても、chusr コマンドの実行直後にユーザ レコードが変更されます。editusr は、新しいユーザを定義することも、既存のユーザのプロパティを変更することもできるコマンドです。newusr は、eTrust Access Control および Windows データベースに新しいユーザを定義するコマンドです。

権限

chusr コマンドおよび editusr コマンドを実行するために必要な権限のレベルは、指定するパラメータによって異なります。以下のルールが適用されます。

- ADMIN 属性が割り当てられている場合は、audit 以外のすべてのパラメータを指定できます。
- audit パラメータを指定するには、ユーザ レコードで AUDITOR 属性が割り当てられている必要があります。
- 既存のレコードを更新する場合、ユーザ レコードの所有者は、admin、auditor、server、operator、および pwmanager 以外のすべてのパラメータを指定できます。ユーザ レコードにセキュリティ カテゴリを割り当てるには、そのセキュリティ カテゴリが所有者のユーザ レコードに存在する必要があります。ユーザ レコードにセキュリティ ラベルを割り当てるには、そのセキュリティ ラベルが所有者のユーザ レコードに割り当てられている必要があります。ユーザ レコードの所有者は、その所有者のユーザ レコードに割り当てられているセキュリティ レベル以下の任意のセキュリティ レベルを割り当てることができます。
- GROUP-ADMIN 属性を持つグループの有効範囲内にユーザ レコードが含まれている場合は、レコードの所有者と同じ権限が与えられます。
- GROUP-AUDITOR 属性を持つグループの有効範囲内にユーザ レコードが含まれている場合は、audit パラメータを指定できます。
- ADMIN クラスの USER レコードのアクセス制御リストで MODIFY(chusr の場合)権限または CREATE(editusr の場合)権限を割り当てられている場合は、ユーザ レコードの所有者と同じ権限が与えられます。

chusr コマンドおよび editusr コマンドに適用される管理者権限の範囲の詳細については、「**管理者ガイド**」を参照してください。

```
{chusr   | cu} user-name | (user-names ...)
または
{editusr | eu} user-name | (user-names ...)
または
{newusr | nu} user-name | {user-names ….}

        [admin | admin-]

        [audit(none | all | success | failure | loginsuccess | loginfail | trace) | audit-]
```

```
            [auditor | auditor-]
            [auth_type(authentication-method)]
            [auth_type+(authentication-method)]
            [auth_type-(authentication-method)]
            [category(category-names...) | category-(category-names...)]
            [comment('installation defined data') | comment- ]
            [country(...)]
            [enable]
            [expire | expire(mm/dd/yy[yy][@hh:mm]) | expire-]
            [fullname('full-name')]
            [gen_prop(property-name) [ {gen_flag | gen_op}(flag)]
gen_val(property-values ...)]
            [gowner(group-name)]
            [grace(number-of-grace-logins) | grace-]
            [ign_hol | ign_hol-]
            [inactive(num-inactive-days) | inactive-]
            [interval(maximum-password-change-interval) | interval-]
            [label(label-name)| label-]
            [level(seclevel-num) | level-]
            [location(...)]
            [maxlogins(maximum-number-of-logins) | maxlogins-]
            [min_life(minimum-password-change-interval) | min_life-]
            [notify(notify-address) | notify-]
            [operator | operator-]
            [organization(name)]
            [org_unit(name)]
            [owner(user-name or group-name)]
            [password(user's temporary password)]
            [phone(...)]
            [pmdb(PolicyModel-name) | pmdb-]
            [record(group-name) | record-]
            [pwmanager | pwmanager-]
            [regular]
            [restrictions(days( day-data ) time(hhmm:hhmm | anytime) ) | restrictions-]
            day-data:{[mon] [tue] [wed] [thu] [fri] [sat] [sun]} | anyday | weekdays
            [resume | resume(mm/dd/yy[yy][@hh:mm]) | resume-]
            [server | server-]
            [suspend | suspend(mm/dd/yy[yy][@hh:mm]) | suspend-]
            [nt| nt( nt-user-attributes )]
            nt-user-attributes
            [admin | admin-]
            [comment('installation defined data') | comment- ]
            [country(any-string)]
            [expire | expire(mm/dd/yy[@hh:mm]) | expire-]
            [flags(account-flags) | -(account-flags)]
            [homedir(any-string)]
            [homedrive(home-drive)]
            [location(any-string)]
            [logonserver(server-name)]
```

```
[name(full-name)]
[organization(name)]
[org_unit(name)]
[password(user's temporary password)]
[pgroup(primary-group)]
[phone(any-string)]
[privileges(privilege-list)]
[restrictions(days( day-data ) time(hhmm:hhmm | anytime) )]
day-data:{[mon] [tue] [wed] [thu] [fri] [sat] [sun]} | anyday | weekdays
[script(logon-script-path)]
[workstation(workstation-list)]
```

user-name

ユーザ レコードの名前です。newusr コマンドを使用する場合、eTrust Access Control では、ユーザはこの名前によって識別されます。各ユーザ名には、現在データベース内でユーザ名またはグループ名として存在していない一意の名前を指定する必要があります。また、ユーザがすでに UNIX/Linux に定義されている場合は、UNIX/Linux のユーザ名と同じ名前を指定する必要があります。

通常、Windows によって認識されるログイン名と同じ名前を eTrust Access Control のユーザ名として指定します。ただし、何らかの目的のために、Windows ログイン名とは異なる eTrust Access Control のユーザ名を指定することもできます(その場合、ユーザは login コマンドでは操作を開始できませんが、sesu コマンドなどの他のコマンドを実行すると操作を開始できます)。

複数のユーザ レコードを定義または変更する場合は、ユーザ名のリストを丸かっこで囲み、各ユーザ名をスペースまたはカンマで区切ります。

admin

ユーザに ADMIN 属性を割り当てます。ADMIN 属性を持つユーザは、audit 以外のすべてのパラメータを使用して eTrust Access Control のすべてのコマンドを発行できます。admin パラメータを発行するには ADMIN 属性が必要です。

admin-

admin- パラメータは、ユーザから ADMIN 属性を削除します。admin- パラメータを使用するには ADMIN 属性が必要です。このパラメータは chusr コマンドまたは editusr コマンドにのみ使用できます(ADMIN 属性を持つユーザがデータベースに 1 ユーザしか定義されていない場合は、そのユーザから ADMIN 属性を削除することはできません。データベースに少なくとも 1 人は ADMIN 属性を持つユーザが常に定義されている必要があります)。

audit(*mode*)

監査ログに記録するユーザ アクティビティを示します。複数のイベント タイプを指定する場合は、各イベント タイプの名前をスペースまたはカンマで区切ります。audit 属性には以下の種類があります。

- all - eTrust Access Control で保護されているリソースに対するすべてのユーザ アクティビティがログに記録されます。監視されるアクティビティは、failure、loginfail、loginsuccess、および success です。

- failure - 失敗したアクセス試行がログに記録されます。
- loginfail - 失敗したログインがログに記録されます。
- loginsuccess - 成功したログインがログに記録されます。
- none - ユーザ アクティビティはログに記録されません。
- success - 成功したアクセスがログに記録されます。

auditor

ユーザに AUDITOR 属性を割り当てます。AUDITOR 属性を持つユーザは、システム リソースの使用状況を監査できます。また、eTrust Access Control の権限チェックで検出された、eTrust Access Control の保護対象であるすべてのリソースへのアクセス、およびデータベースへのアクセスに対するログの記録を制御できます。AUDITOR 属性を持つユーザに与えられる権限の詳細については、「**管理者ガイド**」を参照してください。auditor パラメータを指定するには ADMIN 属性が必要です。

auditor-

ユーザ レコードから AUDITOR 属性を削除します。auditor- パラメータを指定するには ADMIN 属性が必要です。このパラメータは chusr コマンドまたは editusr コマンドにのみ使用できます。

calendar(*calendarName*)

Unicenter TNG で時刻制限を表す Unicenter TNG カレンダ オブジェクトを示します。eTrust Access Control では、これらのオブジェクトのリストは管理目的のみに使用され、オブジェクトは保護されません。

calendarName は、CALENDAR クラスに定義された 1 つまたは複数の Unicenter TNG カレンダ レコードの名前です。複数のカレンダを割り当てる場合は、各カレンダ名をスペースまたはカンマで区切ります。

calendar-

ユーザ レコードから 1 つまたは複数の Unicenter TNG カレンダ レコードを削除します。このパラメータは chusr コマンドまたは editusr コマンドにのみ使用できます。

auth_type(*authentication-method*)

このユーザに対して許可する認証方法を設定します。

auth_type+(*authentication-method*)

このユーザに対して許可する認証方法を追加します。

auth_type-(*authentication-method*)

このユーザに対して許可されている認証方法を削除します。

category(*category-names*)

CATEGORY クラスに定義された 1 つまたは複数のセキュリティ カテゴリ レコードをユーザに割り当てます。複数のセキュリティ カテゴリを割り当てる場合は、各セキュリティ カテゴリ名をスペースまたはカンマで区切ります。セキュリティ カテゴリのチェックの詳細については、「**管理者ガイド**」を参照してください。

category-(*category-names*)

ユーザ レコードから 1 つまたは複数のセキュリティ カテゴリを削除します。複数のセキュリティ カテゴリを削除する場合は、各セキュリティ カテゴリ名をスペースまたはカンマで区切ります。このパラメータは chusr コマンドまたは editusr コマンドにのみ使用できます。

comment(*'installation defined data'*)

ユーザ レコードにコメント文字列を割り当てます。最大 255 文字の英数字から成る文字列を入力します。文字列に空白が含まれる場合は、文字列全体を一重引用符で囲みます。

comment-

ユーザ レコードからコメント文字列を削除します。このパラメータは chusr コマンドまたは editusr コマンドにのみ使用できます。

country('*country-name*')

ユーザの国名を示します。最大 19 文字の英数字から成る文字列を入力します。文字列に空白が含まれる場合は、文字列全体を一重引用符で囲みます。この文字列は認証プロセスでは使用されません。

enable

何らかの理由で無効になっているユーザのログインを有効にします。このパラメータは、chusr コマンドおよび editusr コマンドにのみ使用します。

expire(*date*)

ユーザ アカウントが失効する日付を設定します。この日付が未指定の場合、ユーザがログインしていなければ、ユーザ アカウントはただちに失効します。ユーザがログインしている場合は、ユーザがログアウトした時点で失効します。

このパラメータの値がユーザ レコードに指定されている場合は、ユーザ レコードの値が GROUP クラスのレコードの値よりも優先されます。

有効期限の日付と時刻は、以下の形式で指定します。時刻は省略可能です。
*mm/dd/yy [yy][@HH:MM]*年は、下 2 桁または 4 桁のどちらでも指定できます。

注: 失効したユーザ レコードは、resume パラメータに再開日を指定しても有効にできません。失効したユーザ レコードを有効にするには、expire- パラメータを使用します。

expire-

newusr コマンドの場合は、有効期限のないユーザ アカウントを示します。chusr コマンドおよび editusr コマンドの場合は、ユーザ アカウントから有効期限を削除します。

flags (*account-flags* | *-account-flags*)

ユーザ アカウントの特定の属性を示します。有効なフラグ値の詳細については、付録「Windows の値」を参照してください。

ユーザ レコードからフラグを削除するには、フラグ値の前にマイナス記号(-)を付けます。-flags は、chusr コマンドまたは editusr コマンドにのみ指定できます。

fullname('*full-name*')

ユーザ レコードに関連付けられたユーザのフル ネームを示します。eTrust データベースでは、文字列には最大 256 文字の英数字を含めることができます。文字列に空白文字が含まれる場合は、文字列を一重引用符で囲みます。

gen_prop(property-name)

Active Directory プロパティを示します。

gen_flag|gen_op(*flag*)

gen_val(*property-values*)

Active Directory プロパティに関連付ける値を示します。

gowner(*group-name*)

ユーザ レコードの所有者として eTrust Access Control のグループを割り当てます。ユーザ レコードのグループ所有者には、ユーザ レコード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、グループ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、ユーザ レコード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。ユーザ レコードのグループ所有者は、ユーザ レコードをいつでも更新および削除することができます。詳細については、「**管理者ガイド**」を参照してください。

grace(*number-of-grace-logins*)

ユーザに許可する猶予ログイン回数を設定します。0 から 255 までの正の整数を入力します。

猶予ログイン回数に達するとユーザはシステムにアクセスできなくなるため、システム管理者に連絡して新しいパスワードを設定する必要があります。猶予回数が 0 に設定されている場合、ユーザはログインできません。

このパラメータの値がユーザ レコードに指定されている場合は、ユーザ レコードの値が GROUP クラスのレコードの値よりも優先されます。

このパラメータを指定しない場合でも、ユーザのプロファイル グループにこのパラメータの値が含まれている場合は、GROUP クラスのレコードの値が使用されます。USER レコードと GROUP レコードのいずれにも値がない場合は、eTrust Access Control のグローバルな猶予ログイン設定の値が使用されます。

grace-

ユーザの猶予ログイン設定を削除します。代わりに、eTrust Access Control のグローバル猶予ログイン設定が使用されます。このパラメータは chusr コマンドまたは editusr コマンドにのみ使用できます。

homedir(*any-string*)

ユーザのホーム ディレクトリの完全パスを指定します。パスの最後にスラッシュを付けると、eTrust Access Control によって、指定したパスに userName が自動的に追加されます。

homedrive(*home-drive*)

ユーザのホーム ディレクトリのドライブを示します。ユーザは、自分のホーム ドライブおよびホーム ディレクトリに自動的にログインできます。

ign_hol

ユーザに IGN_HOL 属性を割り当てます。IGN_HOL 属性を持つユーザは、holiday レコードに定義された期間中にログインできます。

ign_hol-

ユーザから IGN_HOL 属性を削除します。属性を削除されたユーザは休日にログインできなくなります。

inactive(*number-of-inactive-days*)

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示します。指定した日数が経過すると、ユーザはログインできなくなります。

正の整数または 0 を入力します。inactive を 0 に設定した場合は、inactive- パラメータを使用した場合と同じ結果になります。

注: ユーザ レコードでは、アクティブでないユーザのマークが設定されません。アクティブでないユーザを識別するには、Inactive Days 値と Last Accessed Time 値を比較する必要があります。

inactive-

ユーザのステータスを非アクティブからアクティブに変更します。このパラメータは chusr コマンドまたは editusr コマンドにのみ使用できます。

interval(*maximum-password-change-interval*)

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。正の整数または 0 を入力します。interval に 0 を設定すると、グループに対するパスワード期間のチェックが無効になり、パスワードが失効しません。setoptions コマンドで設定したデフォルト値は使用されません。セキュリティ要件が厳しくないユーザに対してのみ interval を 0 に設定してください。

指定した日数が経過すると、eTrust Access Control は、現在のパスワードが期限切れになったことをユーザに通知します。通知を受けたユーザは、ただちにパスワードを更新するか、猶予ログイン回数に達するまで古いパスワードを引き続き使用することができます。猶予ログイン回数に達するとユーザはシステムへのアクセスを許可されないため、システム管理者に連絡して新しいパスワードを設定する必要があります。

interval-

ユーザのパスワード期間の設定を取り消します。このパラメータの値がユーザのプロファイル グループに含まれている場合は、その値が使用されます。それ以外の場合は、setoptions コマンドで設定したデフォルト値が使用されます。このパラメータは chusr コマンドまたは editusr コマンドにのみ使用できます。

label(*/abel/-name*)

SECLABEL クラスに定義されているセキュリティ ラベル レコードをユーザ レコードに割り当てます。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。セキュリティ ラベルのチェックの実装方法については、「**管理者ガイド**」を参照してください。

label-

ユーザ レコードからセキュリティ ラベルを削除します。このパラメータは chusr コマンドまたは editusr コマンドにのみ使用できます。

level(*sec/eve/-num*)

ユーザ レコードにセキュリティ レベルを割り当てます。1 から 255 までの正の整数を入力します。セキュリティ レベル チェックの実装方法については、「**管理者ガイド**」を参照してください。

level-

ユーザ レコードからセキュリティ レベルを削除します。セキュリティ レベルを削除すると、ユーザは、アクセサのセキュリティ レベルが指定されているリソースにはアクセスできなくなります。このパラメータは chusr コマンドまたは editusr コマンドにのみ使用できます。

location(*string*)

ユーザの所在地を示します。最大 47 文字の英数字から成る文字列を入力します。文字列に空白が含まれる場合は、文字列全体を一重引用符で囲みます。この文字列は認証プロセスでは使用されません。

logonserver(*server-name*)

ユーザのログイン情報を確認するサーバを示します。ユーザがドメイン ワークステーションにログインすると、eTrust Access Control からそのサーバにログイン情報が送られ、ユーザがワークステーションを使用することが許可されます。

maxlogins(*maximum-number-of-logins*)

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。このパラメータを指定しない場合は、グローバルな最大ログイン回数の設定が使用されます。

注: maxlogins を 1 に設定すると、selang を実行できません。この場合、eTrust Access Control を停止し、maxlogins 設定を 2 以上の値に変更して、eTrust Access Control を再起動する必要があります。

maxlogins-

ユーザの最大ログイン回数の設定を削除します。代わりに、グローバルな設定が使用されます。このパラメータは chusr コマンドまたは editusr コマンドにのみ使用できます。

min_life(*minimum-password-change-interval*)

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です。正の整数を入力します。

min_life-

ユーザの min_life 設定を削除します。このパラメータの値がユーザのプロファイルグループに含まれている場合は、その値が使用されます。それ以外の場合は、setoptions コマンドで設定したデフォルト値が使用されます。このパラメータは chusr コマンドまたは editusr コマンドにのみ使用できます。

name(*full-name*)

ユーザ レコードに関連付けられたユーザのフル ネームを示します。最大 256 文字の英数字から成る文字列を入力します。文字列に空白が含まれる場合は、文字列全体を一重引用符で囲みます。

notify(*notify-address*)

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許可されないアクセス試行に対処する必要があります。

通知メッセージが送信されるたびに、監査ログに監査レコードが書き込まれます。監査レコードのフィルタ処理および表示の詳細については、「**管理者ガイド**」を参照してください。

制限: 30 文字。

notify-

ユーザがログインしたときに誰にも通知を行わないことを示します。このパラメータは chusr コマンドまたは editusr コマンドにのみ使用できます。

nt(*nt-user-attributes*)

chusr コマンドおよび editusr コマンドでこのパラメータを使用する場合、ローカル Windows システムのユーザ定義を変更します。newusr コマンドでこのパラメータを使用する場合、ユーザをローカル Windows システムに追加します。複数の引数を指定する場合は、各引数をスペースで区切ります。

eTrust Access Control 内でローカル Windows システムを操作する方法については、この章の environment コマンドの説明および「Windows 環境の selang のコマンド」の章を参照してください。

operator

ユーザに OPERATOR 属性を割り当てます。OPERATOR 属性を持つユーザは、データベースのすべてのリソース レコードを一覧表示できます。また、このユーザには、eTrust Access Control で定義されたすべてのファイルに対する読み取り権限が与えられます。詳細については、「**管理者ガイド**」を参照してください。

この属性を持つユーザは、secons コマンドのすべてのオプションも使用できます。secons ユーティリティの詳細については、このマニュアルの「ユーティリティ」の章を参照してください。

operator-

ユーザ レコードから OPERATOR 属性を削除します。このパラメータは chusr コマンドまたは editusr コマンドにのみ使用できます。

organization(*name*)

ユーザが所属する組織を示します。最大 256 文字の英数字から成る文字列を入力します。文字列に空白が含まれる場合は、文字列全体を一重引用符で囲みます。この情報は認証プロセスでは使用されません。

org_unit(*name*)

ユーザが所属する組織単位を示します。最大 256 文字の英数字から成る文字列を入力します。文字列に空白が含まれる場合は、文字列全体を一重引用符で囲みます。この情報は認証プロセスでは使用されません。

owner(*user-name*|*group-name*)

ユーザ レコードの所有者として eTrust Access Control のユーザ(*user-name*)またはグループ(*group-name*)を割り当てます。詳細については、「**管理者ガイド**」を参照してください。

password(*user's temporary password*)

最大 14 文字のパスワードをユーザに割り当てます。スペースまたはカンマ以外の任意の文字を示します。パスワード チェックが有効になっている場合、指定したパスワードでログインできるのは 1 回のみです。次回システムにログインする際に、ユーザは新しいパスワードを設定する必要があります。

ADMIN 属性または PWMANAGER 属性を持つユーザまたは eTrust Access Control Admins グループのメンバであっても、自分のパスワードを変更することはできません。

pgroup(*primary-group*)

ユーザのプライマリ グループ ID を設定します。プライマリ グループはユーザが定義されているグループの 1 つで、グローバル グループである必要があります。

eTrust Access Control では、プライマリ グループは特別重要ではありません。

phone(*string*)

ユーザの電話番号を示します。最大 19 文字の英数字から成る文字列を入力します。文字列に空白が含まれる場合は、文字列全体を一重引用符で囲みます。この情報は認証プロセスでは使用されません。

pmdb(PolicyModel-name)

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*)に伝達されることを示します。レジストリのサブキーの parent_pmd 値か passwd_pmd 値で定義されている Policy Model にパスワードは送信されません。

KEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥eTrustAccessControl¥eTrustAccessControl

pmdb-

ユーザ レコードから pmdb 属性を削除します。このパラメータは chusr コマンドまたは editusr コマンドにのみ使用できます。

privileges(*privilege-list*)

Windows のユーザ レコードに特定の権限を追加します。privList の前にマイナス記号(-)を付けた場合は、指定した権限を削除します。このパラメータは、chusr コマンドまたは editusr コマンドで既存のユーザ レコードを変更する場合にのみ指定可能です。新しいユーザ レコードを作成するときに、このパラメータを使用して権限を割り当てることはできません。

record(*group-name*)

ユーザをプロファイル グループに割り当てます。ユーザ レコード内のユーザにプロパティが明示的に割り当てられていない場合は、eTrust Access Control によってプロファイル グループのプロパティがユーザに割り当てられます。

以下の値をプロファイル グループから取得できます。

- audit
- auth_type
- expire
- grace
- inactive
- interval
- maxlogins
- min_life
- nt
- password rules
- pmdb
- pwd_autogen
- pwd_policy
- pwd_sync
- restrictions (days, time)
- resume
- suspend

record-

ユーザをプロファイル グループから削除します。このパラメータは chusr コマンドまたは editusr コマンドにのみ使用できます。

pwasown(*string*)

ユーザ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。このパラメータを指定すると、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。

pwmanager

ユーザに PWMANAGER 属性を割り当てます。この属性を持つユーザは、データベースにあるユーザのパスワードを変更できます。詳細については、「**管理者ガイド**」を参照してください。

pwmanager-

ユーザ レコードから PWMANAGER 属性を削除します。このパラメータは chusr コマンドまたは editusr コマンドにのみ使用できます。

restrictions(days(*day-data*) time(*time-data*))

ユーザがファイルにアクセスできる曜日と時間帯を示します。

days 引数を指定せずに time 引数を指定した場合、レコード内にすでに設定されている曜日制限に対して、指定した時刻制限が適用されます。time 引数を指定せずに days 引数を指定した場合、レコード内にすでに設定されている時刻制限に対して、指定した曜日制限が適用されます。days 引数と time 引数の両方を指定した場合、ユーザは、指定した曜日の指定した時間帯にのみシステムにアクセスできます。

- (*day-data*) はユーザがファイルにアクセスできる曜日を示します。days 引数には以下のサブ引数があります。
  - anyday - ユーザはすべての曜日にファイルにアクセスできます。
  - weekdays - ユーザは月曜から金曜までの平日に限りリソースにアクセスできます。
  - Mon、Tue、Wed、Thu、Fri、Sat、Sun - ユーザは指定した曜日にのみリソースにアクセスできます。曜日は任意の順で指定できます。複数の曜日を指定する場合は、各曜日をスペースまたはカンマで区切ります。
- (*time-data*) には、ユーザがリソースにアクセスできる時間帯を示します。time 引数には以下のサブ引数があります。
  - anytime - ユーザは任意の時間帯にリソースにアクセスできます。

- startTime:endTime - 指定した時間帯に限りリソースにアクセスできます。startTime と endTime の両方とも *hhmm* の形式で指定します。*hh* は 24 時間表記の時間(00 から 23)、*mm* は分(00 から 59)を表します。2400 は有効な time 値ではないことに注意してください。startTime が endTime より小さいこと、および両方が同じ日の時刻であることが必要です。端末がホストと異なるタイム ゾーンにある場合は、端末の開始時間と終了時間をホストのローカル時間に相当する時間に変換し、時間の値を調整してください。たとえば、ホストがニューヨークにあり、端末がロサンゼルスにある場合、端末へのアクセスをロサンゼルス時間の午前 8 時から午後 5 時まで許可するには、「time (1100:2000)」と指定します。

restrictions-(days(*day-data*) time(*time-data*))

ファイルに対するユーザのアクセス権限を限定するすべての曜日および時間帯の制限を削除します。

resume(*date@time*)

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。suspend パラメータと resume パラメータの両方を指定する場合、再開日を一時停止日より後に設定していることを確認する必要があります。そうでないと、ユーザの一時停止が無期限になります。*date@time* を省略すると、chusr コマンドの実行直後にユーザ レコードが再開されます。詳細については、「**管理者ガイド**」を参照してください。

日付と時刻は、以下の形式で指定します。時刻は省略可能です。

m/dd/yy[@HH:MM]

resume-

再開日および再開時間(指定されている場合)をユーザ レコードから消去します。これにより、ユーザのステータスがアクティブ(有効)から一時停止に変更されます。このパラメータは chusr コマンドまたは editusr コマンドにのみ使用できます。

script(*logon-script-path*)

ユーザがログインしたときに自動的に実行されるファイルの場所を示します。このログイン スクリプトによって作業環境が設定されます。ユーザの作業環境は profile パラメータでも設定されるため、このパラメータの指定は省略可能です。

server

SERVER 属性を設定します。現在のユーザに代わり実行しているプロセスから、他のユーザの権限を照会できるようになります。詳細については、「**管理者ガイド**」を参照してください。

server-

SERVER 属性の設定を解除します。このパラメータは chusr コマンドまたは editusr コマンドにのみ使用できます。

suspend(*date@time*)

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。*date@time* を指定すると、指定された日にユーザ レコードが一時停止されます。*date@time* を省略すると、chusr コマンドの実行直後にユーザ レコードが一時停止されます。

日付と時刻は、次の形式で指定します。時刻は省略可能です。*mm/dd/yy[@HH:MM]*

suspend-

一時停止日をユーザ レコードから消去し、ユーザのステータスを無効からアクティブ(有効)に変更します。このパラメータは chusr コマンドまたは editusr コマンドにのみ使用できます。

workstation(*workstation-list*)

ユーザがログインできるワークステーションを最大 8 台まで示します。ワークステーションのリストを一重引用符で囲み、各ステーション名をカンマで区切ります。次に例を示します。「workstation1,workstation2」

関連項目

この章の rmusr コマンドおよび showusr コマンドの説明。

例

- ユーザ Bob が、Jim のレコードに FINANCIAL カテゴリを追加し、Jim のセキュリティレベルを 155 に変更し、さらに Jim によるシステムへのアクセスを平日の午前 8 時から午後 8 時までに制限するとします。
  - ユーザ Bob に ADMIN 属性が割り当てられています。
  - eTrust Access Control にユーザ Jim が定義されています。
  - eTrust Access Control に FINANCIAL カテゴリが定義されています。

  ```
  chusr Jim category(FINANCIAL) level(155) restrictions ¥
  (days(weekdays)time(0800:2000))
  ```

- ユーザ「admin」が、1995 年 8 月 5 日から 3 週間の休暇に入る予定のユーザ Joel を一時停止するとします。
  - ユーザ admin に ADMIN 属性が割り当てられています。
  - eTrust Access Control にユーザ Joel が定義されています。
  - 現在の日付は 1994 年 8 月 3 日です。

  ```
  chusr Joel suspend(8/5/95) resume(8/26/95)
  ```

- ユーザ Security2 が、ユーザ Bill から AUDITOR 属性を削除し、Bill のすべてのアクティビティを監査するとします。

- ユーザ Security2 に ADMIN 属性および AUDITOR 属性が割り当てられています。
- eTrust Access Control にユーザ Bill が定義されています。

```
chusr Bill auditor- audit(all)
```

- ユーザ Rob が、ユーザ Mary のレコードに格納されているコメントを変更するとします。
  - ユーザ Rob が Mary のユーザ レコードの所有者です。

```
chusr Mary comment ('Administrator of the SALES group')
```

- ADMIN 属性を持つユーザ Sally が、ユーザ Jared のレコードに格納されている国名および所在地のプロパティを削除するとします。
  - ユーザ Sally が Jared のユーザ レコードの所有者です。

```
chusr Jared country() location()
```

  - レコード プロパティが文字列で定義されている場合、プロパティを削除するには、「-」記号または空のかっこ「()」のいずれかを付けてプロパティを入力します。
- ユーザ Bob が、ユーザ Peter およびユーザ Joe を eTrust Access Control に定義するとします。
  - ユーザ Bob に ADMIN 属性が割り当てられています。
  - ユーザ Peter およびユーザ Joe が eTrust Access Control に定義されていません。
  - 以下のデフォルト値が当てはまります。
    - owner(Bob)
    - audit(failure, loginfailure)

```
newusr (Peter Joe)
```

    - ユーザ Bob がユーザ Jane を eTrust Access Control に定義し、Jane を所有するグループとして「payroll」を割り当てるとします。
  - ユーザ Bob に ADMIN 属性が割り当てられています。
  - eTrust Access Control にユーザ Jane が定義されていません。
  - ユーザ Jane のフル ネームは JG Harris です。
  - audit(failure, loginfailure)

```
newusr Jane owner(payroll) name('J.G. Harris')
```

- ユーザ Bob がユーザ *JohnD* を eTrust Access Control に定義し、セキュリティ カテゴリ NewEmployee およびセキュリティ レベル 3 を設定するとします。JohnD がシステムを使用できるのは、平日の午前 8 時から午後 6 時までのみに設定します。

- ユーザ Bob に ADMIN 属性が割り当てられています。
- eTrust Access Control に NewEmployee カテゴリが定義されています。
- 新しいユーザのフル ネームは John Doe です。
- 以下のデフォルト値が当てはまります。
  - owner(Bob)
  - audit(failure)

```
newusr JohnD name('John Doe') category(NewEmployee) level(3) ¥
restrictions(days(weekdays)time(0800:1800))
```

deploy

deploy コマンドは、selang のコマンドを実行することによってポリシー展開を開始します。selang のコマンドは、展開対象の POLICY オブジェクトに関連付けられた RULESET オブジェクトと共に保存されています。このコマンドは、ポリシー展開用のコマンドです。

重要: ポリシーの展開には、policydeploy ユーティリティを使用することを強くお勧めします。deploy コマンドを使用すると、ポリシー展開の一部しか実行されず、ポリシーをエンドポイントに展開したときに DMS が更新されません。

deploy コマンドを実行するには、以下が必要となります。

- ポリシーを展開するデータベースの下の階層にある各データベースの POLICY、HNODE、および RULESET クラスに対するサブ管理権限。
- ポリシーを展開するデータベースの下の階層にある各データベースの適切なサブ管理権限。

  これらの権限は、各コンピュータのポリシーを構成する selang のコマンドを実行するうえで必要となります。

  たとえば、新しいファイル リソースを作成する場合は、FILE クラスに対するサブ管理権限が必要になります。

  ```
  nr FILE /inetpub/* defaccess(none)
  ```

注: ポリシーの展開の詳細については、「**管理者ガイド**」を参照してください。policydeploy ユーティリティの詳細については、「**ユーティリティ**」の章を参照してください。

```
deploy POLICY name#xx
```

name#xx

展開するポリシーの POLICY オブジェクトの名前(ポリシー名とバージョン番号)。

deploy-

deploy-(つまり展開解除)コマンドは、selang のコマンドを実行することによってポリシー展開解除を開始します。selang のコマンドは、展開対象の POLICY オブジェクトに関連付けられた RULESET オブジェクトと共に保存されています。このコマンドは、ポリシー展開解除用のコマンドです。

重要: ポリシーの展開解除には、policydeploy ユーティリティを使用することを強くお勧めします。deploy- コマンドを使用すると、ポリシー展開解除の一部しか実行されず、ポリシーをエンドポイントから展開解除したときに DMS が更新されません。

このコマンドを実行するには、以下が必要となります。

- ポリシーを展開解除するデータベースの下の階層にある各データベースの POLICY、HNODE、および RULESET クラスに対するサブ管理権限。
- ポリシーを展開解除するデータベースの下の階層にある各データベースの適切なサブ管理権限。

  これらの権限は、各コンピュータのポリシー展開解除スクリプトを構成する selang のコマンドを実行するうえで必要となります。

注: ポリシーの展開の詳細については、「**管理者ガイド**」を参照してください。policydeploy ユーティリティの詳細については、「**リファレンス ガイド**」を参照してください。

{deploy- | undeploy} POLICY *name#xx*

name#xx

展開解除するポリシーの POLICY オブジェクトの名前(ポリシー名とバージョン番号)。

environment

environment コマンドは、セキュリティ環境を設定します。eTrust Access Control は、eTrust Access Control、Windows、および UNIX/Linux のセキュリティ環境をサポートします。selang コマンド シェルを呼び出すときのデフォルトの環境は eTrust 環境です。

```
{environment | env} {eTrust | native | nt | pmd | unix}
```

eTrust

eTrust のセキュリティ環境を示します。selang のコマンドは、eTrust Access Control データベースに対して実行されます。一部のコマンドでは、接続先ホストのネイティブ OS のセキュリティ設定を同時に更新できます。eTrust 環境の selang のプロンプトは以下のとおりです。

```
eTrustAC>
```

native

ローカルかリモートかに関係なく、接続先ホストのネイティブ OS のセキュリティ環境（Windows または UNIX/Linux）を示します。selang のコマンドは、ネイティブ OS データベースに対して実行されます。ネイティブ環境の selang のプロンプトは以下のとおりです。

```
eTrustAC(native)>
```

nt

Windows のセキュリティ環境を示します。selang のコマンドは、Windows データベースに対して実行されます。一部のコマンドでは、eTrust Access Control の複数のセキュリティ設定を同時に更新できます。Windows 環境の selang のプロンプトは以下のとおりです。

```
eTrustAC(nt)>
```

pmd

リモート管理の環境を示します。selang のコマンドは、選択されたホストの PMDB に対して実行されます。pmd 環境の selang のプロンプトは以下のとおりです。

```
eTrustAC(pmd)>
```

unix

入力するコマンドを UNIX/Linux データベースに対して実行することを示します。UNIX/Linux 環境の selang のプロンプトは以下のとおりです。

```
eTrustAC(unix)>
```

find

find コマンドには以下の機能があります。

- クラスを指定しない場合は、eTrust Access Control に定義されたすべてのクラスの名前が出力されます。
- クラスのみを指定した場合は、指定したクラス内のすべてのオブジェクトの名前が出力されます。
- クラスとオブジェクト マスクの両方を指定した場合は、指定したクラスに属するオブジェクトのうち、指定したオブジェクト マスクに一致するすべてのオブジェクトの名前が出力されます。

注:

- ADMIN 属性、AUDITOR 属性、または OPERATOR 属性が割り当てられている場合は、find コマンドにすべてのパラメータを指定できます。
- ADMIN クラスのレコードのアクセス制御リストに READ 権限が指定されている場合は、レコードが示すクラスに class パラメータを指定できます。

{find | f} [{*className* | class(*className*)} | *className*(*memberName*) | *objMask*]

class(*className*)

SEOS を除く、eTrust 環境で有効なクラスの名前です。

objmask

指定したクラスのオブジェクトのうち、指定したオブジェクト マスクに一致するオブジェクトをすべて一覧表示します。オブジェクト マスクはワイルドカードを使用して指定します。

className(*memberName*)

クラスのメンバの名前です。複数のエントリは、丸かっこで囲み、スペースまたはカンマで区切ります。

例

ADMIN 属性を持つユーザ Sue が、eTrust Access Control データベースに定義されているすべての PROGRAM リソースを一覧表示するとします。

```
eTrustAC> find PROGRAM
(localhost)
_default
C:¥WINNT¥system32¥cidaemon.exe
C:¥WINNT¥system32¥DRWTSN32.EXE
C:¥WINNT¥System32¥WBEM¥WinMgmt.exe
```

get devcalc

get devcalc コマンドは、ポリシー偏差計算の結果を格納するポリシー偏差データ ファイル(deviation.dat)から情報を取得し、少なくとも 1 つの set DMS データベース(121 ページ)にこれらの情報を送信します。start devcalc コマンド(137 ページ)が以前に発行されていない場合、このデータ ファイルは存在しません。

ポリシーまたはホスト レポートを作成する場合は、偏差計算の結果を含めるように指定することもできます。そのように指定すると、レポート作成ユーティリティによってこのコマンドが発行されます。

重要: 偏差計算では、Windows(ネイティブ)ルールが適用されるかどうかはチェックされません。データベースからオブジェクト(ユーザまたはオブジェクト属性、ユーザまたはリソース権限、あるいは実際のユーザまたはリソース)を削除するルールも無視されます。たとえば、偏差計算では、以下のルールが適用されるかどうかは確認できません。

```
rr FILE C:¥tmp¥tmp.txt
```

注: ポリシー偏差データ ファイルと高度なポリシー レポートの詳細については、「**管理者ガイド**」を参照してください。

get devcalc コマンドを実行するには、コンピュータに対する端末アクセス権と DEVCALC サブ管理クラスに対する読み取りアクセス権限を持っている必要があります。

```
get devcalc [params("offset=<number>")]
```

offset=*<number>*

(オプション)ポリシー偏差データ ファイルから追加行を取得するためのオフセットを示します。get devcalc コマンドでは、要求ごとにポリシー偏差データ ファイルの最大行数(max_lines_request レジストリ エントリによって設定)しか返されません。ファイルにその他の情報がある場合は、返される最終行を指定したオフセット データが返されます。

注: レジストリ エントリの詳細については、付録「レジストリ キー」を参照してください。

例: ポリシー偏差データの取得

以下の例では、max_lines_request エントリ値が 10 に設定されている場合に、get devcalc コマンドを使用してポリシー偏差データ ファイルから情報を取得する方法を示します。最初のコマンドによって出力の最初の 10 行が取得された後、2 番目のコマンドによって、次の 10 行が取得されます。

```
eTrustAC> get devcalc
(localhost)
Data for DEVCALC 'deviation'
-----------------------------------------
DATA     : DATE, Mon Mar 20 11:22:15 2006
POLICYSTART, myPolicy#01
DIFF, (FILE), (file1), (*), (*)
DIFF, (FILE), (file2), (*), (*)
DIFF, (FILE), (file3), (*), (*)
DIFF, (FILE), (file4), (*), (*)
DIFF, (FILE), (file5), (*), (*)
DIFF, (FILE), (file6), (*), (*)
DIFF, (FILE), (file7), (*), (*)
OFFSET   : 11

eTrustAC> get devcalc params("offset=11")
(localhost)
Data for DEVCALC 'deviation'
-----------------------------------------
DATA     : DIFF, (FILE), (file8), (*), (*)
DIFF, (FILE), (file9), (*), (*)
DIFF, (FILE), (file10), (*), (*)
DIFF, (FILE), (file11), (*), (*)
DIFF, (FILE), (file12), (*), (*)
DIFF, (FILE), (file13), (*), (*)
DIFF, (FILE), (file14), (*), (*)
DIFF, (FILE), (file15), (*), (*)
DIFF, (FILE), (file16), (*), (*)
DIFF, (FILE), (file17), (*), (*)
OFFSET   : 21
```

help

help は、selang の構文を表示するコマンドです。

- パラメータを指定しない場合は、selang のコマンド リストが各コマンドの簡単な説明と共に一覧表示されます。

  authorize (auth) - リソースに対するユーザまたはグループのアクセス許可を設定します。
  authorize- (auth-) - リソースに対するユーザまたはグループのアクセス許可を削除します。
  .
  .
  .

- selang のコマンド名を指定した場合は、指定したコマンドの構文が表示されます (このセクションの「例」を参照してください)。

- access パラメータを指定した場合は、authorize コマンドの access パラメータの値と new* コマンド、ch* コマンド、および edit* コマンドの defaccess パラメータの値が一覧表示されます。

  すべてのクラスに対するアクセス値として、NONE および ALL が有効です。
  FILE :
  READ, WRITE, EXECUTE, UPDATE, CHOWN, CHMOD,
  RENAME, DELETE, UTIME, SEC, CREATE
  PROGRAM、SUDO :
  EXECUTE
  ADMIN :
  READ, MODIFY, CREATE, DELETE, JOIN, PASSWORD
  その他のリソース :
  READ

  アクセス権限の詳細については、「**管理者ガイド**」を参照してください。

- lineedit パラメータを指定した場合は、selang のコマンド ライン操作で使用する特殊文字が一覧表示されます。

  行の先頭に「#」または「*」がある場合はコメントです。

  行の先頭に「!」がある場合はシェル コマンドです。
  前に入力したコマンドを取得するには、上方向キーを使用します。
  コマンド ラインが指定されている場合は、現在のコマンド ラインと一致する
  コマンドのみが検索されます。

  次のコマンドを取得するには、下方向キーを使用します。

  行の先頭に「^」がある場合は、コマンドを履歴から起動します。
  history の詳細についてヘルプを表示するには、「help history」と入力します。

  行の末尾に「¥」がある場合は、コマンドが次の行に続くことを
  示します。

  行の最後にある「|」 (パイプ) は、
  コマンド出力をパイプに送ることを示しています (パイプは 1 つのみ) 。

  単語補完を使用するには、Tab キーを使用します。

利用できるすべての補完リストを取得するには、Ctrl + D キーを使用します。

現在のコマンドのヘルプ テキストを取得するには、Esc キーを 2 回押します。
たとえば、「authorize FILE /tmp/foo」と入力して Esc キーを 2 回押すと、
authorize コマンドのヘルプ テキストが表示されます。ヘルプの表示後もコマンド ラインは
そのまま残ります。

{help | h | ?} [*command-name* | access | lineedit]

commandName

指定したコマンドの構文を要求します。

access

access パラメータと defaccess パラメータで指定できるアクセス タイプのクラス別リストを要求します。

lineedit

selang のコマンド ライン操作に使用する特殊文字のリストを要求します。

例

以下の例では、showusr コマンドの構文を表示します。

```
eTrustAC> help showusr
>> {showusr | su} user-name
                [nt]
```

history

history は、現在の selang コマンド シェル セッション中に入力されたすべてのコマンドを一覧表示するコマンドです。コマンドは入力した順に表示されます。コマンドの番号が各コマンドの先頭に表示されます。たとえば、3 番目に入力されたコマンドの先頭には番号 3 が表示されます。

history コマンドでは、chusr コマンド、newusr コマンド、または editusr コマンドの一部としてパスワードを入力した場合でも、パスワードは表示されません。パスワードは、通常のテキストではなく複数のアスタリスク(***)で表示されます。

selang コマンド言語は、履歴リストのコマンドを実行する以下のショートカットをサポートしています。

^^ [*string*]

1 つ前のコマンド。*string* を指定した場合は、指定した文字列が元のコマンドに追加されます。

^*n* [*string*]

履歴リスト内で番号 *n* が先頭に付いているコマンド(*n* は正の整数)。*string* を指定した場合は、指定した文字列が元のコマンドに追加されます。

^-*n* [*string*]

履歴リストの最後から *n* 番目のコマンド(*n* は正の整数)。*string* を指定した場合は、指定した文字列が元のコマンドに追加されます。

^match [*string*]

match で始まる最後に発行したコマンド(*match* はテキスト文字列)。*string* を指定した場合は、指定した文字列が元のコマンドに追加されます。*match* と *string* はスペースで区切ります。

```
history
```

hosts

名前が異なるリモートの eTrust Access Control マシンにも接続することができます。したがって、ローカル eTrust Access Control サービスが実行されていなくてもリモート管理が可能です。

hosts は、selang のコマンドを受け取るホストまたは Policy Model を指定するコマンドです。ホストに送信されるコマンドを実行する前に、hosts コマンドを実行する必要があります。ホストを指定しない場合は、デフォルトでローカル ホストが対象になり、すべてのコマンドがローカル ホスト上のデータベースに送信されます。

現在使用可能なすべてのホストおよび PMDB を一覧表示するには、パラメータを設定せずに hosts コマンドを指定します。

注:

- ローカル ホストからリモート ホストのデータベースを管理(更新)するユーザは、以下の条件のいずれかを満たしている必要があります。
  - ローカル データベースからリモート ホスト データベースを更新する権限が明示的に与えられていること。
  - ローカル データベースからリモート ホスト データベースを更新する許可が与えられているグループのメンバであること。
  - リモート ホストに定義された、ローカル ホストの所有者であること。
- ローカル データベースからリモート ホストのデータベースを更新する権限をユーザに与えるには、リモート ホスト上で以下のコマンドを入力します。

  authorize TERMINAL *local_host* uid(*user_name*) access(write)
- ローカル データベースからリモート ホストのデータベースを更新する権限をグループに与えるには、リモート ホスト上で以下のコマンドを入力します。

  authorize TERMINAL local_host gid(group_name) access(write)
- hosts *policy@*を指定した場合は、入力するすべてのコマンドによってローカル ホスト上の PMDB が更新されます。
- eTrust Access Control では、別名ではなく正規のホスト名によってホストが保護されます。別名を使用することで起こる混乱を回避するために、HOST ルールを別名に定義すると警告が表示されます。
- 同様に、完全修飾名を使用せずに HOST を定義すると、警告が表示されます。eTrust Access Control では、完全修飾名(mymachine.yourcompany.com など)でホストを表すためです。

hosts [{*systemIds* | policyModel@hostname}]

systemIds

selang のコマンドを実行する対象であるホストのシステム ID です。複数のホストを指定する場合は、システム ID のリストを丸かっこで囲み、各システム ID をスペースまたはカンマで区切ります。

policyModel@hostname

selang のコマンドを実行する対象である Policy Model のアドレスです。複数の Policy Model を指定する場合は、Policy Model のアドレスのリストを丸かっこで囲み、Policy Model の各アドレスをスペースまたはカンマで区切ります。

ホストを明示的に指定するよりも Policy Model を使用する方が優れている点としては、現在使用できないシステムがある場合でも、Policy Model が格納されているシステムにより Policy Model に定義されているすべてのシステムに対し継続して更新が試行されることが挙げられます。Policy Model の詳細については、「**管理者ガイド**」を参照してください。

例

- 以降実行するすべてのコマンドを端末 h1 上の Policy Model に適用するには、以下のコマンドを入力します。

  ```
  hosts Policy@h1
  ```

  Policy@h1 への接続が確立されると、以下のメッセージが表示されます。

  ```
  >> Successfully connected to h1
  ```

  これ以降に入力するすべてのコマンドは、ローカル ホストではなく Policy@h1 に送信されます。selang プロンプトが以下のように変わります。

  ```
  Remote eTrustAC>
  ```

- 以降のコマンドをすべて端末 athena に適用するには、以下のコマンドを入力します。

  ```
  hosts athena
  ```

  athena への接続が確立されると、以下のメッセージが画面に表示されます。

  ```
  >> (athena)
  >> Successfully connected
  >> INFO: Target version is 2.50
  ```

  入力するすべてのコマンドは athena に適用され、ローカル ホストには送信されません。以下の例のように、新しいユーザを追加すると、ユーザは athena のみに追加されます。

  ```
  Remote eTrustAC>newusr steve
  (athena) >> USER steve successfully added.
  ```

join

join は、1 つまたは複数のグループにユーザを追加するか、グループに関連するユーザのプロパティ セットを変更するコマンドです。eTrust Access Control にすでに存在しているユーザおよびグループを指定する必要があります。

指定したグループ内の指定したユーザの以前のプロパティ セットはすべて、join コマンドのプロパティ セット***に完全に置き換えられます***。以前に定義した古いプロパティは、join コマンドで再度指定しない限り維持されません。

注: ADMIN 属性を持つユーザに、eTrust Access Control の GROUP レコードおよび Windows グループを変更する権限を与える場合は、MODIFY プロパティと JOIN プロパティの両方を設定する必要があります。

```
{join | j} user-name | (user-names ...)

        group(group-names)
        [admin | admin-]
        [auditor | auditor-]
        [gowner(group-name)]
        [operator | operator-]
        [owner(user-name or group-name)]
        [pwmanager | pwmanager-]
        [regular]
        [nt]
```

admin

user-name で指定されたユーザに GROUP-ADMIN 属性を割り当てます。詳細については、「**管理者ガイド**」を参照してください。

admin-

ユーザから GROUP-ADMIN 属性を削除します。

auditor

user-name で指定されたユーザに GROUP-AUDIT 属性を割り当てます。詳細については、「**管理者ガイド**」を参照してください。

auditor-

ユーザから GROUP-AUDITOR 属性を削除します。

gowner(*group-name*)

ユーザをグループ *group-name* に追加することを示します。複数のグループを指定する場合は、グループ名のリストを丸かっこで囲み、各グループ名をスペースまたはカンマで区切ります。

nt

user-name を Windows データベースのグループに連結します。

operator

userName で指定されたユーザに GROUP-OPERATOR 属性を割り当てます。詳細については、「**管理者ガイド**」を参照してください。

operator-

ユーザから GROUP-OPERATOR 属性を削除します。

owner(*user-name* |*group-name*)

join レコードの所有者として eTrust Access Control ユーザまたはグループを示します。連結を作成するときに所有者を指定しなかった場合は、連結の作成者に連結の所有者権限が割り当てられます。

pwmanager

user-name に GROUP-PWMANAGER 属性を割り当てます。pwmanager- は、ユーザをグループに再度連結する際に、この属性を削除します。詳細については、「**管理者ガイド**」を参照してください。

user-name

group パラメータによって指定された 1 つまたは複数のグループに連結(または、新しいプロパティ セットを使用して再度連結)するユーザのユーザ名です。複数のユーザを指定する場合は、ユーザ名のリストをかっこで囲み、各ユーザ名をスペースまたはカンマで区切ります。*userName* は第 1 パラメータとして必ず入力する必要があります。

regular

ユーザの管理フラグをリセットします。

関連項目

この章の showusr コマンドおよび showgrp コマンドの説明。

例

- ユーザ Rory が、ユーザ Bob をグループ staff に追加するとします。
  - Rory に ADMIN 属性が割り当てられています。
  - 以下のデフォルト値が適用されます。
    - admin-
    - auditor-
    - owner(Rory)
    - pwmanager-

```
join Bob group(staff)
```

- ユーザ Rory が、グループ staff の Sue の定義を変更するとします。Sue には現在、GROUP-AUDITOR 属性が割り当てられていて、Rory が GROUP-PWMANAGER 属性を追加します。
- Rory に ADMIN 属性が割り当てられています。
  - 以下のデフォルト値が適用されます。
    - admin-
    - owner(Rory)

  ```
  join Sue group(staff) auditor pwmanager
  ```

  このコマンドを実行すると、以前のレコードは削除されます。Sue の以前の属性に関するレコードは保存されません。したがって、Rory は、Sue に必要となる 2 つの属性を指定する必要があります。
- ユーザ Bill が、グループ PAYROLL からユーザ sales25 および sales43 を削除するとします。
  - ユーザ Bill に ADMIN 属性が割り当てられています。

  ```
  join- (sales25 sales43) group(PAYROLL)
  ```

list

特定の環境に定義されているクラスを一覧表示します。

```
list
```

rename

データベースのオブジェクト名を変更します。古いオブジェクトのすべてのルールは、名前変更後のオブジェクトに適用されます。オブジェクトは新しい名前でしか認識されなくなります。

注: SEOS クラス、UACC クラス、および ADMIN クラスの名前は変更できません。

注: オブジェクト名の最大文字数は 255 文字です。eTrust Access Control では 256 文字以上の名前が付いたリソースを管理できません。この制限事項はネイティブ環境にも適用されます。

権限

rename コマンドを使用するには、実行対象のリソースに対して適切な権限を持っている必要があります。eTrust Access Control では、以下の条件がチェックされ、いずれか 1 つの条件が満たされるとチェックは終了します。

- ADMIN 属性が割り当てられていること。
- GROUP-ADMIN 属性が割り当てられているグループのスコープ内に目的のリソースレコードがあること。
- レコードの所有者であること。
- ADMIN クラスのリソース クラスのレコードの eTrust Access Control リストで、MODIFY アクセス権(chres の場合)または CREATE アクセス権(editres の場合)が割り当てられていること。

```
rename className oldresourceName newresourceName
```

className

オブジェクトが定義されているクラスです。

oldresourceName

オブジェクトの古い名前です。

newresourceName

オブジェクトの新しい名前です。古いオブジェクト名のすべてのルールは、名前変更後のオブジェクトに適用されます。

例

ユーザ ADMIN 1 が、Host クラスのレコードの名前を spree3 から spree4 に変更するとします。ADMIN1 には ADMIN 属性が割り当てられています。この場合は、以下のコマンドを実行できます。

```
rename host spree3 spree4
```

rmfile

rmfile は、データベースからファイルを削除するコマンドです。ファイルは、FILE クラスに属するリソース レコードです。

```
{rmfile | rf} file-name | (file-names ...)
```

file-name

削除するファイルの名前です。複数のファイルを削除する場合は、ファイル名のリストを丸かっこで囲み、各ファイル名をスペースまたはカンマで区切ります。

各ファイル レコードは個別に処理されます。ファイルの処理中にエラーが発生すると、メッセージが表示され、リストの次のファイルから処理が続行されます。

関連項目

この章の checklogin コマンド、editfile/newfile コマンド、および showfile コマンドの説明。

例

セキュリティ管理者が、ファイル C:¥temp¥passwords.txt に対する eTrust Access Control の保護機能を削除するとします。

- セキュリティ管理者に ADMIN 属性が割り当てられています。
- rmfile C:¥temp¥passwords.txt

rmgrp

rmgrp は、eTrust Access Control データベースおよび Windows データベースから 1 つまたは複数のグループを削除するコマンドです。

eTrust Access Control データベースでは、グループ ID は、使用されている場所によって、rmgrp コマンドで更新されない場合があります。これは、rmgrp コマンドの処理機能では、すべての場所にあるグループ ID が削除されないためです。たとえば、グループ ID がリソースのアクセス制御リスト内で使用されている場合、そのグループは不明とみなされます。

Windows では、各 SID(セキュリティ識別子)が一意であるため、グループを削除した場合、そのグループ アカウントの一意の識別子は存在しなくなります。同じ名前で新しいグループを作成しても、新しいグループには別の識別子が割り当てられます。したがって、新しいグループに以前のグループと同じアクセス権限およびその他の必要なプロパティを指定しない限り、以前のグループでアクセスできた対象にアクセスすることはできません。

アクセス制御リストからグループ ID を削除するには、authorize コマンドを実行します。

```
{rmgrp | rg}  group-name | (group-names ...) [nt]
```

group-name

削除する eTrust Access Control グループ レコードの名前を示します。複数のグループを削除する場合は、グループ名のリストを丸かっこで囲み、各グループ名をスペースまたはカンマで区切ります。

グローバル グループに対して、バージョン 4.1 の命名規則を使用している場合は、名前の先頭にチルダ(~)記号を付けます。

nt

削除する Windows グループを示します。

関連項目

この章の chgrp/editgrp/newgrp コマンド、showgrp コマンド、および join コマンドの説明。

例

ユーザ Joe が、eTrust Access Control データベースからグループ DEPT1 および DEPT2 を削除するとします。

- ユーザ Joe に SALES グループに対する GROUP-ADMIN 属性が割り当てられています。
- SALES グループは、グループ DEPT1 および DEPT2 を所有しています。

```
rmgrp (DEPT1 DEPT2)
```

rmres

rmres は、データベースからリソースを削除するコマンドです。rmres コマンドを使用して削除できるレコードは、ADMIN、CATEGORY、CONNECT、FILE、GHOST、GSUDO、GTERMINAL、HOST、HOSTNET、HOSTNP、SECFILE、SECLABEL、SUDO、SURROGATE、TERMINAL、PROGRAM、PROCESS、TCP、UACC の各クラスおよび任意のユーザ定義クラスに属しています。

```
{rmres | rr} class-name record-name | (record-names ...)
```

class-name

リソースが属するクラスの名前です。eTrust Access Control に定義されているリソース クラスを一覧表示するには、find コマンドを実行します。詳細については、この章の find コマンドの説明を参照してください。

record-name

削除するリソース レコードの名前です。複数のリソースを削除する場合は、リソース名のリストを丸かっこで囲み、各リソース名をスペースまたはカンマで区切ります。

各リソース レコードは個別に処理されます。リソースの処理中にエラーが発生すると、メッセージが表示され、リストの次のリソースから処理が続行されます。

関連項目

この章の chres/editres/newres コマンドおよび showres コマンドの説明。

例

ユーザ Admin1 が、データベースの TERMINAL クラスからレコード TERMS を削除するとします。

- ユーザ Admin1 に ADMIN 属性が割り当てられています。
- rmres TERMINAL TERMS

rmusr

rmusr は、データベースからユーザ レコードを削除し、グループ レコードにあるそのユーザ レコードへの参照をすべて削除することによって、eTrust Access Control および Windows からユーザを削除するコマンドです。必要に応じて、Windows データベースからもユーザを削除します。

ユーザのユーザ ID は、eTrust Access Control データベース内で定義されている場所によっては、rmusr コマンドで削除されない場合があります。たとえば、ユーザがグループまたは他のレコードの所有者である場合、またはユーザがリソースのアクセス制御リストに指定されている場合です。必要に応じて、chgrp、chusr、chres、および authorize の各コマンドを実行して、所有者権限を手動で変更し、削除するユーザ レコードに関連するアクセス権限を削除します。

Windows では、各 SID が一意であるため、ユーザを削除した場合は、そのユーザ アカウントに一意の識別子が存在しなくなります。同じ名前で新しいアカウントを作成しても、新しいアカウントには別の識別子が割り当てられます。このため、新しいアカウントに以前のアカウントと同じアクセス許可およびその他の必要なプロパティを指定しない限り、以前のアカウントでアクセスできた対象にアクセスすることはできません。

```
{rmusr | ru} user-name | (user-names ...) [nt]
```

user-name

ユーザ レコードの名前です。複数のユーザ レコードを削除する場合は、ユーザ名のリストを丸かっこで囲み、各ユーザ名をスペースまたはカンマで区切ります。

nt

eTrust Access Control からだけでなく、Windows 環境からもユーザを削除します。

関連項目

この章の chusr/editusr/newusr コマンドおよび showusr コマンドの説明。

例

ユーザ admin が eTrust Access Control からユーザ TerryS を削除するとします。

- ユーザ TerryS が eTrust Access Control に定義されています。
- rmusr TerryS

ruler

ruler は、showusr、showgrp、showres、または showfile の各コマンドの実行時に、eTrust Access Control で表示するプロパティを定義するコマンドです。デフォルトでは、クラスの電子署名以外のすべてのプロパティが表示されます。このコマンドを使用すると、必要なプロパティのみを表示できます。

ruler コマンドは、現在のセッションのホストにのみ適用され、現在のセッションのすべてのホストのルーラが表示されます。各ホストのプロパティは、個別のリストに表示されます。ホストを変更した場合、ruler コマンドで新しいホストのプロパティの表示は変更されません。

このコマンドの実行時にプロパティを 1 つも入力しなかった場合は、現在のルーラにあるプロパティの名前が表示されます。

権限

このコマンドを発行できるのは、以下のユーザのみです。

- ADMIN 属性、AUDITOR 属性、または OPERATOR 属性を持つユーザ。
- ルーラを設定する対象のクラスに対する読み取りアクセス権限が ADMIN クラスに定義されているユーザ。たとえば、TERMINAL クラスを表すレコードに対する読み取りアクセス権限が ADMIN クラスに定義されているユーザは、TERMINAL クラスのルーラを設定できます。

```
ruler class-name [props(all | list-of-property-names)]
```

class-name

表示を変更するクラスの名前です。

props()

表示するプロパティを示します。

- all - クラスのすべてのプロパティを表示することを示します。
- list-of-property-names - 表示する 1 つまたは複数の eTrust Access Control のプロパティの名前を示します。複数のプロパティを指定する場合は、プロパティ名のリストを丸かっこで囲み、各プロパティ名をスペースまたはカンマで区切ります。

関連項目

この章の showfile コマンド、showgrp コマンド、showres コマンド、および showusr コマンドの説明。

例

- ユーザ admin が、所有者、および変更が通知されるユーザという 2 つのプロパティのみを表示するように設定するとします。

  - クラス USER が eTrust Access Control に定義されています。

  ```
  ruler USER props(NOTIFY OWNER)
  ```

- ユーザ admin が、クラス USER に対する現在のルーラのプロパティを表示するとします。

  - クラス USER が eTrust Access Control に定義されています。

  ```
  ruler USER
  ```

- ユーザ admin が、eTrust Access Control のルーラの設定をデフォルトに戻す、つまり USER クラスのすべてのプロパティを表示するとします。

  - クラス USER が eTrust Access Control に定義されています。

  ```
  ruler USER props(all)
  ```

search

この章の find コマンドの説明を参照してください。

setoptions

setoptions は、リソースの保護に関連したシステム全体の eTrust Access Control オプションを動的に設定するコマンドです。たとえば、setoptions を使用すると、クラス単位またはシステム全体の全クラスに対するセキュリティ チェックの有効化または無効化、パスワード ポリシーの設定、および eTrust Access Control オプションの現在の設定値の一覧表示などができます。

setoptions コマンドでは、通常、パラメータを指定してコマンドを実行するために ADMIN 属性が必要です。ただし、AUDITOR 属性のみを持つユーザ、または OPERATOR 属性のみを持つユーザでも、list パラメータを指定して setoptions コマンドを実行できます。

```
{setoptions | so}
 [{class+|class-}(class-name...)]
        class-name には、SECLEVEL、PASSWORD、またはデータベース内の有効なリソース
        クラスを指定できます。
        list コマンドを使用すると、データベース内のすべてのクラスが一覧表示されます。
 [accgrr | accgrr-]
 [accpacl | accpacl-]
 [{cng_adminpwd | cng_adminpwd-}]
 [{cng_ownpwd | cng_ownpwd-}]
 [dms{+|-}(<dms@hostname>)] ¥
 [inactive(num-inactive-days) | inactive-]
 [is_dms{+|-}] ¥
 [maxlogins(maximum-number-of-logins) | maxlogins-]
 [password(
        [history(number-stored-passwords) | history-]
        [interval(maximum-password-change-interval) | interval-]
        [min_life(minimum-password-change-interval) | min_life-]
        [rules(
                [alpha(minimum-alpha-characters)]
                [alphanum(minimum-alphanumeric-characters)]
                [grace(number-of-grace-logins)]
                [min_len(minimum-password-length)]
                [max_len(maximum-password-length)]
                [lowercase(minimum-lowercase-characters)]
                [max_rep(max-repetitive-characters)]
                [namechk | namechk-]
                [numeric(minimum-numeric-characters)]
                [oldpwchk | oldpwchk-]
                [special(minimum-special-characters)]
                [uppercase(minimum-uppercase-characters)]
                [use_dbdict | use_dbdict-]
                [bidirectional | bidirectional-]
                [prohibited(prohibited-characters)]
        )]
        [rules-]
 [use_dma{+|-}] ¥
```

)]
または
setoptions list | tngclslist

accgrr

複数のグループに属するユーザの権限が、属しているグループのすべての権限全体と同じになることを示します。ただし、いずれかのアクセス タイプが NONE の場合は、NONE が常に他のグループのアクセス タイプよりも優先されます。eTrust Access Control をインストールすると、このプロパティの値は yes に設定されます。

accgrr-

アクセス権限のチェック時に、ユーザのグループ権限を蓄積**せず**、その代わり最初にチェックするグループのアクセス タイプをユーザに割り当てることを示します。ただし、いずれかのアクセス タイプが NONE の場合は、NONE が常に他のグループのアクセス タイプよりも優先されます。

accpacl

各プログラムに関連付けられたアクセス タイプに応じて特定のリソースを実行できるアクセサおよびプログラムを示します。

ユーザのアクセス権が ACL で明示的に指定されている場合は、そのアクセス権が許可されるアクセス権となります。アクセス権が ACL で明示的に指定されていない場合、または NONE 以外のアクセス権が指定されている場合は、PACL での指定と ACL での指定を組み合わせたアクセス ルールが適用されます。

accpacl-

ACCPACL を無効にします。ACCPACL がアクティブでない場合、ユーザのアクセス権が ACL で明示的に指定されているときは、そのアクセス権が許可されるアクセス権になります。ACL で明示的にアクセス権が指定されていない場合、許可されるアクセス権は、PACL のアクセス権に従います。

class+(*class-name*)

1 つまたは複数の eTrust Access Control クラスを有効にします。eTrust Access Control でクラスのリソースを保護するためには、クラスが有効であることが必要です。GROUP、SECFILE、SEOS、UACC、および USER 以外のすべてのクラスを示します。これらの保護されているクラスは無効にできません。クラスの有効化は、クラスに属するリソースへのアクセスを許可するために必要なレコードを定義した後に行う必要があります。eTrust Access Control で提供されるリソース クラスの詳細については、「**管理者ガイド**」を参照してください。

以下のいずれかの値を使用して、*class-name* 引数をすべて大文字で指定します。

- eTrust Access Control クラスの名前です。
- SECLEVEL（セキュリティ レベルのチェックを有効にします）
- PASSWORD（パスワード品質のチェックを有効にします）

class-(*class-name*)

1 つまたは複数の eTrust Access Control クラスを無効にします。無効なクラスに属するリソースは保護されません。以下のいずれかの値を使用して、*class-name* 引数をすべて大文字で指定します。

- eTrust Access Control クラスの名前です。
- SECLEVEL（セキュリティ レベルのチェックを無効にします）
- PASSWORD（パスワード品質のチェックを無効にします）

class-name 引数は、**すべて大文字で入力**する必要があります。

cng_adminpwd

PWMANAGER 属性を持つユーザが ADMIN ユーザのパスワードを変更できるようにします。

cng_adminpwd-

PWMANAGER 属性を持つユーザが ADMIN ユーザのパスワードを変更できないようにします。これがデフォルトの設定です。

cng_ownpwd

ユーザが selang を使用して自分のパスワードを変更できるようにします。

cng_ownpwd-

ユーザが selang を使用して自分のパスワードを変更できないようにします。これがデフォルトの設定です。

dms{+|-}(*<dms@hostname>*)

このデータベースの DMS データベースのリストに DMS データベースを追加するか、リストから DMS データベースを削除します。

inactive(*num-inactive-days*)

ユーザ ログインを一時停止するまでの非アクティブ状態の日数を示します。非アクティブ状態の日とは、ユーザがログインできない日を指します。正の整数を入力します。inactive を 0 に設定した場合は、inactive- パラメータを使用した場合と同じ結果になります。

inactive-

非アクティブ ログイン チェックを無効にします。

is_dms+

現在のデータベースを DMS として指定します。

is_dms-

現在のデータベースの DMS としての指定を解除します。

list

パスワード ポリシーの現在の値を表示します。

maxlogins(*maximum-number-of-logins*)

ユーザが同時にログインできる端末台数のデフォルトの最大値を設定します。値 0 (ゼロ)は、最大値が指定されないため、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。

注: maxlogins を 1 に設定すると、selang を実行できません。この場合、eTrust Access Control をシャットダウンし、maxlogins 設定を 2 以上の値に変更して、eTrust Access Control を再起動する必要があります。

ユーザのユーザ レコードに値を指定すると、この値よりも優先されます。

maxlogins-

グローバルな最大ログイン回数のチェックを無効にします。ユーザ レコードでログインが制限されていない限り、ユーザがログインできる端末の台数は無制限となります。

password

パスワード オプションを設定します。

history(*number-stored-passwords*)

データベースに保存するパスワード履歴の数を示します。新しいパスワードの作成時、ユーザは履歴リストに保存されているパスワードを指定できません。
number-stored-passwords は 1 から 24 までの整数です。0 を指定した場合、パスワードは保存されません。

history-

パスワード履歴のチェックを無効にします。

interval(*maximum-password-change-interval*)

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。

maximum-password-change-interval の値には、正の整数または 0 を指定します。期間を 0 に設定すると、ユーザに対するパスワード期間のチェックは無効になります。パスワードに有効期限を設定しない場合は、interval を 0 に設定します。

interval-

パスワード期間の設定を取り消します。

min_life(*minimum-password-change-interval*)

変更したパスワードを再度変更できるようになるまでの最短日数を設定します。*minimum-password-change-interval* の値には、正の整数を指定します。

min_life-

パスワード変更後、再度変更できるようになるまでの最短日数の設定を無効にします。

rules

新しいパスワードの品質をチェックする際に使用される 1 つまたは複数のパスワード ルールを設定します。ルールは以下のとおりです。

- alpha(minimum-alpha-characters) - 新しいパスワードで使用する必要がある英字の最低文字数を設定します。整数を入力します。
- alphanum(minimum-alphanumeric-characters) - 新しいパスワードで使用する必要がある英字の最低文字数を設定します。整数を入力します。
- bidirectional - 双方向パスワード暗号化を有効にします。双方向パスワード暗号化が有効になっている場合、新しいパスワードはすべて暗号化され、クリアテキストに復号化できるようになります。この暗号化によって、新しいパスワードと古いパスワード(パスワード履歴)を広範囲にわたって比較できます。

  注(UNIX/Linux の場合): この機能を使用するには、トークンのパスワード形式を NT に設定する必要があります。
- bidirectional- - 双方向パスワード暗号化を無効にします。双方向暗号化を無効にすると、一方向のパスワード履歴暗号化が有効になり、古いパスワードを復号化できなくなります。
- grace(number-of-grace-logins) - ユーザのログインが一時停止になるまでに許可される最大猶予ログイン回数を設定します。猶予ログイン回数には、0 から 255 までの値を指定する必要があります。

  min_len(minimum-password-length) - パスワードの最低文字数を設定します。新しいパスワードで使用する必要がある文字の合計最低文字数を入力します。
- max_len(maximum-password-length) - パスワードの最大文字数を設定します。新しいパスワードで使用する必要がある文字の合計最大文字数を入力します。
- lowercase(minimum-lowercase-characters) - 新しいパスワードで使用する必要がある小文字の最低文字数を設定します。整数を入力します。
- max_rep(max-repetitive-characters) - 新しいパスワードで使用する必要がある反復文字の最大文字数を設定します。整数を入力します。
- namechk - パスワードにユーザ名の一部または全部が含まれているかどうかをチェックします。デフォルトでは、このチェックが実行されます。
- namechk- - このチェックを無効にします。

- numeric(minimum-numeric-characters) - 新しいパスワードで使用する必要がある数字の最低文字数を設定します。整数を入力します。
- oldpwchk - 新しいパスワードに古いパスワードの一部分または全部が含まれているかどうかをチェックします。デフォルトでは、このチェックが実行されます。
- oldpwchk- - このチェックを無効にします。
- prohibited(prohibited-characters) - パスワードで使用できない文字を示します。禁止文字を入力します。
- special(minimum-special-characters) - 新しいパスワードで使用する必要がある特殊文字の最低文字数を設定します。整数を入力します。
- uppercase(minimum-uppercase-characters) - 新しいパスワードで使用する必要がある大文字の最低文字数を設定します。整数を入力します。
- use_dbdict | use_dbdict- - パスワード辞書を設定します。use_dbdict は、トークンを db に設定し、eTrust Access Control データベース内の単語とパスワードを比較します。use_dbdict- は、トークンを file に設定し、UNIX/Linux の場合は seos.ini ファイルとパスワードを照合し、Windows の場合は Windows レジストリのファイルとパスワードを照合します。

rules-

パスワード品質のチェックを無効にします。rules 引数で指定したルールは、パスワード品質のチェックに使用されません。

use_dma{+|-}

コンピュータに DMA がインストールされているかどうかを示します。

例

ユーザ Mike が、6 文字以上のパスワードをユーザに選択させるパスワード ポリシーを設定するとします。さらに、パスワード ポリシーの適用を有効にするとします。

- ユーザ Mike に ADMIN 属性が割り当てられています。

```
setoptions password(rules(length(6)))
```

showfile

showfile は、ファイルのプロパティを表示するコマンドです。

権限

標準アクセス権限に加えて、以下の条件を 1 つでも満たしていれば、showfile コマンドを実行できます。

- AUDITOR 属性または OPERATOR 属性のいずれかが割り当てられています。
- ファイルを所有するグループまたはファイルを所有するグループの親グループで GROUP-AUDITOR 属性が割り当てられています。
- ADMIN クラスの FILE クラス レコードを表すオブジェクトのアクセス制御リストに読み取り権限が割り当てられています。

注:

- showfile コマンドは、ファイル レコードのすべてのプロパティを一覧表示します。

eTrust Access Control では、各レコードを個別に処理し、十分な権限を持つリソースに対してのみ情報を表示します。

```
{showfile | sf} fileName ¥
        [addprops(propName)] ¥

        [next] ¥
        [props(all | propName)] ¥
        [useprops(propName)] ¥
    [nt]
```

addprops(*propName*)

プロパティ名の一覧です。表示するプロパティ(ルーラ)を設定します。プロパティのリストは現在のルーラに追加されます。ルーラは、現在のクエリに対してのみ設定され、現在のクエリが終了すると前のルーラ設定に戻ります。

fileName

一覧表示するプロパティが含まれているファイル レコードの名前です。複数のファイルのプロパティを一覧表示する場合は、ファイル名のリストを丸かっこで囲み、各ファイル名をスペースまたはカンマで区切ります。

名前パターンを指定すると、指定したパターンに一致するすべてのファイルのプロパティを一覧表示できます。

各ファイル レコードは個別に処理されます。ファイルの処理中にエラーが発生すると、メッセージが表示され、リストの次のファイルから処理が続行されます。

next(*propName*)

要求されたデータの一部を表示します。このオプションは、設定されているクエリ サイズよりもクエリ データが大きい場合に役に立ちます。

クエリの最大サイズは、seos.ini ファイルの lang セクションで設定する query_size トークンによって決まります。デフォルトのクエリ サイズは 100 に設定されています。

nt

eTrust Access Control のプロパティおよび Windows のファイル属性を表示します。

props(all|*propName*)

表示するプロパティ(ルーラ)を設定します。

設定したルーラは将来のクエリにも有効です。

useprops(*propName*)

表示するプロパティ(ルーラ)を設定します。現在のルーラは無視されます。ルーラは現在のクエリに対してのみ設定されます。

関連項目

この章の checklogin コマンド、newfile コマンド、および rmfile コマンドの説明。

例

- ユーザ Lyn が、ファイル レコード d:¥winnt35¥win.ini のプロパティを一覧表示するとします。

  - ユーザ Lyn に ADMIN 属性が割り当てられています。

  ```
  showfile D:¥winnt35¥win.ini
  ```

showgrp

showgrp は、グループ レコードのすべての eTrust Access Control プロパティの設定を表示するコマンドです。Windows プロパティも表示されます(オプション)。

権限

標準アクセス権限以外に、以下の条件を 1 つ以上満たしていれば、showusr コマンドを実行することができます。

- AUDITOR 属性または OPERATOR 属性のいずれかが割り当てられています。
- 一覧表示する各グループで GROUP-AUDITOR 属性が割り当てられているか、一覧表示する各グループが GROUP-ADMIN 属性が割り当てられているグループのスコープ内にあります。
- ADMIN クラスの GROUP クラス レコードを表すオブジェクトのアクセス制御リストに読み取り権限が割り当てられています。

```
{showgrp | sg} groupName ¥
        [addprops(propName)] ¥
        [next] ¥
        [props(all | propName)] ¥
        [useprops(propName)] ¥

        [nt]
```

addprops(*propName*)

プロパティ名のリストです。

表示するプロパティ(ルーラ)を設定します。プロパティのリストは現在のルーラに追加されます。ルーラは、現在のクエリに対してのみ設定され、現在のクエリが終了すると前のルーラ設定に戻ります。

groupName

一覧表示するプロパティが含まれているグループの名前です。複数のグループのプロパティを一覧表示する場合は、グループ名のリストを丸かっこで囲み、各グループ名をスペースまたはカンマで区切ります。共通の名前パターンを持つ複数のグループを識別するマスクを指定できます。eTrust Access Control のすべてのグループ レコードに保存されている情報を一覧表示するには、アスタリスク(*)を指定します。

名前に特殊文字またはスペースが含まれている 1 つのグループのプロパティを表示するには、特殊文字またはスペースの前に円記号(¥)を入力します。

next

要求されたデータの一部を表示します。このオプションは、設定されているクエリ サイズよりもクエリ データが大きい場合に役立ちます。

クエリの最大サイズは、seos.ini ファイルの lang セクションで設定する query_size トークンによって決まります。デフォルトのクエリ サイズは 100 に設定されています。

nt

データベースのプロパティおよびローカル Windows システムのグループの詳細情報を表示します。

props(all|*propName*)

表示するプロパティ(ルーラ)を設定します。設定したルーラは将来のクエリにも有効です。

useprops(*propName*)

表示するプロパティ(ルーラ)を設定します。現在のルーラは無視されます。ルーラは現在のクエリに対してのみ設定されます。

関連項目

この章の chgrp/editgrp/newgrp コマンドおよび rmgrp コマンドの説明。

例

- root ユーザが、セキュリティ グループのプロパティを表示するとします。
  - root ユーザにセキュリティ グループの GROUP-ADMIN 属性が割り当てられています。

```
showgrp security
```

- ユーザ admin がすべての eTrust Access Control グループのプロパティを表示するとします。
  - ユーザ admin に ADMIN 属性および AUDITOR 属性が割り当てられています。

```
showgrp *
```

showres

showres は、データベースのクラスに属するリソースのプロパティを表示するコマンドです。

showres コマンドを実行して一覧表示できるクラスは、ADMIN、CATEGORY、CONNECT、FILE、GHOST、GSUDO、GTERMINAL、HOST、HOSTNET、HOSTNP、SECFILE、SECLABEL、SUDO、SURROGATE、TERMINAL、PROGRAM、PROCESS、TCP、UACC の各クラスおよび任意のユーザ定義クラスです。

権限

標準アクセス権限以外に、以下の条件を 1 つ以上満たしていれば、showusr コマンドを実行することができます。

- AUDITOR 属性または OPERATOR 属性のいずれかが割り当てられています。
- リソースを所有するグループまたはリソースを所有するグループの親グループで GROUP-AUDITOR 属性が割り当てられています。
- ADMIN クラスで、目的のリソース クラス レコードを表すオブジェクトのアクセス制御リストに読み取り権限が割り当てられています。

注:

- showres は、既存のリソースまたはリソース グループ レコードのすべてのプロパティを一覧表示するコマンドです。eTrust Access Control の各クラスのすべてのプロパティのリストについては、このマニュアルの「eTrust 環境のクラスとプロパティ」の章を参照してください。

  Windows のリソース タイプのすべてのプロパティのリストについては、このマニュアルの「Windows 環境のクラスとプロパティ」の章を参照してください。
- eTrust Access Control では、各リソースを個別に処理し、適切な権限を持つリソースに対してのみ情報を表示します。

```
{showres | sr} className resourceName ¥
        [addprops(propName)] ¥

        [next] ¥
        [props(all | propName)] ¥
        [useprops(propName)]
```

addprops(*propName*)

表示するプロパティ(ルーラ)を設定します。プロパティのリストは現在のルーラに追加されます。ルーラは、現在のクエリに対してのみ設定され、現在のクエリが終了すると前のルーラ設定に戻ります。

className

リソースが属するクラスの名前です。eTrust Access Control に定義されているリソース クラスを一覧表示するには、find コマンドを実行します。詳細については、この章の find コマンドの説明を参照してください。

next

要求されたデータの一部を表示します。このオプションは、設定されているクエリ サイズよりもクエリ データが大きい場合に役に立ちます。

クエリの最大サイズは、seos.ini ファイルの lang セクションで設定する query_size トークンによって決まります。デフォルトのクエリ サイズは 100 に設定されています。

props(all|*propName*)

表示するプロパティ(ルーラ)を設定します。設定したルーラは将来のクエリにも有効です。

resourceName

一覧表示するプロパティが含まれているリソース レコードの名前です。複数のリソースのプロパティを一覧表示する場合は、リソース名のリストを丸かっこで囲み、各リソース名をスペースまたはカンマで区切ります。

名前パターンを指定すると、指定したパターンに一致するすべてのリソースのプロパティを一覧表示できます。指定したクラスに定義されているすべてのリソースのプロパティを表示するには、アスタリスク(*)を指定します。名前に特殊文字またはスペースが含まれている 1 つのリソースのプロパティを表示するには、特殊文字またはスペースの前に円記号(¥)を入力します。

各リソース レコードは個別に処理されます。リソースの処理中にエラーが発生すると、メッセージが表示され、リストの次のリソースから処理が続行されます。

useprops(*propName*)

表示するプロパティ(ルーラ)を設定します。現在のルーラは無視されます。ルーラは現在のクエリに対してのみ設定されます。

関連項目

この章の chres/editres/newres コマンドおよび rmres コマンドの説明。

例

ユーザ Admin1 が、TERMINAL クラスのレコードのうち、マスク ath* に名前が一致するレコードのプロパティを一覧表示するとします。

- ユーザ Admin1 に ADMIN 属性および AUDITOR 属性が割り当てられています。

```
showres TERMINAL ath*
```

showusr

showusr は、eTrust Access Control ユーザ レコードに保存されているすべてのプロパティの値を一覧表示するコマンドです。*userName* も *mask* も指定せずに showusr コマンドを実行した場合は、自分のユーザ レコードの情報が一覧表示されます。

権限

標準アクセス権限以外に、以下の条件を 1 つ以上満たしていれば、showusr コマンドを実行することができます。

- AUDITOR 属性または OPERATOR 属性のいずれかが割り当てられています。
- ユーザ レコードを所有するグループまたはユーザ レコードを所有するグループの親グループで GROUP-AUDITOR 属性が割り当てられています。
- ADMIN クラスの USER クラス レコードを表すオブジェクトのアクセス制御リストに読み取り権限が割り当てられています。

```
{showusr | su} userName ¥
        [addprops(propName)] ¥
        [next] ¥
        [props(all | propName)] ¥
        [useprops(propName)] ¥
    [nt]
```

addprops(*propName*)

表示するプロパティ(ルーラ)を設定します。プロパティのリストは現在のルーラに追加されます。ルーラは、現在のクエリに対してのみ設定され、現在のクエリが終了すると前のルーラ設定に戻ります。

userName

ユーザ レコードの名前です。複数のユーザ レコードのプロパティを一覧表示する場合は、ユーザ名のリストを丸かっこで囲み、各ユーザ名をスペースまたはカンマで区切ります。名前に特殊文字またはスペースが使用されている 1 つのユーザのプロパティを表示するには、特殊文字またはスペースの前に円記号(¥)を入力します。

名前パターンを指定すると、同様のレコード名を持つユーザのグループを指定できます。たとえば、名前が A で始まるすべてのユーザを一覧表示するには、「A*」と指定します。

nt

データベースのプロパティおよびローカル Windows システムのユーザの詳細情報を表示します。

props(all|*propName*)

表示するプロパティ(ルーラ)を設定します。設定したルーラは将来のクエリにも有効です。

useprops(*propName*)

表示するプロパティ(ルーラ)を設定します。現在のルーラは無視されます。ルーラは現在のクエリに対してのみ設定されます。

例

- root ユーザが、Robin のユーザ レコードのプロパティを一覧表示するとします。
  - ユーザ Robin が eTrust Access Control に定義されています。
  - UserName=root (*showusr コマンドを実行するユーザのユーザ名*)

  ```
  showusr Robin
  ```

- root ユーザが、ユーザ Robin および Leslie のユーザ プロパティを一覧表示するとします。
  - root ユーザに ADMIN 属性および AUDITOR 属性が割り当てられています。

  ```
  showusr (Leslie, Robin)
  ```

関連項目

この章の chusr/editusr/newusr コマンドおよび rmusr コマンドの説明。

source

source は、ファイルに記述された 1 つまたは複数の selang のコマンドを実行できるコマンドです。eTrust Access Control は指定されたファイルを読み取り、コマンドを実行して、selang のプロンプトを返します。eTrust Access Control データベースに定義されているすべてのユーザがこのコマンドを実行できます。

このコマンドは、UNIX/Linux の csh および tcsh の source コマンドと同様のコマンドです。

source *fileName*

fileName

selang のコマンドが保存されているファイルの名前です。

例

ユーザ admin が、initf1 というファイル内のコマンドを実行する場合は、以下のコマンドを入力します。

```
source initf1
```

start devcalc

start devcalc コマンドは、ポリシー偏差計算を開始し、偏差ステータスを送信します。偏差データは、ローカル ポリシー偏差データ ファイル(deviation.dat)に格納され、ポリシー偏差ステータスは、少なくとも 1 つの DMS データベース(121 ページ)に送信されます。実際の偏差データを取得するには、get devcalc コマンド(104 ページ)を実行する必要があります。

注: ポリシー偏差計算の詳細については、「**管理者ガイド**」を参照してください。

start devcalc コマンドを実行するには、コンピュータに対する端末アクセス権と DEVCALC サブ管理クラスに対する実行アクセス権を持っている必要があります。

```
start devcalc [params("-pn name#xx -dms dms@hostname -strict")]
```

-pn *name#xx*

(オプション)偏差計算機能で計算の対象とするポリシー オブジェクト(ポリシー名とバージョン番号)のカンマ区切りリストを示します。ポリシーが指定されていない場合は、ローカル ホストに展開されているすべてのポリシーの偏差が計算されます。

-dms *dms@hostname*

(オプション)ポリシー偏差ステータスの結果の送信先とする DMS データベースのカンマ区切りリストを示します。DMS が指定されていない場合は、ローカル eTrust Access Control データベースに対して指定されている DMS リストが使用されます。

-strict

(オプション)ローカル HNODE オブジェクトに関連付けられたポリシーと、使用可能な最初の DMS 上の HNODE オブジェクトに関連付けられたポリシーを比較します。

通常、偏差計算機能はローカル ホスト上でのみ偏差をチェックします。このオプションを指定すると、偏差計算機能では、ローカル ポリシーと、リストの最初の DMS にあるポリシーも比較されます。比較される内容は以下のとおりです。

1. ローカル ホストを表す HNODE オブジェクトに関連付けられたポリシーのリスト。
2. HNODE オブジェクトに関連付けられた各 POLICY オブジェクトのポリシーのステータス。
3. HNODE オブジェクトに関連付けられた各 POLICY オブジェクトのポリシーのシグネチャ。

偏差計算の結果を検証する必要がある場合は、このオプションを使用します。

注: 偏差計算を多数のエンドポイントで同時に実行している場合は、DMS の負荷が大きくなります。DMS リストを使用するようにエンドポイントを設定するか、階層を複数の小さな階層に分割して、分割後の階層内でこのオプションを使用することをお勧めします。

例: 特定のポリシーに関するポリシー偏差計算の開始

以下の例では、start devcalc コマンドを使用して、myPolicy というポリシーの 2 番目のバージョンに関するポリシー偏差を計算し、ローカル eTrust Access Control データベースで指定されている DMS リストに偏差ステータスを送信する方法を示します。

```
eTrustAC> start devcalc params("-pn myPolicy#02")
```

第 3 章: Windows 環境の selang のコマンド

このセクションには、以下のトピックが含まれます。

Windows 環境での作業

この章では、Windows(ネイティブ)環境で使用できる selang のすべてのコマンドをアルファベット順に示します。Windows 環境では、selang のコマンドを使用して、ローカル Windows ホストに対してユーザやグループを追加、削除、変更、および一覧表示します。また、Windows のファイル アクセス許可(NTFS ファイル システムのみ)や所有者権限の設定を変更したり一覧表示したりすることもできます。selang の他の環境についての一般情報、ヘルプの表示方法、コマンド構文、およびコマンドの全体的な構成については、「selang – eTrust AC のコマンド言語」の章を参照してください。

Windows のコマンド リファレンス

このセクションでは、Windows 環境で使用できるすべての selang のコマンドをアルファベット順に示します。

authorize

authorize は、特定のリソースへのアクセスを許可されているユーザおよびグループのリストを管理するコマンドです。authorize コマンドを使用すると、ユーザまたはグループのリストを以下のように変更できます。

- 特定の eTrust Access Control ユーザまたはグループのリソースへのアクセスを許可します。
- 特定の eTrust Access Control ユーザまたはグループのリソースへのアクセスをブロックします。
- 特定のユーザまたはグループのリソースへのアクセス権限レベルを変更します。

authorize- は、標準アクセス制御リストからアクセサを削除することによって、リソースへのアクセス権を取り消すコマンドです。このコマンドを実行すると、特定のリソースに対するアクセサのアクセス権はデフォルトのアクセス権のみになります。

アクセス制御リストに対応している Windows 環境のクラスは以下のとおりです。これらのクラスは、authorize コマンドを使用して制御できます。

- COM
- DISK
- FILE
- PRINTER
- REGKEY
- SHARE

上記リストにないクラスは、アクセス制御リストがないため authorize コマンドで制御できません。

```
{authorize | auth} className resourceName ¥
        access(accessValue)              ¥
        [gid(groupName, ...) ]           ¥
        [uid(userName, ...)]

authorize | auth} className resourceName  ¥
        [deniedaccess(accessvalue)]

{authorize- | auth-} className resourceName       ¥
        [gid(groupName, ...) ]           ¥
        [uid(userName, ...)]
```

access(*accessValue*)

uid パラメータまたは gid パラメータに指定したアクセサに対して設定する、リソースへのアクセス権を示します。

accessValue の有効な値は、リソースのタイプによって異なります。

- COM および DISK - all、change、changePermissions、delete、none、read、takeOwnership、および write
- FILE - all、change、chmod、chown、control、delete、execute、none、read、sec、write、および update

  注: FILE リソースでアクセス権限を定義できるのは NTFS ファイルのみです。FAT ファイルにはアクセス権限を定義できません。
- PRINTER - all、none、manage、および print
- REGKEY - all、append、chown、create、delete、enum、link、manage、none、notify、query、read、readcontrol、sec、set、subkey、および write
- SHARE - all、change、read、および none

className

resourceName が属するクラスの名前を示します。

deniedaccess(*accessvalue*)

uid パラメータまたは gid パラメータに指定したアクセサに対して設定する、リソースへのアクセス禁止を示します。

拒否できる *accessvalue* は、all、create、delete、join、modify、none、password、および read です。

注: *accessValue* は authorize コマンドのみで使用できます。authorize- コマンドでは使用できません。

gid(*groupName*)

リソースへのアクセス権を設定する対象の 1 つまたは複数の Windows グループを示します。*groupName* の値は、1 つまたは複数の Windows グループの名前を表します。複数のグループを指定する場合は、各グループ名をスペースまたはカンマで区切ります。

resourceName

変更または追加するリソース レコードの名前です。複数のリソースを変更または追加する場合は、リソース名のリストを丸かっこで囲み、各リソース名をスペースまたはカンマで区切ります。少なくとも 1 つのリソース名を指定する必要があります。

eTrust Access Control では、指定したパラメータに従って、各リソース レコードが個別に処理されます。リソースの処理中にエラーが発生すると、メッセージが表示され、リストの次のリソースから処理が続行されます。

uid(*userName*)

リソースへのアクセス権限を設定する Windows ユーザを示します。 *userName* は、1 人または複数の Windows ユーザのユーザ名を表します。複数のユーザを指定する場合は、各ユーザ名をスペースまたはカンマで区切ります。Windows に定義されているすべてのユーザを指定する場合は、*userName* にアスタリスク(*)を指定します。

chfile / editfile

chfile と editfile は同じコマンドです。どちらのコマンドも FILE クラスの 1 つまたは複数のレコードを変更します。

NTFS ファイル システムの場合

```
{chfile | cf | editfile | ef} fileName | (fileNames...)     ¥
        [attrib(attributeValue)]          ¥
        [attrib(-attributeValue)]
        [defaccess(accessValue)]          ¥
        [owner(userName or groupName)]
```

FAT ファイル システムの場合

```
{chfile | cf | editfile | ef} fileName | (fileNames...)     ¥
        [attrib(attributeValue)]          ¥
        [attrib(-attributeValue)]
```

attrib(*attributeValue*)

ファイルの特性を決定する一連の属性を示します。*value* 引数の前にマイナス記号(-)を付けた場合は、属性が削除されます。Windows のファイル属性の一覧については、付録「Windows の値」を参照してください。

defaccess(*accessValue*)

ネイティブ セキュリティが組み込まれているグループ Everyone に対するアクセス権限を示します。すべてのシステム ユーザは Everyone グループのメンバです。Everyone グループにアクセス権を与えると、認証されたすべてのユーザだけではなく、すべての潜在的な匿名ユーザもアクセスできるようになります。

注: eTrust Access Control 環境で定義されたオブジェクトの defaccess には、別の意味があります。この場合、デフォルトのアクセス権限とは、リソースの eTrust Access Control のリストに含まれていないアクセサがリソースへのアクセス要求をした場合に与えられる権限のことです。また、デフォルトのアクセス権限は、eTrust Access Control で定義されていないユーザにも適用されます。

defaccess パラメータは、NTFS ファイル システムにのみ適用されます。

owner(*userName*|*groupName*)

ファイル レコードの所有者としてユーザまたはグループを割り当てます。ファイル レコードの所有者には、ファイルに対する無制限のアクセス権が与えられます。ファイルの所有者は、ファイル レコードを常時更新または削除することができます。

包括的なファイル保護

包括的なファイル保護により、正規表現で指定したファイル名のパターンに一致するすべてのファイルに対し、特定のアクセス ルールを適用できます。包括的なアクセス ルールとは、ワイルドカードを使用したパターンに名前が一致するすべてのファイル リソースを保護するルールです。リソースが複数の包括的なアクセス ルールに一致する場合は、リソースに最も厳密に一致するルールが eTrust Access Control によって選択されます。

包括的なファイル保護を使用すると、ほんのわずかなセキュリティ ルールを定義するだけで、Windows システム内で保護を必要とする多数のファイルを保護できます。

ただし、以下のパターンは*使用できません*。

- ¥*
- ¥tmp¥*
- ¥etc¥*

注: 複数のファイル名が指定された場合は、指定されたパラメータに基づいて各ファイル レコードが個別に処理されます。ファイルの処理中にエラーが発生すると、メッセージが表示され、リストの次のファイルから処理が続行されます。

関連項目

この章の showfile コマンドの説明。

chgrp / editgrp / newgrp

newgrp は、新しいグループのレコードを Windows データベースに追加することによって、新しい Windows グループを定義するコマンドです。

chgrp は、Windows グループの定義を変更するコマンドです。グループが eTrust Access Control に対しても定義されている場合は、chgrp コマンドを使用して eTrust Access Control でのグループの定義を変更できます。chgrp コマンドは一度に複数のグループの定義を変更できます。

editgrp は、newgrp コマンドと同様にデータベースに新しいグループを追加するか、chgrp コマンドと同様に既存の Windows グループの定義を変更するコマンドです。

複数のグループを定義する場合、または複数グループのプロパティを変更する場合は、グループ名のリストを丸かっこで囲み、各グループ名をスペースまたはカンマで区切ります。

注: **グループにメンバを追加するには join コマンドを使用し、グループからメンバを削除するには** join コマンドを使用します。

```
{chgrp | cg | editgrp | eg | newgrp | ng} (groupName) | (groupNames...) | ¥
(~groupName) | ( ~groupNames) ¥
[global] ¥
[comment(string) | comment- ] ¥
[privileges(privList)]  ¥
[privileges(-privList)]  ¥
[rename_group]
```

comment(*string*)

グループ レコードに最大 255 文字の英数字から成るコメント文字列を追加します。グループ レコードにすでにコメント文字列が追加されている場合、既存の文字列はここで指定した新しい文字列に置き換えられます。文字列に空白が含まれる場合は、文字列全体を一重引用符で囲みます。

標準 Windows グループには、システムのインストール時に説明のコメントが追加されています。Windows 環境と eTrust 環境の両方に新しいグループを作成すると、eTrust Access Control によって「eTrust Group」というコメントが追加されます。

global

グローバル グループを示します。Windows データベースに存在しない一意のグループ名を指定する必要があります。Windows では、グループとユーザに同じ名前を指定できません。

注: global グループを作成して、eTrust Access Control バージョン 4.1 を使用する場合は、*~groupName* を使用します。バージョン 4.1 以降では、旧バージョンとの互換性を保つために、この形式がサポートされています。

groupName

newgrp コマンドの場合は、データベースに追加されるグループ レコードの名前を示します。Windows データベースに存在しない一意のグループ名を指定する必要があります。eTrust データベースとは異なり、Windows では、グループとユーザに同じ名前を指定できません。

chgrp コマンドの場合は、変更するプロパティが含まれているグループの名前を示します。

複数のグループを定義する場合、または複数グループのプロパティを変更する場合は、グループ名のリストを丸かっこで囲み、各グループ名をスペースまたはカンマで区切ります。

privileges(*privList*|-*privList*)

Windows のグループ レコードに特定の権限を追加します。privList の前にマイナス記号(-)を付けた場合は、指定した権限を削除します。有効な値は、ネイティブ Windows で指定できるすべての権限です。

このパラメータは、chgrp コマンドまたは editgrp コマンドで既存のグループ レコードを変更する場合にのみ指定できます。新しいグループ レコードを作成するときに、このパラメータを使用して権限を割り当てることはできません。Windows の権限の一覧については、付録「Windows の値」を参照してください。

rename_group

Windows データベースのグループ アカウント名を変更します。古いグループ名のすべてのプロパティは、名前を変更したグループ アカウントに適用されます。Windows データベースに存在する一意のグループ名を指定する必要があります。eTrust Access Control データベースとは異なり、Windows では、グループとユーザに同じ名前を指定できません。

注: Active Directory がインストールされている Windows 2000 に eTrust Access Control をインストールすると、eTrust Access Control によって、以前の Windows 2000 のグループ名が変更されます。

関連項目

この章の rmgrp コマンド、showgrp コマンド、および join コマンドの説明。

chres / editres / newres

newres は、eTrust Access Control クラスに新しいリソースを定義するコマンドです。chres は、eTrust Access Control クラスに属する 1 つまたは複数のリソース レコードを変更するコマンドです。editres は、新しいリソースを定義することも、既存のリソースを変更することもできるコマンドです。

```
{chres | cr | editres | er | newres | nr}        ¥
   className resourceName | (resourceNames...)       ¥
   [comment(string) | comment-]           ¥
   [defaccess(accessValue)]               ¥
   [dword(integer)|string(string)|binary(hexastring)|multistring(string)] ¥
   [location(string) | location()] ¥
   [maxusers(integer)]                  ¥
   [owner(userName | groupName)]
   [share_name(string) | sharename-]    ¥

{chres | cr | editres | er | newres | nr}    ¥
   DOMAIN resourceName | (resourceNames...)   ¥
   [computer(workstationName) | computer-(workstationName)]¥
[domainpwd(connectPassword)]              ¥
   [trusted(domainName) | trusted-(domainName)]
```

binary(*hexastring*)

レジストリ キーが 16 進数の場合に、レジストリ キーの値を示します。

className

resourceName が属するクラスの名前を示します。

newres コマンドの場合、有効な値は REGKEY、REGVAL、OU、および SHARE です。chres コマンドおよび editres コマンドの場合、有効な値は COM、DISK、DOMAIN、FILE、PRINTER、REGKEY、REGVAL、SERVICE、DEVICE、SESSION、OU、および SHARE です。

comment(*string*)

リソース レコードにコメント文字列を追加します。リソース レコードにすでにコメント文字列が追加されている場合、既存の文字列はここで指定した新しい文字列に置き換えられます。このパラメータは、SHARE リソースおよび PRINTER リソースに対してのみ有効です。

computer(*workstationName*)|computer-(*workstationName*)

ドメインに追加するワークステーションの名前を示します。引数の前にマイナス記号を付けた場合は、ドメインから削除するワークステーションを示します。このパラメータは、DOMAIN リソースに対してのみ使用でき、chres コマンドまたは editres コマンドにのみ指定可能です。

defaccess(*accessValue*)

ネイティブ セキュリティが組み込まれているグループ Everyone に対するアクセス権限を示します。すべてのシステム ユーザは Everyone グループのメンバです。Everyone グループにアクセス権を与えると、認証されたすべてのユーザだけでなく、すべての潜在的な匿名ユーザもアクセスできるようになります。

注: eTrust Access Control 環境で定義されたオブジェクトの defaccess には、別の意味があります。この場合、デフォルトのアクセス権限とは、リソースの eTrust Access Control のリストに含まれていないアクセサがリソースへのアクセス要求をした場合に与えられる権限のことです。また、デフォルトのアクセス権限は、eTrust Access Control で定義されていないユーザにも適用されます。

defaccess パラメータは、NTFS ファイル システムにのみ適用されます。

domainpwd(*connectPassword*)

管理者が信頼関係を変更するときに入力する必要があるパスワードを示します。

このパラメータは、DOMAIN リソースに対してのみ使用でき、chres コマンドまたは editres コマンドにのみ指定可能です。

dword(*integer*)

レジストリ キーが整数の場合に、レジストリ キーの値を示します。

gen_prop(*propertyName*)

OU クラスのプロパティを示します。

このパラメータは OU クラスに対してのみ有効です。

gen_value(*valueName*)

OU クラスのプロパティ値を示します。

このパラメータは OU クラスに対してのみ有効です。

location(*string*)

プリンタの場所を示します。このプロパティを削除するには、( ) 内に何も指定しません。

このパラメータは PRINTER リソースに対してのみ有効です。

maxusers(*integer*)

共有ディレクトリに同時に接続できるユーザの最大数(*integer*)を示します。

このパラメータは SHARE リソースに対してのみ有効です。

multistring(*string*)

レジストリ キーが複数文字列の場合に、レジストリ キーの値を示します。

owner(*userName*|*groupName*)

リソース レコードの所有者としてユーザまたはグループを割り当てます。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。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許可が常に与えられます。詳細については、「**管理者ガイド**」を参照してください。

FAT ファイル システムの FILE レコードまたは SHARE レコードには、owner パラメータを指定できません。このパラメータは、DEVICE、DOMAIN、OU、PROCESS、REGVAL、SERVICE、および SESSION の各リソースに対しても指定できません。

resourceName

変更または追加するリソース レコードの名前です。複数のリソースを変更または追加する場合は、リソース名のリストを丸かっこで囲み、各リソース名をスペースまたはカンマで区切ります。少なくとも 1 つのリソース名を指定する必要があります。

eTrust Access Control では、指定したパラメータに従って、各リソース レコードが個別に処理されます。リソースの処理中にエラーが発生すると、メッセージが表示され、リストの次のリソースから処理が続行されます。

share_name(*shareName*) | share_name-

プリンタの共有ポイントを示します。

このパラメータは PRINTER リソースに対してのみ有効です。

string(*string*)

レジストリ キーが文字列の場合に、レジストリ キーの値を示します。

trusted(*domainName*) | trusted-(*domainName*)

trusted ドメインに追加するドメインの名前を示します。ドメインを untrusted にする場合は、引数の前にマイナス記号を付けてドメイン名を示します。このパラメータは、DOMAIN リソースに対してのみ使用でき、chres コマンドまたは editres コマンドにのみ指定可能です。

chusr / editusr / newusr

newusr は、1 人または複数の新規ユーザを Windows システムに定義するコマンドです。chusr は、Windows システムの 1 人または複数のユーザの定義を変更するコマンドです。editusr は、新しいユーザを定義することも、既存のユーザのプロパティを変更することもできるコマンドです。

```
{{chusr | cu | editusr | eu | newusr | nu} userName   ¥
        [comment(string) | comment- ]  ¥
        [country(string)]  ¥
        [expire | expire(mm/dd/yy[@hh:mm]) | expire-]  ¥
        [flags(accountFlags) |-(accountFlags)]  ¥
        [full_name(fullName)]   ¥
        [homedir(homeDir)]  ¥
        [homedrive(homeDrive)]   ¥
        [location(string)]   ¥
        [logonserver(serverName)]   ¥
        [organization(name)]   ¥
        [org_unit(name)]   ¥
        [password(password)]   ¥
        [pgroup(primaryGroup)]   ¥
        [phone(string)]   ¥
        [privileges(privList)]   ¥
        [profile(path)]   ¥
        [restrictions(days( day-data ) time(hh:hh | anytime) )]¥
day-data: {[mon] [tue] [wed] [thu] [fri] [sat] [sun]} | anyday | weekdays ¥
        [rename_user]
        [restrictions-]   ¥
        [resume[(date)] | resume-} ¥
        [script(logonScriptPath)]   ¥
        [suspend[(date)] | suspend-] ¥
        [terminals(terminalList) | terminals-(terminalList)]  ¥
        [workstations(workstationList)|workstations-(workstationList)|workstations-]
```

comment(*string*)|comment-

ユーザ レコードにコメント文字列を割り当てます。

引数は最大 255 文字の英数字から成る文字列です。文字列に空白が含まれる場合は、文字列全体を一重引用符で囲みます。

country(*string*)

ユーザの国名を示します。この文字列は認証プロセスでは使用されません。

引数は最大 19 文字の英数字から成る文字列です。文字列に空白が含まれる場合は、文字列全体を一重引用符で囲みます。

expire|expire(*mm/dd/yy[@hh:mm*) | expire-

ユーザ アカウントが失効する日付を設定します。この日付を指定しない場合、ユーザが現在ログインしていなければ、ユーザ アカウントはただちに失効します。ユーザがログインしていれば、アカウントはユーザがログアウトした時点で失効します。

newusr コマンドでは、有効期限のないユーザ アカウントを定義する場合に expire- パラメータを指定します。chusr コマンドおよび editusr コマンドでは、指定されたユーザ アカウントから有効期限を削除する場合にこのパラメータを指定します。

date 引数は次の形式で指定します。*mm*/*dd*/*yy* [@*hh*:*mm*]

flags(*accountFlags*/- *accountFlags*)

ユーザ アカウントの特定の属性を示します。有効なフラグ値の詳細については、付録「Windows の値」を参照してください。

ユーザ レコードからフラグを削除するには、*accountFlags* の前にマイナス記号 (-) を付けます。

full_name(*fullName*)

ユーザ レコードに関連付けられたユーザのフル ネームを示します。

引数は最大 256 文字の英数字から成る文字列です。文字列に空白が含まれる場合は、文字列全体を一重引用符で囲みます。

homedir(*homeDir*)

ユーザのホーム ディレクトリを示します。ユーザは、自分のホーム ドライブおよびホーム ディレクトリに自動的にログインできます。

homedrive(*homeDrive*)

ユーザのホーム ディレクトリのドライブを示します。ユーザは、自分のホーム ドライブおよびホーム ディレクトリに自動的にログインできます。

location(*string*)

ユーザの所在地を示します。この文字列は認証プロセスでは使用されません。

引数は最大 19 文字の英数字から成る文字列です。文字列に空白が含まれる場合は、文字列全体を一重引用符で囲みます。

logonserver(*serverName*)

ユーザのログイン情報を確認するサーバを示します。ユーザがドメイン ワークステーションにログインすると、eTrust Access Control からこの引数で指定したサーバにログイン情報が送られ、ユーザがワークステーションを使用することが許可されます。

organization(*name*)

ユーザが所属する組織を示します。この情報は認証プロセスでは使用されません。

引数は最大 256 文字の英数字から成る文字列です。文字列に空白が含まれる場合は、文字列全体を一重引用符で囲みます。

org_unit(*name*)

ユーザが所属する組織単位を示します。この情報は認証プロセスでは使用されません。

引数は最大 256 文字の英数字から成る文字列です。文字列に空白が含まれる場合は、文字列全体を一重引用符で囲みます。

password(*password*)

ユーザにパスワードを割り当てます。パスワード チェックが有効になっている場合、指定したパスワードでログインできるのは 1 回のみです。次回システムにログインする際に、ユーザは新しいパスワードを設定する必要があります。

引数はスペースやカンマを含まない最大 14 文字の文字列です。パスワード チェックが有効になっている場合、指定したパスワードでログインできるのは 1 回のみです。「Password Never Expires」のフラグが設定されている場合を除いて、次回システムにログインする際に、ユーザは新しいパスワードを設定する必要があります。ADMIN 属性を持つユーザまたは eTrust Access Control Admin グループのメンバであっても、chusr コマンドまたは editusr コマンドを使用して自分のパスワードを変更することはできません。

Windows NT システム上でユーザのパスワードを設定している場合は、以下のメッセージが表示されることがあります。

パスワードが必要な長さよりも短い。

このエラーは、パスワードがポリシー要件を満たしていないことを意味します。このエラーの原因は、以下のいずれかです。

- パスワードが必要な長さよりも短いか、または長い。
- パスワードが最近使用されており、Windows NT Change History フィールドに存在します。
- パスワードに十分に一意である文字が含まれていません。
- パスワードが他のパスワード ポリシー要件(eTrust Access Control パスワード ポリシーで設定された要件など)を満たしていません。

このエラーを回避するには、該当するすべての要件を満たすパスワードを設定するようにしてください。

pgroup(*primaryGroup*)

ユーザのプライマリ グループ ID を設定します。プライマリ グループはユーザが定義されているグループの 1 つで、グローバル グループであることが必要です。

引数はスペースやカンマを含まない最大 14 文字の文字列です。

phone(*string*)

ユーザの電話番号を示します。この情報は認証プロセスでは使用されません。

privileges(*privList*)

Windows のユーザ レコードに特定の権限を追加します。*privList* の前にマイナス記号 (-) を付けた場合は、指定した権限を削除します。このパラメータは、chusr コマンドまたは editusr コマンドで既存のユーザ レコードを変更する場合にのみ指定可能です。新しいユーザ レコードを作成するときに、このパラメータを使用して権限を割り当てることはできません。

Windows の権限の一覧については、付録「Windows の値」を参照してください。

profile(*path*)

デスクトップ環境(プログラム グループ、ネットワーク接続)のユーザのプロファイルが含まれているファイルの完全パスを指定します。ユーザがワークステーションにログインすると、毎回同じ環境が画面に表示されます。

rename_user

Windows データベースのユーザ アカウント名を変更します。古いユーザ名のすべてのプロパティは、名前を変更したユーザ アカウントに適用されます。Windows データベースに存在する一意のユーザ名を指定する必要があります。eTrust Access Control データベースとは異なり、Windows では、グループとユーザに同じ名前を指定できません。

注: Active Directory がインストールされている Windows 2000 に eTrust Access Control をインストールすると、eTrust Access Control によって、ユーザ ログオン名(以前の Windows 2000 のユーザ名)が変更されます。ただし、eTrust Access Control では、Windows と異なり、フル ネームは変更されません。

注: オブジェクト名の最大文字数は 255 文字です。eTrust Access Control および Windows では、256 文字以上の名前が付いたリソースを管理できません。

restrictions([*days*] [*time*])|restrictions-([*days*] [*time*])

ユーザがファイルにアクセスできる曜日と時間帯を示します。

days 引数を指定せずに time 引数を指定した場合、レコード内にすでに設定されている曜日制限に対して、指定した時刻制限が適用されます。time 引数を指定せずに days 引数を指定した場合、レコード内にすでに設定されている時刻制限に対して、指定した曜日制限が適用されます。days 引数と time 引数の両方を指定した場合、ユーザは、指定した曜日の指定した時間帯にのみシステムにアクセスできます。

- [days] には、ユーザがファイルにアクセスできる曜日を示します。days 引数には以下のサブ引数があります。
  - anyday - ユーザはすべての曜日にファイルにアクセスできます。

- weekdays - ユーザは月曜から金曜までの平日に限りリソースにアクセスできます。
  - Mon、Tue、Wed、Thu、Fri、Sat、Sun - ユーザは指定した曜日にのみリソースにアクセスできます。曜日は任意の順で指定できます。複数の曜日を指定する場合は、各曜日をスペースまたはカンマで区切ります。
- [time] には、ユーザがリソースにアクセスできる時間帯を示します。time 引数には以下のサブ引数があります。
  - anytime - ユーザは任意の時間帯にリソースにアクセスできます。
  - startTime:endTime - 指定した時間帯に限りリソースにアクセスできます。startTime と endTime の両方とも *hhmm* の形式で指定します。*hh* は 24 時間表記の時間(00 から 23)、*mm* は分(00 から 59)を表します。2400 は有効な time 値ではないことに注意してください。startTime が endTime より小さいこと、および両方が同じ日の時刻であることが必要です。端末がホストと異なるタイム ゾーンにある場合は、端末の開始時間と終了時間をホストのローカル時間に相当する時間に変換し、時間の値を調整してください。たとえば、ホストがニューヨークにあり、端末がロサンゼルスにある場合、端末へのアクセスをロサンゼルス時間の午前 8 時から午後 5 時まで許可するには、「time (1100:2000)」と指定します。

resume(*date*)|resume-

ユーザ アカウントの再開日および再開時間(オプション)です。suspend パラメータと resume パラメータの両方を指定する場合、再開日を一時停止日より後に設定していることを確認する必要があります。そうでないと、ユーザの一時停止が無期限になります。

日付と時刻は、以下の形式で指定します。時刻は省略可能です。

mm/dd/yy[@HH:MM]

resume- パラメータを使用して、ユーザ アカウントのステータスをアクティブ(有効)から一時停止に変更します。このパラメータは chusr コマンドまたは editusr コマンドにのみ使用できます。

script(*loginScriptPath*)

ユーザがログインしたときに自動的に実行されるファイルの場所を示します。このログイン スクリプトによって作業環境が設定されます。ユーザの作業環境は profile パラメータでも設定されるため、このパラメータの指定は省略可能です。

suspend(*date*)|suspend-

ユーザ アカウントを無効にします。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。date を指定すると、指定した日にユーザ アカウントが一時停止されます。date を省略すると、chusr コマンドの実行直後にユーザ アカウントが一時停止されます。

日付と時刻は、次の形式で指定します。時刻は省略可能です。*mm/dd/yy[@HH:MM]*

suspend- パラメータを使用して、ユーザ アカウントのステータスを無効からアクティブ（有効）に変更します。このパラメータは chusr コマンドまたは editusr コマンドにのみ使用できます。

terminals(*terminalList*)|terminals-(*terminalList*)

ユーザがログインできる端末を最大 8 台まで指定します。端末のリストを一重引用符で囲み、各端末の名前をカンマで区切ります。以下に例を示します。

“terminal1,terminal2”

workstations(*workstationList*)|workstations-(*workstationList*)|workstations-

ユーザがログインできるワークステーションを最大 8 台まで指定します。ワークステーションのリストを一重引用符で囲み、各ステーション名をカンマで区切ります。以下に例を示します。

“workstation1,workstation2”

関連項目

この章の rmusr コマンド、showusr コマンド、および join コマンドの説明。

environment

environment コマンドは、セキュリティ環境を設定します。eTrust Access Control は、eTrust Access Control、Windows、および UNIX/Linux のセキュリティ環境をサポートします。selang コマンド シェルを起動すると、デフォルトでは eTrust 環境が選択されます。

{environment | env} {etrust | native | nt |pmd | seos | unix}

eTrust

eTrust のセキュリティ環境を示します。selang のコマンドは、eTrust データベースに対して実行されます。一部のコマンドでは、接続先ホストのネイティブ OS のセキュリティ設定を同時に更新できます。eTrust 環境の selang のプロンプトは次のとおりです。eTrustAC>

native

入力するコマンドを、ローカルまたはリモートの接続先ホストのネイティブ環境（Windows または UNIX/Linux）にあるデータベースに対して実行することを示します。ネイティブ環境の selang のプロンプトは次のとおりです。eTrustAC(native)>

nt

Windows のセキュリティ環境を示します。selang のコマンドは、Windows データベースに対して実行されます。一部のコマンドでは、eTrust のセキュリティ設定を同時に更新できます。Windows 環境の selang のプロンプトは次のとおりです。eTrustAC(nt)>

pmd

リモート管理環境で selang のコマンドを示します。selang コマンド シェルを pmd 環境に設定すると、selang のコマンドは、選択されたホストの PMDB に対して実行されます。pmd 環境の selang のプロンプトは次のとおりです。eTrustAC(pmd)>

seos

eTrust のセキュリティ環境を示します。このパラメータは、旧バージョンとの互換性を保つために維持されています。selang のプロンプトは次のとおりです。eTrustAC>

unix

UNIX/Linux のリモート ホストに接続する場合に、入力するコマンドを UNIX/Linux データベースに対して実行することを示します。UNIX/Linux 環境の selang のプロンプトは次のとおりです。eTrustAC(unix)>

find

find は、環境に定義されているクラスを一覧表示するコマンドです。このコマンドに *className* パラメータを指定すると、指定した Windows 環境のクラスに含まれるすべてのレコードの名前が一覧表示されます。「file」パラメータを指定すると、マスクに一致するすべてのファイルが一覧表示されます。マスクは文字列です。

注: file パラメータのこの使用方法は、eTrust 環境での使用方法と異なります。

find コマンドを SEOS クラスに使用することはできません。

```
{find | f} [{className | class(className)} | className(memberName) | objMask ] ¥
                        file ¥[directory][¥mask]
```

class(*className*)

SEOS を除く、Windows 環境の有効なクラスの名前です。

className(*memberName*)

クラスのメンバの名前です。複数のエントリは、丸かっこで囲み、スペースまたはカンマで区切ります。

objmask

指定したクラスのオブジェクトのうち、指定したオブジェクト マスクに一致するオブジェクトをすべて一覧表示します。オブジェクト マスクはワイルドカードを使用して指定します。

file ¥*directory*¥

directory で指定したディレクトリ内のすべてのファイルを一覧表示します。

¥*directory*¥*mask*

directory で指定したディレクトリ内のファイルのうち、*mask* 変数に一致するすべてのファイルを一覧表示します。*mask* には、ワイルドカード文字を使用する必要があります。

ワイルドカードによる一致

selang では、以下のワイルドカード文字を使用できます。

***（アスタリスク）**

0 個以上の文字列

?（疑問符）

任意の 1 文字

任意の 1 文字に一致するパターンを指定するには、以下の例のように、疑問符(?)を使用します。

ワイルドカード指定	一致パターン
mmc?	mmc3、mmcx、mmc5
mmc?.t	mmc1.t、mmc2.t
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、以下の例に示すようにアスタリスク(*)を使用します。

ワイルドカード指定	一致パターン
i.c	main.c、list.c
st*.h	stdio.h、stdlib.h、string.h
*	指定されたクラスのすべてのレコード

help

Windows 環境 で selang のコマンドのヘルプを表示します。

{help | h | ?} [*command-name* | access | privileges]

command-name

指定したコマンドの構文を表示します。

access

access パラメータおよび defaccess パラメータで指定できるアクセス タイプをクラス別に一覧表示します。

privileges

chgrp、editgrp、chusr、および editusr コマンドで使用できる Windows の権限を一覧表示します。

history

これまでに入力したコマンドの履歴を一覧表示します。このマニュアルの第 1 章「selang コマンド言語」にある説明を参照してください。

history

join

join は、ユーザをグループに追加するコマンドです。join- は、グループからユーザを削除するコマンドです。Windows にすでに定義されているユーザまたはグループを指定する必要があります。

権限

管理者は、標準権限要件（第 1 章「selang コマンド言語」の「権限」を参照）を満たしていて、さらに MODIFY プロパティと JOIN プロパティの**両方**を持っている場合に限り、eTrust Access Control の GROUP レコードおよび Windows グループを変更する権限があります。

{join | j} *userName* group(*groupName*)

{join- | j-} *userName* group(*groupName*)

group(*groupName*)

ユーザを追加または削除するグループを示します。*groupName* 引数には既存の Windows グループの名前を指定する必要があります。

userName

Group パラメータで指定したグループに追加する Windows ユーザの名前、またはこのグループから削除する Windows ユーザの名前を指定します。複数のユーザを指定する場合は、ユーザ名のリストをかっこで囲み、各ユーザ名をスペースまたはカンマで区切ります。

関連項目

この章の chgrp コマンド、rmgrp コマンド、および showgrp コマンドの説明。

list

特定の環境に定義されているクラスを一覧表示します。このコマンドに *className* パラメータを指定すると、指定した Windows 環境のクラスに含まれるすべてのレコードの名前が一覧表示されます。このコマンドに「file」パラメータを指定すると、ディレクトリ内のマスクに一致するファイルが一覧表示されます。このコマンドは、find コマンドと同じです。詳細については、この章の find コマンドの説明を参照してください。

list {[*className*] | file ¥[*directory*][¥*mask*]}

関連項目

この章の find コマンドの説明。

rmgrp

rmgrp は、Windows システム データベースから 1 つまたは複数のグループを削除するコマンドです。

{rmgrp | rg} *groupName*

groupName

削除するグループの名前です。既存の Windows グループ名を指定する必要があります。1 つまたは複数のグループ名を指定します。複数のグループを削除する場合は、グループ名のリストをかっこで囲み、各グループ名をスペースまたはカンマで区切ります。

関連項目

この章の chgrp コマンド、newgrp コマンド、および showgrp コマンドの説明。

rmres

rmres は、Windows システム データベースから 1 つまたは複数のリソースを削除するコマンドです。

{rmres | rr} *className resourceName*

className

リソースが属するクラスの名前です。

resourceName

className で指定したクラスの既存の Windows リソースの名前です。複数のリソースを削除する場合は、ユーザ名のリストをかっこで囲み、各ユーザ名をスペースまたはカンマで区切ります。

関連項目

この章の chres コマンド、newres コマンド、および showres コマンドの説明。

rmusr

rmusr は、Windows システム データベースから 1 人または複数のユーザを削除するコマンドです。

{rmusr | ru} *userName*

userName

既存の Windows ユーザのユーザ名です。複数のユーザを削除する場合は、ユーザ名のリストをかっこで囲み、各ユーザ名をスペースまたはカンマで区切ります。

関連項目

この章の chusr コマンド、newusr コマンド、および showusr コマンドの説明。

search

このコマンドは、find コマンドと同じです。詳細については、この章の「find」コマンドの説明を参照してください。

search {[*className*] | file ¥[*directory*][¥*mask*]}

関連項目

この章の find コマンドの説明。

setoptions

setoptions は、リソースの保護に関連するシステム全体の eTrust Access Control オプションを動的に設定するコマンドです。たとえば、setoptions を使用すると、クラス単位またはシステム全体の全クラスに対するセキュリティ チェックの有効化または無効化、パスワード ポリシーの設定、および eTrust Access Control オプションの現在の設定値の一覧表示などができます。

setoptions コマンドでは、通常、パラメータを指定してコマンドを実行するために ADMIN 属性が必要です。ただし、AUDITOR 属性のみを持つユーザ、または OPERATOR 属性のみを持つユーザでも、list パラメータを指定して setoptions コマンドを実行できます。

```
eTrustAC( nt )> help setoptions
    {setoptions | so}
        [password(
                [history(number-stored-passwords) | history-]
                [interval(maximum-password-change-interval) | interval-]
                [min_life(minimum-password-change-interval) | min_life-]
                [force_logoff(minutes)| force_logoff-]
                [maxlogins(maximum-number-of-logins) | maxlogins-]
        )]
```

または

```
    setoptions list
```

history(*NStoredPasswords*)

データベースに格納される使用済みパスワードの数を示します。新しいパスワードの作成時、ユーザは履歴リストに保存されているパスワードを指定できません。*NStoredPasswords* は 1 から 24 までの整数です。0 を指定した場合、パスワードは保存されません。

history

パスワード履歴のチェックを無効にします。

interval(*nDays*)

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。

nDays の値には、正の整数または 0 を指定します。期間を 0 に設定すると、ユーザに対するパスワード期間のチェックは無効になります。パスワードに有効期限を設定しない場合は、期間を 0 に設定します。

interval

パスワード期間の設定を取り消します。

min_life(*NDays*)

変更したパスワードを再度変更できるようになるまでの最短日数を設定します。*NDays* には、正の整数を指定します。

min_life

パスワード変更後、再度変更できるようになるまでの最短日数の設定を無効にします。

showfile

showfile は、1 つまたは複数のファイルの詳細を一覧表示するコマンドです。複数のファイルの詳細を表示するには、ファイル名を個々に指定するか、ワイルドカードを使用します。

{showfile | sf} *fileName*

fileName

詳細を一覧表示するファイルの完全パスおよび名前です。1 つまたは複数の Windows ファイル名を入力します。複数のファイルを指定する場合は、ファイル名のリストをかっこで囲み、各ファイル名をスペースまたはカンマで区切ります。

関連項目

この章の chfile コマンドの説明。

showgrp

showgrp は、1 つまたは複数の Windows グループの詳細を表示するコマンドです。

{showgrp | sg} *groupName*

groupName

詳細を表示するグループの名前です。既存の Windows グループ名を指定する必要があります。1 つまたは複数のグループ名を指定します。複数のグループを表示する場合は、グループ名のリストをかっこで囲み、各グループ名をスペースまたはカンマで区切ります。

関連項目

この章の chgrp コマンド、newgrp コマンド、および rmgrp コマンドの説明。

showres

Windows リソースのプロパティを表示します。

{showres | sr } *className resourceName*

className

リソースが属するクラスの名前です。

resourceName

className で指定したクラスの既存の Windows リソースの名前です。

showusr

showusr は、1 人以上の Windows ユーザのプロパティを表示するコマンドです。

{showusr | su} *userName*

userName

Windows のプロパティを表示するユーザの名前です。既存の Windows ユーザ名を指定します。複数のユーザのプロパティを表示する場合は、ユーザ名のリストをかっこで囲み、各ユーザ名をスペースまたはカンマで区切ります。

関連項目

この章の chusr コマンド、newusr コマンド、および rmusr コマンドの説明。

xaudit

xaudit は、システム アクセス制御リスト(SACL)にエントリを追加するコマンドです。このリスト内の各エントリには、指定したユーザまたはグループがリソースへのアクセス権を取得しようとしたときに、監査メッセージが記録されます。xaudit- コマンドは、SACL からエントリを削除するコマンドです。このコマンドは、FILE、PRINTER、REGKEY、DISK、COM、および SHARE タイプのリソースに対して有効です。

```
xaudit className, resourceName ¥
[failure(auditMode)]     ¥
[gid(groupName)] ¥
[success(auditMode)] ¥
[uid(userName)]

xaudit- className, resourceName ¥
    [gid(groupName)] ¥
    [uid(userName)]
```

className

リソースが属するリソース タイプの名前です。

failure(*auditMode*)

リソースに対する許可されないアクセス試行を記録します。

auditmode の有効な値は、リソースが属するリソース タイプによって以下のように異なります。

注: 監査モードを設定できるのは NTFS ファイルのみです。

- DISK および COM: changePermissions、delete、modify、query、read、synchronize、および takeOwnership
- FILE: changePermissions、delete、execute、read、takeOwnership、および write
- PRINTER: changePermissions、delete、print、および takeOwnership
- REGKEY: delete、enumerate、link、notify、queryValue、readControl、setValue、subkey、および write

すべてのリソース タイプ: none および all

gid(*groupName*)

リソースへのアクセスが監査対象になる 1 つまたは複数のグループを示します。複数のグループを指定する場合は、各グループ名をスペースまたはカンマで区切ります。

resourceName

システム アクセス制御リスト(SACL)を変更するリソース レコードの名前を示します。

success(*auditMode*)

リソースに対して許可されたアクセスを記録します。

auditmode の有効な値は、リソースが属するリソース タイプによって以下のように異なります。

注: 監査モードを設定できるのは NTFS ファイルのみです。

- DISK および COM: changePermissions、delete、modify、query、read、synchronize、および takeOwnership
- FILE: changePermissions、delete、execute、read、takeOwnership、および write
- PRINTER: changePermissions、delete、print、および takeOwnership
- REGKEY: delete、enumerate、link、notify、queryValue、readControl、setValue、subkey、および write

すべてのリソース タイプ: none および all

uid(*userName*)

リソースへのアクセスが監査対象になるユーザを示します。複数のユーザを指定する場合は、各ユーザ名をスペースまたはカンマで区切ります。Windows NT データベースで定義されているすべてのユーザを指定する場合は、*userName* にアスタリスク(*)を指定します。

第 4 章: Policy Model 環境の selang のコマンド

このセクションには、以下のトピックが含まれます。

Policy Model 環境での作業

この章では、pmd 環境で使用できる selang のコマンドについて詳しく説明します。Policy Model をリモート管理することによって、サブスクライバの管理、更新ファイルの切り捨て、Policy Model エラー ファイルの管理を行うことができます。selang の他の環境についての一般情報、ヘルプの表示方法、コマンド構文、およびコマンドの全体的な構成については、「selang – eTrust AC のコマンド言語」の章を参照してください。

Policy Model 環境のコマンド リファレンス

このセクションでは、Policy Model 環境で使用できるすべての selang のコマンドをアルファベット順に示します。

createpmd

createpmd は、リモート ホスト上に PMDB を定義するコマンドです。1 人以上のユーザを PMDB の管理者、監査者、およびパスワード管理者に指定できます。特定の PMDB に対する親 PMDB およびサブスクライバ PMDB を定義することもできます。createpmd コマンドは、ローカルで実行する必要がありますが、リモート シェルから実行することもできます。

createpmd *pmdname* [options]

admins(*user1 [user2 . . .]*)

PMDB 管理者の名前を示します。複数指定する場合は、スペースで区切ります。

auditors(*user1 [user2 . . .]*)

PMDB の監査ファイルを表示できるユーザを示します。複数指定する場合は、スペースで区切ります。

pwmans(*user1 [user2 . . .]*)

PMDB のパスワード管理者を示します。複数指定する場合は、スペースで区切ります。

parentpmd(pmdname@*host*)

作成する PMDB の親 PMDB の名前を示します。

desktop(*host1 [host2 . . .]*)

管理者が PMDB の管理を行うホストを示します。複数指定する場合は、スペースで区切ります。デフォルトでは、新しい PMDB のホストが設定されます。

subscribers(*host1 | pmd1 [host2 | pmd2 . . .]*)

新しい PMDB のサブスクライバになるホストまたは PMDB を示します。複数指定する場合は、スペースで区切ります。

pwdfile(filename)

PMDB パスワード ファイルを示します。

grpfile(*filename*)

PMDB グループ ファイルを示します。

deletepmd

deletepmd は、リモート ホストから以下の項目を削除するコマンドです。

- PMDB の selang 保護ファイルの場合
  - データベース ファイル
  - レジストリ エントリ
- PMDB ディレクトリの内容
- PMDB ディレクトリ

注: PMDB を削除する場合、PMDB の各ファイルを手動で削除しないでください(処理に重大な問題が生じるのを防ぐため)。リモート PMDB には常に deletepmd コマンドを使用してください。

```
deletepmd pmdname
```

findpmd

findpmd は、接続先のホストの PMDB を一覧表示するコマンドです。

```
findpmd
```

listpmd

listpmd は、PMDB とそのサブスクライバ、更新ファイル、およびエラー ログに関する情報を一覧表示するコマンドです。オプションを指定しない場合は、 *pmdName* で指定した Policy Model データベースのすべてのサブスクライバが一覧表示されます。

```
listpmd pmdName  ¥
[cmd(offset)]  ¥
[errors|all_errors[next(N)]]  ¥
[info]  ¥
[subscriber(subNames)]
[log]
```

cmd *(offset)*

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。オフセットを指定すると、リストはオフセット位置から開始されます。オフセットが指定されていない場合は、更新ファイルの先頭から表示が開始されます。

errors|all_errors [next(*N*)]

Policy Model のエラー ログを表示します。errors を指定すると、接続障害以外のすべての種類のエラーが表示されます。all_errors を指定すると、すべてのエラーが表示されます。

next を指定すると、次の *N* 個のエラーが表示されます。*N* は、レジストリ サブキー HKEY_LOCAL_MACHINE¥ SOFTWARE¥ComputerAssociates¥eTrustAccessControl¥lang の query_size の値です。

info

pmdName に指定した Policy Model に関する一般情報を表示します。Policy Model に親が存在するかどうかなどの情報が表示されます。

subscriber(*subNames*)

Policy Model のサブスクライバおよび各サブスクライバ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、次に伝達するコマンドなどの情報が表示されます。subNames を指定すると、サブスクライバのサブセットを選択できます。

listpmd は、PMDB とそのサブスクライバ、更新ファイル、およびエラー ログに関する情報を一覧表示するコマンドです。

log

Policy Model の一般ログ ファイルを表示します。

注: 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。更新ファイルの初期オフセットと最新のオフセットが表示されます。

pmd

pmd は、Policy Model エラー ログの消去、サブスクライバ リストの更新、Policy Model サービスの開始または停止、および更新ファイルの切り捨てを行うコマンドです。

```
pmd pmdName  {                    ¥
    backup                        ¥
    operation                     ¥
   [{clrerr|clrerror}]            ¥
   [killog]                       ¥
   [release(subName)]             ¥
   [startlog]                     ¥
   [start]                        ¥
   [stop]                         ¥
   [{trunc|truncate}(offset)] }
```

backup

Policy Model をバックアップ ステータスに移行します。

clrerror|clrerr

Policy Model エラー ログを消去します。

killlog

Policy Model の一般的なログ ファイルを無効にします。

重要: kill コマンドを使用して PMDB サービスを停止しないでください。

operation

Policy Model をバックアップ ステータスから運用ステータスに移行します。

release(*subName*)

使用不可のサブスクライバのリストから、*subName* で指定されたサブスクライバを削除します。その結果、サブスクライバはただちに更新情報を受信できます。*subName* は、更新情報を受信できるようにするサブスクライバを示します。

startlog

Policy Model の一般的なログ ファイルの書き込みを可能にします。

start

eTrust Access Control Policy Model サービスを開始します。このオプションは、他のコマンドを実行しない場合に使用します。

stop

eTrust Access Control Policy Model デーモンおよびサービスを停止します。

truncate|trunc[*offset*]

更新ファイルを切り捨てます。オフセットを指定していない場合、ファイルは可能な最大オフセットで切り捨てられます。可能な最大オフセットは、正常にサブスクライバを更新した最後のコマンドの位置になります。*offset* を指定すると、指定したオフセットまでのすべてのエントリが削除されます。

subs

subs は、親 PMDB にサブスクライバを追加するか、親 PMDB に対してデータベースをサブスクライブするコマンドです。

```
subs pmdName {                              ¥
    [newsubs(subsName)]                      ¥
    [parentpmd(pmdName2@host)]                ¥
    [subs(subName)]                          ¥
    [host_type(Mainframehosttype)               ¥
      sysid(systemId)                        ¥
      mf_admin(Mainframeadministrator)        ¥
      port(Remoteport)]                      ¥
     {offset(offset)} }
```

host_type(*Mainframehosttype*)

サブスクライバのメインフレーム ホスト タイプです。

mf_admin(*Mainframeadministrator*)

サブスクライバのメインフレーム管理者です。

newsubs(*subsName*)

subName を *pmdName* という Policy Model にサブスクライブして、新しいサブスクライバに PMDB 全体、パスワード、およびグループ ファイルの内容を送信します。

parentpmd(*pmdName2@host*)

引数 *pmdName2@host* で指定された PMDB を *pmdName* の親 Policy Model として設定します。

port(*Remoteport*)

サブスクライバのポート番号です。

subs(*subsName*)

サブスクライバを PMDB に割り当てます。

sysid(*systemId*)

サブスクライバのシステム ID です。

ホストを PMDB にサブスクライブする場合は、以下の条件が満たされている必要があります。

- ホストが起動していること。
- そのホスト上で eTrust Access Control が実行中であること。
- PMDB が、サブスクライブされるホストの親 PMDB であること。この関係は、サブスクライバの seos.ini ファイルにある parent_pmd トークンによって設定され、ホストのサブスクライブ先 PMDB の名前が含まれている必要があります。

PMDB を別の PMDB にサブスクライブする場合は、以下の条件が満たされている必要があります。

- サブスクライバになる PMDB の pmd.ini ファイルにある parent_pmd トークンに、サブスクライブ先となる PMDB（親 PMDB）の名前が設定されていること。
- サブスクライブされる PMDB が格納されているホスト上で eTrust 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 PMDB を設定する場合は、親 PMDB のリストが含まれているファイルの名前を 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。

subspmd

subspmd は、接続先ホストの eTrust Access Control データベースの親を変更するコマンドです。新しい親 PMDB は、*pmdName@host.* で指定します。

subspmd parentpmd(*pmdName@host*)

unsubs

unsubs は、*pmdName* で指定した Policy Model のサブスクライバ リストから *subName* で指定したサブクライバを削除するコマンドです。

unsubs *pmdName* subs(*subName*)

第 5 章: ユーティリティ

このセクションには、以下のトピックが含まれます。

ユーティリティ

ユーティリティは、 eTrustACDir¥bin ディレクトリにあります(*eTrustACDir* は eTrust Access Control のインストール先です)。ユーティリティは DOS コマンドと同様に、DOS ウィンドウで使用します。各ユーティリティに適用されるスイッチ、オプション、およびパラメータについては、以下のセクションで説明します。

カテゴリ別のユーティリティ

このセクションでは、eTrust Access Control ユーティリティをカテゴリ別に一覧表示します。このリストをもとに、詳しい説明を参照してください。

ユーザ ユーティリティ

defclass

各データベースおよび定義済みの新しい PMDB に Unicenter TNG 基本アセット タイプを示します。

ExportTngDb

現在の Unicenter セキュリティのデータをローカル eTrust Access Control データベースまたは PMDB に移行します。

MigOpts

eTrust Access Control プログラムは、インストール時に実行され、現在の Unicenter セキュリティ環境を、ローカルの eTrust 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。

segrace

ユーザのさまざまなログイン設定およびパスワードを表示します。

SegraceW

ユーザは、失効したパスワードを変更できます。

sesudo

一般ユーザに代わって、管理者権限を必要とするコマンドを実行します。

一般的な管理ユーティリティ

eacpg_gen

eTrust Access Control 制御ポリシーを自動的に生成します。

seaudit

eTrust Access Control; 監査ログを表示するための機能を提供します。

sechkey

さまざまな eTrust Access Control プログラムの暗号化鍵を変更します。

secons

eTrust Access Control エンジンを制御するためのコンソールを起動します。

selang

eTrust Access Control のコマンド ライン言語です。

sereport

データベースおよび Policy Model 情報の HTML レポートを作成します。このレポートには Web ブラウザを使用してアクセスできます。

seretrust

untrusted プログラムを Trusted プログラムに戻します。

データベース管理ユーティリティ

eACSyncLockout

アカウントのロックアウトを eTrust Access Control データベースと同期させます。

dbmgr

eTrust Access Control データベースを管理します。このユーティリティは、旧バージョンのいくつかのデータベース ユーティリティに取って代わります。

ntimport

Windows システムのユーザおよびグループの情報を eTrust Access Control データベースにコピーします。

seclassadm

ローカル eTrust Access Control データベースに新しいクラスを追加します。

sepmd

PMDB を管理します。

サポート ユーティリティ

dbmgr

eTrust Access Control データベースのレコードを管理し、レコードに関する情報を報告します。

DictImport

パスワードの照合に使用する辞書ファイルをインポートします。

semsgtool

eTrust Access Control のメッセージ ファイルを管理します。

sepropadm

ローカル eTrust Access Control データベースのプロパティを管理します。

ユーティリティの詳細

このセクションでは、eTrust Access Control のユーティリティをアルファベット順に示し、各ユーティリティについて詳しく説明します。

ユーティリティは、特定のタスクを実行するように変更することができます。そのために使用するコマンド修飾子は、構文では***スイッチ***という用語で表されます。スイッチは、動作を制御する引数です。一部のスイッチには、選択したスイッチの動作をカスタマイズする***パラメータ***があります。パラメータとしてさまざまな***値***を指定できます。

構文

ユーティリティで使用する構文は selang の構文と同じです。詳細については、このマニュアルの第 1 章「selang コマンド言語」を参照してください。

ユーティリティの使用中にヘルプ メニューを呼び出すには、スイッチを省略できる場合はスイッチを指定せずにユーティリティを実行します。ユーティリティによっては、ヘルプ画面を表示するために -h スイッチを指定する必要があります。

dbmgr

eTrust 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します。

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 sepropadm の各ユーティリティに取って代わります。

重要: 問題を解決するためにこのユーティリティを使用する場合は、必ずテクニカル サポート担当者の指示に従ってください。指定するオプションによっては、このユーティリティは、eTrust Access Control が実行されていない状態のときに、eTrust Access Control データベースが格納されているディレクトリから起動する必要があります。

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。

構文

dbmgr ユーティリティの一般的な構文は以下のとおりです。

```
dbmgr option switch [parameter][filename]
```

以下のセクションでは、個々の構文、オプション、およびスイッチについて機能別に説明します。

データベースの作成

-create は、空の新規 eTrust Access Control データベースを生成するオプションです。このオプションは、secredb ユーティリティに取って代わるものです。

構文

```
dbmgr [-h] |-c -c[q] [-v |-d] [-u(username)]  ¥
[-t(terminalname1[,terminalname2]…) [-o | -w]
```

オプション

-create | -c-c[q]

新しいデータベースを作成します。-cq スイッチを指定した場合、確認のプロンプトは表示されません。

スイッチ

-d

データベース レイアウト ドキュメントを作成します。

-h

ヘルプを表示します。すべてのオプションのヘルプを表示する場合は、「dbmgr -h」と入力します。使用しているオプションのヘルプのみを表示する場合は、「dbmgr -c」(**-h は入力しない**)と入力します。

-o

Unicenter TNG クラスを既存のデータベースに追加します。

-t *terminalName*

管理者がローカル データベースの管理タスクを実行できる端末を示します。複数の端末を指定する場合は、各端末名をカンマで区切ります。

-u *userName*

userName に指定したユーザに、データベースに対する ADMIN 属性を与えます。指定しない場合、デフォルト ユーザは Administrator になります。

-v

進行状況を表示する詳細モードを無効にします。-d スイッチと -v スイッチは同時に指定できません。

-w

Unicenter TNG クラスが含まれている新しいデータベースを作成します。

注:

このコマンドは、インストール時か、新しいデータベースまたは Policy Model Database (PMDB)の作成時にのみ使用します。データベースは現在のディレクトリに作成されます。

たとえば、c:¥temp> というシステム プロンプトで、以下のように入力します。

c:¥Program Files¥CA¥eTrustAccessControl¥bin¥dbmgr-c -c -u userName ¥
-t terminalName

ユーティリティにより、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。 *userName* で指定したユーザがデータベースに作成されます。このユーザは、ADMIN 属性を持ち、*terminalName* で指定した端末からデータベースを管理できます。

特別なファイルも使用されません。

データベースのダンプ

このオプションは、dbdump ユーティリティおよび rdbdump ユーティリティに取って代わるものです。

構文

```
dbmgr [-h ] |{-d | -dump} [-r]        ¥
   [c] | [d class [property | @filename]] |    ¥
   [o class record [property | @filename]]|     ¥
   [e class record [property]] |       [f] | [fc] |    ¥
   [p(class)] |       [fp(class)] | [g(user)] |[l(class)]       ¥
```

オプション

-d | -dump -r

データベースの情報を表示します。-r スイッチを指定した場合は、現在使用中のデータベースの内容がダンプされます。

スイッチ

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* [*property*/*@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。変数 *class* はクラス名を指定します。*property* には、値を表示するプロパティのリストを指定します。複数のプロパティを指定する場合は、各プロパティ名をスペースで区切ります。ファイルからプロパティ リストを読み込むには、*property* の代わりにアット マーク(@)を入力し、その後に(スペースを入れないで)ファイル名を指定します。ファイルでは、1 行に 1 つのプロパティが表示されている必要があります。*property* 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。

e *class record* [*property*/ *@filename*]

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。変数 *class* はクラス名を指定します。*record* には、リストから除外するレコードの名前を指定します。*property* には、値を表示するプロパティのリストを指定します。複数のプロパティを指定する場合は、各プロパティ名をスペースで区切ります。ファイルからプロパティ リストを読み込むには、*property* の代わりにアット マーク(@)を入力し、その後に(スペースを入れないで)ファイル名を指定します。ファイルでは、1 行に 1 つのプロパティが表示されている必要があります。*property* 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。

f

指定したファイルにデータを書き込みます。

fc

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

fp *class*

指定したクラスのプロパティについて、すべてのデータベース プロパティ情報を一覧表示します。

g *userName*

指定したユーザが所属するグループを一覧表示します。

-h

ヘルプを表示します。すべてのオプションのヘルプを表示する場合は、「dbmgr -h」と入力します。使用しているオプションのヘルプのみを表示する場合は、「dbmgr -d」(-h は入力しなくても可)と入力します。

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*|*@filename*]

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。変数 *class* はクラス名を指定します。*record* はレコード名を示します。変数 *property* は、値を表示するプロパティのリストを示します。複数のプロパティを指定する場合は、各プロパティ名をスペースで区切ります。ファイルからプロパティ リストを読み込むには、*property* の代わりにアット マーク(@)を入力し、その後に(スペースを入れないで)ファイル名を指定します。各行に 1 つのプロパティが表示されている必要があります。 *property* 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。

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:

現在のディレクトリにあるローカル データベースの情報を表示するには、-r スイッチを指定せずに -dump オプションを使用します。このオプションを使用するには、eTrust Access Control が実行されていない状態のときに、ローカル データベースが格納されているディレクトリからユーティリティを起動する必要があります。-r スイッチを指定すると、認証エンジンで現在使用されているローカル データベース内のレコードに関する情報が表示されます。この場合、このユーティリティをローカル データベースがあるディレクトリから実行する必要はありません。このユーティリティは以下の機能を実行します。

- 指定したクラスの複数のレコード情報をダンプします。
- 指定したクラスの 1 つのレコード情報をダンプします。
- 指定したレコードを除く、1 つのクラスのすべてのレコード情報をダンプします。
- クラスおよびプロパティの定義のリストを生成します。

- 指定したユーザが属するグループのリストを生成します。
- 特定のクラスのレコードのリストを生成します。

-dump オプションまたは -dump −r オプションで指定できるスイッチは 1 つのみです。

データベースのエクスポート

このオプションは、sedb2scr ユーティリティに取って代わるものです。

構文

```
dbmgr [-h ] | {-e | -export} ¥
    [-l | -r] [-c(classes)] [-f(filename)]
```

オプション

-e|-export

ローカル データベースの複製に必要な selang のコマンドが含まれているスクリプトを作成します。

スイッチ

-c *classes*

指定されたクラスのデータのみをエクスポートします。各クラス名はスペースで区切ります。このスイッチは、-l スイッチまたは -r スイッチのいずれかと共に使用します。

-f *fileName*

指定したファイルにデータを書き込みます。このスイッチは、-l スイッチまたは -r スイッチのいずれかと共に使用します。

-h

ヘルプを表示します。すべてのオプションのヘルプを表示する場合は、「dbmgr -h」と入力します。使用しているオプションのヘルプのみを表示する場合は、「dbmgr -e」(-h は入力しなくても可)と入力します。

-l

現在のディレクトリで検出されたデータベースをエクスポートします。

-r

seosd 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。このオプションを使用できるのは、ADMIN 属性または SERVER 属性を持つユーザのみです。また、eTrust Access Control エンジンが稼動している必要があります。

注:

-export オプションを使用した場合、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が作成され、それらのコマンドが標準出力に書き込まれます。このスクリプトを使用すると、データベースを他の端末にコピーできます。

eTrust Access Control の実行中は、-l スイッチを指定してこのオプションを**使用しないでください**。eTrust Access Control の実行中に -l スイッチを呼び出すと、エラー メッセージが発行されます。

-f スイッチを使用し、生成されたコマンドをファイルに書き込みます。次に、この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が作成されます。

データベースのメンテナンス

このオプションは、dbutil ユーティリティに取って代わるものです。

構文

```
dbmgr [-h] | {-u | -util}
      -all  <filename> ¥
 -build <filename> ¥
 -close <filename>  ¥
 -dump  <filename> ¥
 -dup   <filename> <destfile>  ¥
 -f     <outfile>  ¥
 -free  <filename>  ¥
 -index <filename>   ¥
 -key   <filename>    ¥
 -load  <filename> <ASCIIfile>   ¥
 -scan  <filename>  ¥
 -scana <filename>   ¥
 -stat  <filename>
```

オプション

-u |-util

既存のデータベースをメンテナンスします。

スイッチ

-all *filename*

すべてのインデックスのチェックを実行します。インデックスを指定して、free スイッチを指定した場合と同じ機能を実行します。

-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。

-close

データベース ファイルを閉じます。

-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 *filename destfile*

ファイル ヘッダに基づいて DBIO ファイルをコピーします。ソース ファイルとコピー先ファイルの両方を指定する必要があります。

-f *outfile*

指定したファイルにデータを書き込みます。このスイッチは他のすべてのスイッチと共に使用できます。

-free *filename*

フリー インデックスをチェックします。

-h

ヘルプを表示します。すべてのオプションのヘルプを表示する場合は、「dbmgr -h」と入力します。使用しているオプションのヘルプのみを表示する場合は、「dbmgr -u」(-h は入力しなくても可)と入力します。

-index *filename*

インデックスの一貫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 *filename ASCIIfilename*

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

データベース ファイルのヘッダ情報を一覧表示します。

注:

-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。データベース インデックス ファイル(拡張子.001)では −util オプションを使用できません。

データベースのバックアップ

dbmgr −backup は、指定されたディレクトリに eTrust Access Control データベースをオンラインでバックアップする機能です。

この機能は、eTrust Access Control サービスが実行されているかどうかに関係なく利用できます。

バックアップ 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。ディレクトリが存在しない場合、dbmgr −backup オプションにより、指定したディレクトリが作成されます。

構文

```
dbmgr −backup | −b backup_directory
```

関連項目

この章の secons ユーティリティの説明。

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 レコードのデータをフラット ファイルにコピーする機能です。また、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モジュールを使用する必要があります。複数のバージョンがある場合は、最新バージョンを使用することを強くお勧めします。

構文

```
dbmgr migrate | -m switch [option]
```

スイッチ

-r *filename*

現在のディレクトリにあるデータベースを読み取り、コマンド ライン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。

-w *filename*

コマンド ライン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。

オプション

-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。Windows の GUI で作業している場合は、このオプションを指定する必要があります。

-s

データベースを直接読み取るのではなく、eTrust 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 スイッチを指定した場合にのみ有効です。-s を指定してコマンドを実行するには、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。

インポートされたデータの説明。

インポートされた USER データには以下の情報が含まれます。

- OLD_PASSWD – ユーザの古いパスワード(ユーザのパスワード履歴)
- PASSWRD_L_C – ユーザのパスワードが最後に更新された日時
- LAST_ACC_TERM – ユーザが最後にログインした端末
- LAST_ACC_TIME – ユーザ レコードが最後にアクセスされた日時

注:

-migrate 機能では、-s オプションを指定しない限り、常に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。

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。

セキュリティを向上させるために、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。

フラット ファイルはバイナリ フォーマットで書き込まれます。

例

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 C:¥Tmp¥old_db ディレクトリにあると仮定します。新しいデータベースは eTrustACdir/seosdb ディレクトリにあるとします(eTrustACdir は eTrust Access Control のインストール ディレクトリです)。

1. eTrust Access Control サービスが実行中の場合は、以下のコマンドを入力して停止します。

   ```
   > secons -s
   ```

2. 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。

3. データベースを C:¥Tmp¥old_db にコピーします。その後、古いデータベースで dbmgr ユーティリティを実行して、古いデータベースをコピーするスクリプトを作成します。

   ```
   > cd C:¥Tmp¥old_db
   > dbmgr -export -l > lang_script
   ```

4. 新しいデータベースを作成します。

   ```
   > cd .¥Program Files¥CA¥eTrustAccessControl¥data¥seosdb
   > dbmgr -c -c -u <Administrator name> -t <terminal name>
   ```

5. 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 .¥Program Files¥CA¥eTrustAccessControl¥data¥seosdb
   > selang -l C:¥Tmp¥old_db¥lang_script
   ```

6. 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 C:¥Tmp¥old_db
   > dbmgr -migrate -r flat_file
   ```

7. 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 .¥Program Files¥CA¥eTrustAccessControl¥data¥seosdb
   ```

```
> dbmgr -migrate -w C:¥Tmp¥old_db¥flat_file
```

レジストリの設定

-migrate 機能では、現在のディレクトリにあるデータベース ファイルを使用します。レジストリの設定は使用しません。

関連項目

- このセクションの dbmgr -export 機能の説明。
- この章の secons ユーティリティの説明。

dmsmgr

dmsmgr ユーティリティの機能

- eTrust Access Control がインストールされたコンピュータに DMS または DMA を作成します。

  注: これはインストール時に行うこともできます。
- eTrust Access Control コンピュータから DMS または DMA を削除します。
- DMS データベースから古いノードを削除します。

  これらは HNODE オブジェクトで、一定期間使用されなかった eTrust Access Control ノードを表します。

-create 機能 - DMS または DMA の作成

dmsmgr -create は、eTrust Access Control がインストールされたコンピュータに展開マップ サーバ(DMS)または展開マップ エージェント(DMA)を作成する機能です。

注: DMS または DMA はインストール時に作成することもできます。

```
dmsmgr -create -dms <name> [-admin <users>] [-desktop <hosts>]
dmsmgr -create -dma [<hosts>] [-admin <usernames>] [-desktop <hosts>] ¥
[-subscriber <dms_names>]
```

-admin *〈users〉*

(オプション)作成された DMS または DMA の管理者のリストをカンマで区切って示します。

注: 指定するかどうかに関係なく、ユーティリティを実行するユーザには、作成された DMS または DMA に対する管理権限が常に与えられます。

-desktop *〈hosts〉*

(オプション)DMS または DMA が作成されたコンピュータに対する TERMINAL アクセス権限を持つコンピュータのリストをカンマで区切って示します。

注: 指定するかどうかに関係なく、ユーティリティを実行する端末には、作成された DMS または DMA に対する管理権限が常に与えられます。

-dma [*〈hosts〉*]

カンマで区切った *〈hosts〉* の指定リストに DMA を作成します。ホストを指定しない場合は、ローカル コンピュータに DMA を作成します。

注: 適切なサブ管理権限があり、ユーティリティを実行しているコンピュータに、DMA をインストールするコンピュータに対する TERMINAL 権限が与えられている場合は、リモート コンピュータから DMA を作成できます。

-dms *〈name〉*

ローカル ホストに指定された *〈name〉* で DMS を作成します。

-subscriber *〈dms_names〉*

(オプション)作成された DMA の通知の送信先となる DMS ノードのリストをカンマで区切って示します。各 DMS は次の形式で指定します。
〈DMS_name〉@*〈hostname〉*.

-remove 機能 - DMS または DMA の削除

dmsmgr -remove は、eTrust 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 DMA を削除する機能です。

```
dmsmgr -remove {-dms <name> | -dma [<hosts>]}
```

-dms *〈name〉*

〈name〉 が指定された DMS をローカル ホストから削除します。

-dma [*〈hosts〉*]

指定された *〈hosts〉* のカンマ区切りリストから DMA を削除します。ホストが指定されていない場合は、ローカル コンピュータから DMA を削除します。

注: 適切なサブ管理権限があり、ユーティリティを実行しているコンピュータに、DMA を削除するコンピュータに対する TERMINAL 権限が与えられている場合は、リモート コンピュータから DMA を削除できます。

-cleanup 機能 - 古いノードの削除

dmsmgr -cleanup は、DMS データベースから古いノードを削除する機能です。削除されるノードは HNODE オブジェクトで、一定期間使用されなかった eTrust Access Control ノードを表します。

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

```
dmsmgr -cleanup <number> -dms <name>
```

-cleanup *〈number〉*

ユーティリティで HNODE オブジェクトを削除することを示します。このオブジェクトは *〈number〉* 日間以上使用されていない eTrust Access Control ノードを表します。

-dms *〈name〉*

古いノードを削除する DMS の *〈name〉* を示します。

defclass

各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 タイプを示します。

eTrust Access Control は、各 eTrust 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 タイプを示します。このスクリプトは、ユーザ定義のセキュリティのアセット タイプを eTrust Access Control データベースの eTrust Access Control クラスとして示します。

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。

構文

```
defclass.bat
```

DictImport

-f フラグを付けて eTrust Access Control データベースにインポートする辞書ファイルを作成します。

eTrust Access Control をインストールした後に、パスワード保護を設定するには、辞書ファイルを eTrust Access Control データベースにインポートして、アクティブにします。

DictImport プログラムによって作成された辞書ファイルは、-f コマンドを使用してインポートできます。

DictImport プログラムは use_dbdict パスワード ルールを db に設定して、DICTIONARY クラスと PASSWORD クラスをアクティブにします。

注: PASSWORD クラスがアクティブでない場合、集中管理される辞書は無効になります。

構文

```
eTrustACDir¥bin¥DictImport.exe switches ¥
[-o selangFilename] [-f dictionaryFilename] [-h]
```

スイッチ

-f *dictionaryFilename*

指定し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。

注: -f フラグを設定しない場合、seos.ini ファイルの[passwd]]セクションに定義されている辞書ファイルがインポートされます。

-h

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。

注: -o フラグが設定されていない場合、コマンドは標準出力に書き込まれます。

eacpg_gen

eacpg_gen はポリシー生成プログラムです。このユーティリティはメニュー選択方式で、eTrust Access Control アプリケーションのポリシーを簡単に定義できます。また、重要な資産に最適なセキュリティ対策を適用して、企業のアプリケーションやオペレーティングシステム、およびそれらの機密データを保護します。

構文

eacpg_gen –u *<username>* –g *<groupname>* –p *<programname, full path>* -*o* <.....>
(etc.)

オプション

-u *user*

プロセスを実行するユーザです。

-g *group*

プロセスを所有するグループ名です。

-p *path*

実行可能ファイルの完全パスです。

-o *owner*

ポリシーの所有者です。

-w *wheel*

secadmins グループとして設定します(推奨)。

-m *machine*

マシン名です。

-a *apply policy*

生成ルールを適用するかどうかを設定します。

-s *save policy to file*

ポリシー ルールを保存するときの完全パスとファイル名です。

-# *step 1-2*

この変数を「2」に設定します。

-x *toggle warn/fail mode*

警告モードとフェール モードを切り替えます。

注: 実行する前に、secadmin と secadmin グループがデータベースに存在することを確認してください。

ファイル

- eacpg_gen.exe
- eacpg_selang.exe
- eacpg_seaudit.exe
- eacpg_filter.exe
- eacpg_os.exe

eacpg ファイルは <eAC root dir>/bin/ ディレクトリに格納されています。

説明

アプリケーション セルは「デフォルト拒否」パラダイムを使用して作成されます。これらのポリシーは UNIX/Linux の chroot() jail の概念に類似しています。インターネット フェーシング アプリケーションにこのようなポリシーが生成されると、そのアプリケーションを介してホストが危険にさらされる可能性が大幅に低減します。

アプリケーション セルは、アプリケーションをブロックする ACL ルールです。アプリケーションごとに eacpg で多数のアプリケーション セルが生成されます。アプリケーション セルは特定のリソースに対してのみアクセスを実行します。セル ポリシーで保護されたプロセスは、ポリシーで明記してアクセス権が与えられないリソースにはアクセスできません。そのため、攻撃者はディスクの未許可領域に書き込んだり未許可バイナリを実行することはできません。

ポリシーは以下の手順に従って生成されます。

- 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

ユーザの視点

初期化

1. ポリシー生成プログラムを実行します。

   /eacpg_gen

2. システムを「警告」モードにします（プロンプトで「y」を入力します）。
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。次に例を示します。

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

4. ユーザ名を入力してプロセスを実行するか、Enter キーを押してデフォルトのユーザ名を使用します（デフォルトを推奨）。

5. プロセスを所有するグループ名を入力するか、Enter キーを押してデフォルトのグループ名を使用します(デフォルトを推奨)。
6. 情報が正しいことを確認します(プロンプトで「y」を入力します)。

アプリケーションの検査

1. アプリケーションの検査が開始しました。ポリシー生成プログラムによって、ポリシーを作成するプロセスに関する情報の収集が開始されます。

   画面の情報を確認して、Enter キーを押します。

アプリケーションのテスト

1. アプリケーションを開始します。次に例を示します。

   ```
   ./apachectl start
   ```

2. アプリケーションを停止します。次に例を示します。

   ```
   ./apachectl stop
   ```

これでアプリケーションが開始されて停止されました。アプリケーションを再度開始すると、通常の使用データを収集できます。この検査は何時間でも続けることができます。検査が長くなるとポリシー生成プログラムが収集するデータ量が増えるため、ポリシーも正確になります。十分にデータを収集できたら、次の手順に進みます。

ポリシーの生成

1. ポリシーをファイルに保存します(*filename*.txt を入力して、Enter キーを押します)。

ポリシーの適用

1. ポリシーを適用します(プロンプトで「y」を入力します)。
7. システムを「フェール」モードにして、ポリシーの適用を開始します(プロンプトで「y」を入力します)。

ポリシーのテスト

1. ポリシーをテストします。下の画面は、evil.html という名前のファイルに対するポリシー テストを示します。

```
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 this 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ているので、evil.html ファイルは使用できません。これは、ファイルが通常の使用プロファイルの範囲外になったためです。

eACoexist

eACoexist ユーティリティはローカル システムで共存するプログラム(eTrust Antivirus、Brightstor など)を検出します。Trusted プログラムが検出された場合は、eTrust Access Control SPECIALPGM ルールに登録し、アクセスのタイプを定義して、アクセスを許可するときに eTrust Access Control がバイパスできるようにします。アクセス タイプには DCM、PBF、PBN、STOP、および REGISTRY があります。アクセス タイプの詳細については、「*環境*のクラスと*プロパティ*」を参照してください。

共存するプログラムについて Access Control ではプラグイン *バイナリ モジュール*がサポートされます。プラグインは、製品 CD の Coexistence フォルダおよび eTrust Access Control インストール ディレクトリに格納されています。eACoexist ユーティリティを実行すると、このディレクトリへのパスがコマンド ラインに渡され、以下が実行されます。

1. プラグインを起動し、共存するプログラムに関する情報を受け取ります。各プラグインは以下の操作を行います。
   a. 共存するプログラムがローカル システムにインストールされているかどうかを検出します。
   b. 共存するプログラムのバージョンとホーム ディレクトリを検出します。
   c. 共存するプログラムの一部として存在するバイナリを検出します。
   d. 共存するプログラムの一部としてインストールされているサービスを検出します。
   e. 応答ファイルに結果を書き込みます。
2. eTrustAccessControl¥data ディレクトリに格納された response.ini に定義される情報に基づき、以下の 1 つまたは複数のアクションを実行します。
   - 共存するプログラムのサービスを停止します。
   - 共存するプログラムのサービスを開始します。
   - 共存するプログラムのバイナリまたはサービスに対する SPECIALPGM ルールを作成します。

   注: 最初の 2 つのアクションはインストール時とアンインストール時のみに実行されます。アクションは、response.ini ファイルのヘッダに示されるコードで識別されます。

response.ini ファイルには、共存する各プログラムのセクションがあります。セクション名に eTrust Audit-1.5 のようにバージョン番号が表示された場合は、特定のバージョンに対してのみアクションが実行されます。

構文

```
eACoexist plug-ins-path
```

引数

plug-ins-path

製品 CD の Coexistence フォルダまたは共存するプログラムのプラグインが格納されているインストール ディレクトリのパスを示します。

eACSigUpdate

eACSigUpdate コマンドを使用して、ローカル Stack Overflow Protection（STOP）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に置き換えます。

注: eACSigUpdate ユーティリティは、eTrust Access Control を起動すると自動的に実行されます。シグネチャ ファイル ブローカまたは親 Policy Model を定義した場合は定期的に実行されます。

eACSigUpdate <*hostname*> <*taget_file*>

〈hostname〉

このコンピュータにコピーする更新された 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示します。

注: コマンドを実行するには、リモート ホストの管理者権限が必要です。

〈taget_file〉

新しいシグネチャ ファイルの完全パスと名前を示します。これが、指定されたホストから取得したシグネチャの保存場所と名前になります。

eACSyncLockout

アカウントのロックアウトを eTrust Access Control データベースと同期させます(つまり、アカウント ロックアウトが発生すると、このアカウントに対応する eTrust Access Control データベース内のユーザ レコードが一時停止になります)。このユーティリティは、パスワードの同期が有効、**かつ**ユーティリティを実行しているユーザが ADMIN プロパティを保持している場合にのみ有効です。

構文

```
eACSyncLockout ¥
    -start | -stop | -remove ¥
    -p (password) ¥
    -u (user) ¥
```

引数

-p (*password*)

現在のユーザの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。引数としてパスワードを指定できます。

-remove

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再起動時には、このサービスは Service Control Manager に表示されません)。

-start

ユーザがパスワードを指定していないと仮定して、現在のユーザの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*)

ユーザがパスワードを指定していないと仮定して、引数に指定したユーザ 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。

注:「-u(*user*) -p(*password*)」と入力すると、パスワードを引数として、引数に指定したユーザのコンテキストでサービスがインストールされます。

ExportTngDb

ExportTngDb は、現在の Unicenter セキュリティ データをローカル eTrust Access Control データベースまたは PMDB に移行します。

構文

ExportTngDb.exe

オプション

/A

アセット タイプをローカル データベースに移行します。

/I:*casecdb*

/A オプションで必要になります。データのインポート元を指定します。

/O:*selang*

/A オプションで必要になります。データの出力方法を指定します。

/N:*nodeName*

eTrust Access Control のプッシュ テクノロジを使用するサテライト ノード(コンピュータ)が対象です。デフォルトでは、ローカル ノードです。

/S

サイレント モード(無人モード)でデータを移行します。

/L:*fileName*

すべての出力をログ ファイルに送信します。

説明

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

インストール プログラムで[Unicenter 統合]を選択すると、このプログラムが自動的に実行されます。

MigOpts

MigOpts は、現在の Unicenter セキュリティ環境をローカル eTrust 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するユーティリティです。

構文

MigOpts.exe

オプション

-d *pmdName*

任意の selang 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 eTrust Access Control データベースではなく)を更新する前に、eTrust Access Control の 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。

説明

MigOpts.exe は、現在の Unicenter セキュリティ環境を、ローカル eTrust 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するプログラムです。

インストール プログラムで[Unicenter 統合]を選択すると、このプログラムが自動的に実行されます。

新しい PMDB の作成時には、MigOpts プログラムを必ず手動で実行する必要があります。

ntimport

ntimport は、Windows 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するユーティリティです。

構文

ntimport <switches> <options>

オプション

-D

使用可能な最初のドメイン コントローラからユーザ情報とグループ情報を取得します。

-f *filename*

指定されたファイルに出力します。

-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*

ユーザとグループを pmdb の eTrust 環境にインポートするコマンドを生成します。

-pa *pmdb*

ユーザとグループを pmdb の eTrust 環境と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。

-pn *pmdb*

ユーザとグループを 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*

指定したリモート ホストからユーザ情報とグループ情報を取得します。

-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。

スイッチ

-a

-c スイッチ、-g スイッチ、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

プレフィクスにドメインを指定してユーザとグループをインポートします。

-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。

-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。名前は 40 文字に切り捨てられます。

-U

ユーザの Surrogate ルールをインポートする selang のコマンドを生成します。

注:

ntimport は、ユーザまたはグループをローカル eTrust Access Control データベースに追加するための Windows のコマンドを作成するユーティリティです。

通常、ntimport ユーティリティはインストール手順の一部として使用されます。

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 *filename* オプションを使用します。

policydeploy

ポリシーを DMS ノードに格納したり、Policy Model 階層または eTrust Access Control エンドポイントに格納されているポリシーを展開または展開解除する場合は、policydeploy ユーティリティを使用します。

```
policydeploy -store name -ds file1 -uds file2 [-dms list]
policydeploy -deploy name[#xx] -root dbs [-dms list]
policydeploy -undeploy name[#xx] -root dbs [-uds file2] [-dms list]
```

-deploy *name*[#*xx*]

格納ポリシーの指定されたバージョンを、定義された eTrust Access Control Policy Model 階層に展開するかどうかをユーザに尋ねるメッセージが表示されます。

格納されたポリシーの最新バージョンを展開する場合は、ポリシー バージョン番号を省略できます。

-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です。ポリシーを展開または展開解除する場合は、これらの DMS ノードはアクションの報告先になります。ポリシーを格納する場合は、これらの DMS ノードはポリシーの格納先になります。

このオプションで DMS を指定しない場合は、ローカル eTrust Access Control データベースで指定された DMS ノードがユーティリティで使用されます。

-ds *file1*

展開ルールが含まれているファイルのパス名を定義します。これらは、階層内の各コンピュータに展開するポリシーを作成するために必要なコマンドです。

重要: ポリシーの展開では、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展開スクリプト ファイルに含めないでください。UNIX/Linux(ネイティブ)selang の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。

-root *dbs*

ポリシーの展開または展開解除を行うデータベースのカンマ区切りリストを示します。

注: ルート データベースが親 Policy Model の場合、ポリシーはサブスクライブしているデータベース全体で展開または展開解除されます。ルート データベースが eTrust Access Control エンドポイントの場合、ポリシーは指定されたデータベースでのみ展開または展開解除されます。

-store *name*

ポリシー *name* の格納先を、コマンドで指定した DMS ノードにするかまたはローカル eTrust Access Control データベースにするかどうかを尋ねるメッセージが表示されます。

ポリシー *name* の前のバージョンが DMS に格納されていない場合は、ポリシーのバージョン 1 が作成されます(ポリシー *name*#01)。この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が作成されます(*名前*#*last_version+1*)。

注: ポリシー名には #(シャープ)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*

ポリシーの展開解除に必要なルールが含まれているファイルのパス名を示します。これらは、階層内のコンピュータからポリシーを展開解除するために必要なコマンドです。

ポリシーを展開解除する場合

- ポリシー展開解除スクリプトを指定しない場合は、格納されたポリシーに含まれている展開解除ルールからルールが取得されます。
- ポリシー展開解除スクリプトを指定しても、DMS には、新しいスクリプトではなく、ポリシーを格納したときに指定されたルールが引き続き記録されます。

-undeploy *name*[#*xx*]

指定したポリシー バージョン *name*#*xx* を、定義された eTrust Access Control Policy Model 階層から展開解除するかどうかを尋ねるメッセージが表示されます。

格納されたポリシーの最新バージョンを展開解除する場合は、ポリシー バージョン番号を省略できます。

policyreport

policyreport ユーティリティを使用して、Policy Model 階層についてホスト中心またはポリシー中心のレポートを作成します。

```
policyreport [-f] -name <name> -targetpath <path> -mode h -dms <name> ¥
-root <dbs> [-norec] [-dev] [-tree] [-hide p,d] -hn <hosts> -hstat <status> ¥
-sd <DD-MM-YYYY> -ed <DD--MM-YYYY> -st <HH:MM> -et <HH:MM>
```

```
policyreport [-f] -name <name> -targetpath <path> -mode p -dms <name> ¥
-root <dbs> [-norec] [-dev] [-hide p,d] -pn <policies> -pstat {<status>|None} ¥
-sd <DD-MM-YYYY> -ed <DD--MM-YYYY> -st <HH:MM> -et <HH:MM>
```

-dev

(オプション)偏差計算結果をレポートに含めるように指定します。

重要: 偏差計算では、ネイティブ ルールが適用されるかどうかはチェックされません。データベースからオブジェクト(ユーザまたはオブジェクト属性、ユーザまたはリソース権限、あるいは実際のユーザまたはリソース)を削除するルールも無視されます。たとえば、偏差計算では、以下のルールが適用されるかどうかは確認できません。
rr FILE /etc/passwd

-dms *〈name〉*

(オプション)情報の収集先の DMS ノードのカンマ区切りリストです。DMS を指定しない場合、レポート情報は *DMS__@localhost* から収集されます。

注: DMS ノードは次の形式で指定します。*〈DMS_name〉*@*〈hostname〉*

-ed *date*

フィルタ処理に使用する終了日を示します。指定日以後にステータスが変更されたリストは含まれません。*date* は *dd-mm-yyyy* 形式で指定します。

-et *time*

フィルタ処理に使用する終了時刻を示します。指定時刻以後にステータスが変更されたリストは含まれません。*time* は 24 時間表記の *hh:mm* 形式で指定します。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 *date*、-ed *date*、またはその両方と組み合わせて指定します。

-f

(オプション)ユーティリティを「強制」モードで実行することを指定し、すべての警告を無視します。

このオプションを使用して既存のレポートにコンテンツを追加します(または現在の情報でレポートを***更新***します)。同じレポート名を使用すると、ユーティリティを実行して、前回レポートを作成した後に更新されたか、元のレポートの作成時には含めなかったオプションまたはフィルタを使用して更新された領域のレポートを更新できます。

-hide {p|d|p,d}

(オプション)非表示にするレポートの列を示します。

p - [ポリシー]列を非表示にします。

d - [偏差]列を非表示にします。

-hn [*<hosts>*]

(オプション)レポートに含めるホストをフィルタ処理するホスト名マスクを示します。たとえば、-hn prod* を指定すると、ホスト名が prod から始まるコンピュータのみがホスト レポートに含まれます。

注: マスクを空白のままにすると、ワイルドカード、「*」を指定したことと同じになります。UNIX/Linux では、マスクを二重引用符で指定する必要があります。

-hstat [*<stats>*]

(オプション)レポートに含めるホストをフィルタ処理するホスト ステータス マスクを示します。ホスト ステータスには、Available、Unavailable、Sync(同期)、または Unknown があります。

注: マスクを空白のままにすると、ワイルドカード、「*」を指定したことと同じになります。UNIX/Linux では、マスクを二重引用符で指定する必要があります。

-mode {h|p}

生成されたレポートがホスト(h)中心かポリシー(p)中心かを示します。

-name *<name>*

レポートの名前を示します。レポート ファイル(XML および HTML)は、この名前を持つディレクトリに格納されます。

-norec

(オプション)-root フラグで指定したデータベースにのみ詳細なホスト レポートを作成するように指定します(それぞれのサブスクライバを含みません)。-root フラグにワイルドカード「*」を指定する際にこのオプションを使用すると、詳細レポートのサブセットを作成または更新できます。

-pn [*<policies>*]

(オプション)レポートに含めるホストをフィルタ処理するポリシー名マスクを示します。たとえば、-pn prod* を指定すると、名前が prod から始まるポリシーのみがポリシー レポートに含まれます。ポリシーのすべてのバージョンを含めるには、ポリシー名にサフィックス #* を追加します。

注: マスクを空白のままにすると、ワイルドカード、「*」を指定したことと同じになります。UNIX/Linux では、マスクを二重引用符で指定する必要があります。

-pstat [*<stats>*|None]

(オプション)レポートに含めるポリシーをフィルタ処理するポリシー ステータス マスクまたはカンマ区切りリストを示します。*None* を指定した場合は、ポリシー ステータスを持たないホストのみがレポートに含まれます。

ポリシー ステータスには、Deployed、Undeployed、Transferred、Deployed with Failures、Queued、Transfer Failures、Signature Faillures、Undeployed with Failures、Unknown があります。

注: マスクを空白のままにすると、ワイルドカード、「*」を指定したことと同じになります。UNIX/Linux では、マスクを二重引用符で指定する必要があります。

-root *<dbs>*

レポートに情報を含めるデータベースのリストをカンマ区切りで示します。

注: レポート情報は、指定する root データベースのすべてのサブスクライバ データベースについて再帰的に収集されます(-norec フラグを指定する場合または root データベースが eTrust Access Control エンドポイントである場合を除きます)。

-sd *date*

フィルタ処理に使用する開始日を示します。ステータスが指定した日付より前に変更されたリストは含まれません。*date* は *dd-mm-yyyy* 形式で指定します。

-st *time*

フィルタ処理に使用する開始時刻を示します。ステータスが指定した時刻より前に変更されたリストは含まれません。*time* は、24 時間表記の *hh:mm* 形式で指定します。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 *date*、-ed *date*、またはその両方と組み合わせて指定します。

-targetpath *<path>*

レポートを作成する場所の完全パスを指定します。

注: このフラグを指定しない場合は、レポートはデフォルトで以下の場所に生成されます。

<eTrustACDir>/data/reports/

-tree

(オプション)ホスト レポートに階層をグラフィカル表示するように指定します。

注: サブスクライバがレポートに含まれていると、このレポート タイプではフィルタ処理された親が引き続き表示されます。

seaudit

seaudit は、eTrust Access Control 監査ログを表示するユーティリティです。

権限

seaudit ユーティリティを実行するには、AUDITOR 属性が必要です。

ファイル

seaudit ユーティリティは、Windows のレジストリ サブキー HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥ eTrustAccessControl¥ の以下の値を使用します。

サブキー	値
logmgr	audit_back error_size
message	filename

詳細については、付録「レジストリ キー」を参照してください。

デフォルトでは、監査ファイルは *eTrustACDir*¥log¥seos.audit にあります（eTrustACDir は eTrust Access Control のインストール ディレクトリで、デフォルトでは、Program Files¥CA¥eTrustAccessControl です）。

構文

```
seaudit -h |{-a |-all} |   ¥
   {-i |-inet} host service |  ¥
   {-l |-login} user terminal |  ¥
   -nt | m       ¥
   {-r |-resource}(class)(resource)(user)|¥
   {-s |-start} |     ¥
   {-t |-table} |      ¥
   {-u |-update}command class record user | ¥
   {-w |-watchdog       ¥
   [-delim(delimiter) ]      ¥
   [-detail ]         ¥
   [-ed(date) ]         ¥
   [-et(time) ]         ¥
   [-f |-failure]       ¥
   [-fn |-filename] filename    ¥
   [-g |-grant] | [-gn |-grantnotify] ¥
   [-logout ]        ¥
   [-millenium ]      ¥
   [-n |-netaddr]      ¥
   [-notify ]         ¥
   [-o |-origin] host       ¥
   [-pwa ]         ¥
   [-sd(date) ]         ¥
   [-st(time) ]       ¥
   [-v |-servnum ]      ¥
   [-warn ]
```

スイッチ

-a

監査ログに送信されたレコード以外のすべてのレコードを表示します。

-h

例およびヘルプを表示します。

-i(*host service*)

service の *host* から受け取った TCP 要求の INET 監査レコードを一覧表示します。変数 *host* および *service* は、検索対象のホストおよびサービスを特定するマスクです。

-l(*user terminal*)

terminal 上の *user* について記録された LOGIN レコードを一覧表示します。*user* と *terminal* は両方ともマスクです。

-nt

Windows 環境のレコードのみを表示します。

-r(*class resource user*)

user の *resource* リソース上の *class* に関する一般的なリソース監査を一覧表示します。*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

eTrust Access Control エンジンの起動メッセージおよび停止メッセージを一覧表示します。

-t

ログ コードの表を表示します。

-u(*command class record user*)

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 の監査レコードを一覧表示します。

オプション

-delim(*delimiter*)

delimiter で指定した区切り文字を使用して各フィールドを区切ります。

-detail

各フィールドの詳細情報を表示します。

-ed(*date*)

終了日（*dd-mmm-yyyy*）を示します。指定した終了日より後にログに記録されたレコードはリストに表示されません。現在の日付を終了日として指定する場合は、文字列 *today* を使用します。現在の日付の *n* 日前を終了日として指定する場合は、文字列 today-*n* を使用します。

-et(*time*)

終了時間(*hh:mm*)を 24 時間表記で指定します。指定した終了時間より後にログに記録されたレコードはリストに表示されません。現在の時刻を終了時間に指定する場合は、文字列 *now* を使用します。現在の時刻の *n* 分前を終了時間として指定する場合は、文字列 now-*n* を使用します。

-f

失敗したレコードが表示されないことを示します。

-fn(*fileName*)

検索対象の監査ログの名前を示します。

-g

成功した(許可された)アクセスのレコードが表示されないことを示します。

-gn

通知レコードが作成された場合を除き、成功した(許可された)アクセスのレコードが表示されないことを示します。

-logout

ログアウト レコードが表示されないことを示します。

- millennium

年を下 2 桁ではなく 4 桁で表示することを示します。

-n

TCP/IP サービスをホスト名ではなくインターネット アドレスで表示することを示します。

-notify

通知監査レコードが表示されないことを示します。

-o(*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ことを示します。このオプションは、 selogrcd ログ ルーティング収集エンジ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

パスワード試行レコードが表示されないことを示します。

-sd(*date*)

開始日(*dd-mmm-yyyy*)を示します。指定した開始日より前にログに記録されたレコードはリストに表示されません。現在の日付を開始日として指定するには、文字列 *today* を使用します。現在の日付の *n* 日前を開始日として指定する場合は、文字列 today-*n* を使用します。

-st(*time*)

開始時間(*hh:mm*)を 24-時間表記で示します。指定した開始時間より前にログに記録されたレコードはリストに表示されません。現在の時刻を開始時間に指定する場合は、文字列 *now* を使用します。現在の時刻の *n* 分前を開始時間として指定する場合は、文字列 now-*n* を使用します。

-v

サービス名ではなく、ポート番号を表示します。

-warn

警告レコードが表示されないことを示します。

注:

(リソースの監査モード プロパティの指定に従って)リソースへのアクセスに監査が必要な場合、またはアクセスするユーザの監査モード プロパティでアクセス操作の監査が必要と指定されている場合は、eTrust Access Control の認証エンジンである seosd によってログ レコードが送信されます。このコマンドライン ユーティリティは、eTrust Access Control 監査ログからレポートを生成する場合に使用します。

パスワードが含まれる監査レコードを表示する場合は、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。

出力

seaudit で表示される各レコードには、列で構成されたデータが含まれています。最初の 3 列に表示されるデータの意味は、すべての種類のレコードで共通です。残りの表示データはレコードの種類によって異なります。以下の表に、最も一般的な種類のレコードの出力形式を列ごとに示します。

列	内容	説明
1	日付	アクセスされた日付またはアクセスが試みられた日付。
2	時刻	アクセスされた時刻またはアクセスが試みられた時刻。

列	内容	説明
3	リターン コード	結果を示す eTrust Access Control のリターン コード。有効な値は以下のとおりです。 D - アクセサに適切な権限がなかったため、リソースへのアクセスが拒否されたか、ローカル データベースの更新が許可されませんでした。 F - ローカル データベースの更新の操作が失敗しました。 M - eTrust Access Control が起動または停止しました。 O - ユーザがログアウトしました。 P - 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 - ローカル データベースの更新に成功しました。 U - Trusted 状態の PROGRAM または SECFILE が変更されたので、Untrusted になりました。 W - アクセサには指定されたリソースへの適切なアクセス権限がありませんでしたが、そのリソースに警告モードが設定されているため、アクセスが許可されました。
4	イベントの種類/クラス	監査対象のイベントの種類またはアクションが実行されたクラス。
5	アクセサ/クラス	前の列にクラス名が表示されている場合、この列には、そのコマンドを実行したアクセサの名前が表示されます。 前の列に UPDATE と表示されている場合、この列には、そのアクションが実行されたクラスの名前が表示されます。 それ以外の場合、この列には、コマンドを実行したアクセサの名前、またはクラスに関する適切な情報が表示されます。
6	アクセス タイプ/アクセサ	前の列にアクセサの名前が表示されている場合、この列には(該当する場合)アクセス タイプが表示されます。 前の列にクラス名が表示されている場合、この列には、そのコマンドを実行したアクセサの名前が表示されます。 それ以外の場合、この列にはアクセス タイプ(該当する場合)またはクラスに応じた情報が表示されます。
7	ステージ コード	eTrust Access Control が実行するアクションを決定したステージおよびその理由を示す最大 3 桁の数字。
8	監査レコード コード	eTrust Access Control の監査レコードに書き込まれた理由を示す数字。
9	リソース	この列には、アクセスされたリソースまたは更新されたリソースの名前が表示されます。

列	内容	説明
10	端末/ プログラム	列 4 に UPDATE と表示されている場合、この列には、更新を実行するために使用された端末の名前が表示されます。 それ以外の場合は、リソースにアクセスしたプログラムの名前が表示されます。
11	コマンド	列 4 に UPDATE と表示されている場合、この列には、アクセサが入力したコマンドの完全なコピーが表示されます。コマンドがパスワード更新の場合、パスワードの代わりにアスタリスクが表示されます。 列 4 に UPDATE と表示されておらず、リモート端末経由で CLASS オブジェクト上でアクションが実行されている場合、この列には、リモート端末の IP アドレスが表示されます。

seaudit で生成される出力は、一般的に以下のようになります。

```
07 Mar 99 17:42 P FILE      Dennis    Read 59  2
                ¥device¥harddisk0¥partition1¥file.txt
07 Mar 99 17:59 O LOGOUT     Bill           49  2
07 Mar 99 18:05 M START                        seosd
07 Mar 99 18:07 M SHUTDOWN    John             452 seosd
この出力の行ごとの解説を以下に示します。
07 Mar 99 17:42 P FILE      Dennis    Read 59  2
                ¥device¥harddisk0¥partition1¥file.txt
```

ユーザ Dennis は、1999 年 3 月 7 日 17 時 42 分にファイル ¥device¥harddisk0¥partition1¥file.txt の読み取りを許可されました。eTrust Access Control のステージ コードは 59(リソース UACC チェック)です。このユーザの監査レコードにあるコード 10(ユーザ監査モード)は、すべてのタイプのアクセスの監査を必要とするため、イベントが監査ログに記録されます。

```
07 Mar 99 17:59 O LOGOUT     Bill           49  2
```

ユーザ Bill がシステムからログオフしました。eTrust Access Control では、システム内で終了したプロセスのほとんどが把握されていて、ユーザ Bill のクレデンシャルに関連するすべてのプロセスが終了すると、Bill はシステムからログオフしたものとみなされます。LOGOUT クラス エントリおよび返された列の O は、ログアウト レコードを特定します。コード 49 は LOGOUT 監査レコードを表します。コード 2 は、ユーザの監査モードの設定に従ってイベントが記録されたことを表します。ユーザのログアウトは、ユーザのログインが報告された場合にのみ報告されます。

```
07 Mar 99 18:05 M START                        seosd
07 Mar 99 18:07 M SHUTDOWN    John             452 seosd
```

この監査レコードは、eTrust Access Control エンジンである seosd の起動および停止を表します。Seosd が 18 時 05 分に開始され、John によって 18 時 07 分に停止されました。John には ADMIN 属性があるので seosd を停止することが許可されました。これを示すのが理由コード 452 です。リターン コード M は、seosd の起動または停止を表します。

例

操作	コマンド
2003 年 1 月 3 日以降のすべての監査レコードを一覧表示します。	`seaudit -a -sd 03-Jan-2003`
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します。	`seaudit -r FILE \* John`

操作	コマンド
昨日の 17:00 から今日の 08:00 までに記録されたすべての監査レコードを一覧表示します。	`seaudit -a -st 17:00 -et 08:00`
今日の 08:00 から 17:00 までに記録されたすべての監査レコードを一覧表示します。	`seaudit -a -st 08:00 -et 17:00`
昨日の監査レコードをすべて一覧表示します。	`seaudit -a -sd today-1 -ed today-1`

sechkey

sechkey は、さまざまな eTrust Access Control プログラムの暗号化鍵を変更するユーティリティです。

構文

```
sechkey [-d]| [-h] |[-s <registry path>]
```

パラメータ

-d

eTrust Access Control のデフォルトの暗号化鍵を復元します。

-h

ヘルプを表示します。このユーティリティでは、ヘルプを表示するために -h スイッチを入力する必要があります。

-s *registry-path*

eTrust Access Control プログラムの暗号化鍵が保存されているレジストリ ルート パスを示します。

注:

パラメータを指定せずに「sechkey」と入力した場合、新しい暗号化鍵を入力するように指示するメッセージが表示されます。

注: sechkey ユーティリティを実行する前に、DOS ウィンドウで secons -s コマンドを実行して eTrust Access Control を停止します。eTrust Access Control の再起動後に、新しい暗号化鍵の使用が開始されます。eTrust Access Control を再起動するには、seosd -start コマンドを実行します。Windows タスクバーの[スタート]ボタンから、SeStart ユーティリティおよび SeStop ユーティリティを実行することもできます。

sechkey ユーティリティは以下の 2 種類のプログラムで使用できます。

- 通信を保護するために常に暗号化鍵が使用される eTrust Access Control プログラム グループ(*eTrustACDir*¥bin にある SeOSAgent、selang、seosd、および sepmdd)。
- eTrust Access Control API を使用して作成され、eTrust Access Control サービスと通信するプログラム。これらのプログラムの通信は、デフォルトの eTrust Access Control 暗号化鍵を使用して暗号化されます。

通信を正常に実行するには、これらのすべてのプログラムに同じ暗号化鍵を使用する必要があります。Windows の場合、暗号化鍵を変更すると、sechkey によって eTrust Access Control データベース内のすべてのプログラムの暗号化鍵が同時に変更されます(UNIX/Linux の場合は、1 つのプログラムの暗号化鍵を変更せずに、別のプログラムの暗号化鍵を変更できます。ただし、一方のプログラムの暗号化鍵だけを変更すると、2 つのプログラム間の通信が正常に実行できなくなります)。

暗号化鍵が異なるためにホスト間で正常に通信できないという問題を回避するには、Windows および UNIX/Linux のいずれの環境でも、1 つのホストで暗号化鍵を変更したら、そのホストと通信するすべてのホストでも暗号化鍵を変更する必要があります。

コメント

- 旧バージョンの eTrust Access Control では、デフォルトの暗号化鍵を使用することによってのみ、Windows コンピュータと UNIX/Linux コンピュータの両方に接続できました。sechkey を使用して暗号化鍵が変更されると、UNIX/Linux コンピュータとの通信が実行できなくなりました。これは、UNIX/Linux コンピュータおよび Windows コンピュータでの鍵の暗号化がそれぞれ異なる規則に従って異なる方法で行われるためです。その結果、Windows コンピュータと UNIX/Linux コンピュータは互いに相手を認識できなくなりました。

  eTrust Access Control バージョン 4.1 のパッチ 4 以降では、UNIX/Linux と Windows に同じ形式の鍵暗号化が使用されています。したがって、sechkey ユーティリティを使用すると、Windows コンピュータから UNIX/Linux コンピュータに接続する場合でも、通信に影響を及ぼすことなく暗号化鍵を変更できます。

  ネットワークで旧バージョンの eTrust Access Control for Windows を使用している場合は、最新バージョンの *eTrustACDir*¥bin¥sechkey.exe ファイルを旧バージョンの同名のディレクトリにある同名のファイルに上書きして、sechkey ユーティリティを更新する必要があります。

- 暗号化鍵の最大文字数は 55 文字です。

seclassadm

seclassadm は、ローカル データベースに新しいクラス(ユーザ定義クラス)を追加するユーティリティです。

ファイル

seclassadm ユーティリティでは、ローカル データベース ファイルが現在のディレクトリにある場合は、それらのファイルが使用されます。

重要: 高度なポリシー ベース管理およびレポートを使用する場合は、eTrust Access Control データベースでクラスを追加または削除するときやクラス プロパティを追加または削除するときに、eTrust Access Control 初期データベース(init_ac_db)で同じ操作を行う必要があります。このデータベースは、ポリシー偏差計算に使用されます。このデータベースは、init_ac_db レジストリ エントリによって指定されているパス(デフォルトでは *<eTrustACDir>*¥data¥devcalc¥init_ac_db)にあります。

構文

```
seclassadm [-h] | {-add |-del |-upd} classname ¥
[-a modes]-d access] |[-f] |[-g] |[-n] |[-o] |[-p]
```

コマンド

-add(*className*)

既存のローカル データベースに新しいリソース クラスを追加します。*className* は新しいクラスの名前です。eTrust Access Control では、すべて大文字のクラス名が予約されています。そのため、クラスを追加する場合は、クラス名に小文字を 1 文字以上使用する必要があります。クラス名の最大文字数は 15 文字です。

新しいクラスを追加した後に、selang の setoptions コマンドを使用してクラスを有効にする必要があります。詳細については、「eTrust 環境の selang のコマンド」の章の setoptions の説明を参照してください。

-del(*className*)

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(*className*)

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。このコマンドの構文は、以下のとおりです。

```
Seclassadm -upd <ClassName> {-|+}c
```

c スイッチは、クラスの大文字と小文字の機能の変更を示します。{-|+} は、クラスが大文字と小文字が区別されるオブジェクトをサポートするかどうかを示します(- を指定した場合、大文字と小文字が区別されるオブジェクトはサポートされません)。その他のスイッチは、入力しても無視されます。

スイッチ

-a(*modes*)

クラスのアクセス モードを設定します。文字列 *modes* 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 - 管理
D	delete - 削除
E	create - 作成
F	filescan - ファイル スキャン
M	chmod - モード変更
O	chown - 所有者変更
R	read - 読み込み
S	security - セキュリティ
T	utime - タイムスタンプの変更
U	update - 更新
V	rename - 名前の変更
W	write - 書き込み
X	execute - 実行

-d(*access*)

クラスのデフォルトのアクセス権限(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ユーザに割り当てられるアクセス権限)を設定します。これは、authorize コマンドで使用される暗黙的なアクセス権限であり、リソースに割り当てられるデフォルトのアクセス権限とは異なります。有効なアクセス タイプについては、「-a(mode)」のリストを参照してください。アクセス権限を指定する場合、アクセス タイプを示す文字は任意の順序で指定可能です。ただし、文字列には空白または英文字以外の文字を使用できません。

-f

クラス名がすべて大文字の場合でも、eTrust Access Control が新しいクラス名を受け入れるようにします。

-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、ローカル データベースの TERMINAL クラスと GTERMINAL クラスの関係に類似しています。

原則として、既存のクラスのメンバをグループ化するリソースの名前には、既存のクラス名の先頭に大文字の G を付けた名前を指定します。

-n

指定した名前のファイルに出力を書き込みます。

-o

指定したデフォルト アクセス権限を持つクラスの _default オブジェクトを作成します。

-p

ローカル ホスト データベースの完全パスの場所。

-r

このクラスに(eTrust Web Access Control クラスの)リソース記述オブジェクトがあることを示します。

-t

このクラスが Unicenter TNG クラスであることを示します。

注:

- seclassadm ユーティリティは、ローカル データベースが格納されているディレクトリから起動する必要があります。
- eTrust Access Control サービスの実行中は、このプログラムを使用できません。
- 指定できるコマンドは 1 つだけです。
- スイッチの指定は省略できます。また、複数のスイッチを指定することもできます。

- 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、*dbmgr -c* を使用して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。新しいデータベースを作成するたびにこの手順を繰り返す必要があります。

例

操作	コマンド
dbfield というリソース クラスを追加します。	`seclassadm -add dbfield`
読み取り専用アクセス権限を持つ report というリソース クラスを追加します。	`seclassadm -add report -d R -a R`
読み取り、書き込み、および変更許可を持ち、指定がない場合はデフォルトとして読み取りアクセス権限を持つ batch_jobs というリソース クラスを追加します。	`seclassadm -add batch_jobs -d R -a RWM`
CLASS クラス内のレコードをグループ化し、実行アクセス権限およびデフォルトの実行アクセス権限を持つリソース クラスを追加します。	`seclassadm -add GCLASS -d X -a X -f -g`

secons

secons は、eTrust Access Control エンジンの管理コンソールを提供するコマンド ライン ユーティリティです。secons は、以下のようなさまざまな機能を実行します。

- eTrust Access Control 認証エンジンのトレース機能を管理します。
- 同時ログインを制御します。
- 実行時の統計情報を表示します。
- ローカル端末または 1 台以上のリモート端末上で実行中の eTrust Access Control エンジンおよびその他の eTrust Access Control サービスをすべて停止します。

権限

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が使用できるのは、オプション -m のみです。

eTrust 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だけです。リモート端末上の eTrust Access Control を停止できるのは、そのリモート端末で ADMIN または OPERATOR として定義されたユーザだけです。

ファイル

secons ユーティリティは、Windows のレジストリ サブキー HKEY_LOCAL_MACHINE¥Software¥ComputerAssociates¥ eTrustAccessControl の以下の値を使用します。

サブキー	値
SeOSD	trace_file trace_file_type trace_space_saver trace_to

これらのトークンの詳細については、付録「レジストリ キー」を参照してください。

デフォルトでは、トレース ファイルは *eTrustACDir*¥log¥seosd.trace にあります（eTrustACDir は eTrust Access Control のインストール ディレクトリです。デフォルトは Program Files¥CA¥eTrustAccessControl です）。

構文

secons <options>

オプション

-d+

ユーザの同時ログインを有効にします。

-d-

ユーザの同時ログインを無効にします。

-ds

ユーザの同時ログイン ステータスを表示します。

-file *FName*

¥Program Files¥CA¥ eTrustAccessControl¥log¥seosd.trace 以外に指定したファイルの参照を開始します。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。

-i

実行時統計情報を取得して、以下の「出力」のセクションで説明するさまざまな情報を書式付きテキストで表示します。

-l+

一般同時ログインを有効にします。

-l-

一般同時ログインを無効にします。

-ls

一般同時ログイン ステータスを表示します。

-m *message*

コンソールにメッセージを送信し、eTrust Access Control 認証エンジンによって作成されたトレース ファイルにテキストを追加します。

-reflP [*hosts*]

eTrust Access Control がネットワーク リソース用の IP アドレスを更新するホストのスペース区切りリストを示します。リストにホストが含まれていない場合は、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すると、現在の IP アドレスで eTrust Access Control リソースを更新することができるので、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。

注: 特定のホストが正常に更新されるには、そのホストが DNS によってすでに更新されている必要があります。DNS を手動で更新するには、Windows の ipconfig /flushdns コマンドを使用します。

-s [*host*|*ghost list*]

eTrust Access Control エンジンを停止します。eTrust Access Control エンジンは、その他の eTrust Access Control サービスを停止した後に停止します。*host* および *ghost* には、1 台のホストまたはホスト グループを指定するか、またはホストおよびホスト グループのリストを指定できます。リストのメンバはスペースまたはカンマで区切ります。*host* または *ghost* を指定しないと、ローカル端末でのみサービスが停止されます。

-t+

トレースを有効にします。その結果、eTrust Access Control エンジンの 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。このオプションを使用できるのは、ADMIN 属性または OPERATOR 属性を持つユーザだけです。

-t-

トレースを無効にします。その結果、eTrust 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。このオプションを使用できるのは、ADMIN 属性または OPERATOR 属性を持つユーザだけです。

-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。このオプションを使用できるのは、ADMIN 属性または OPERATOR 属性を持つユーザだけです。

-ts

現在のトレース ステータスを表示します。このオプションを使用できるのは、ADMIN 属性または OPERATOR 属性を持つユーザだけです。

-tt

トレース ステータスの有効化および無効化を切り替えます。このオプションを使用できるのは、ADMIN 属性または OPERATOR 属性を持つユーザだけです。

-tv [*KBytes*]

参照を開始し、オンライン トレース ビューを表示します。このオプションを使用できるのは、ADMIN 属性を持つユーザだけです。

KBytes を指定すると、UNIX/Linux の tail-f ユーティリティと同様の方法で、トレース ファイルの参照が開始され、オンライン トレース ビューが表示されます。KB 単位でサイズを指定して、出力を制限します。デフォルト値は 2 です。0 を指定すると、トレース ファイル全体が表示されます。

この操作を中止するには、Ctrl キーを押しながら C キーを押します。

-u+ *UName*

ユーザ(*UName*)の同時ログインを有効にします。

-u- *UName*

ユーザの同時ログインを無効にします。

-us *UName*

ユーザの同時ログイン ステータスを表示します。

出力

-i オプションで生成される画面出力は以下のようになります。

```
# ¥Program Files¥CA¥eTrustAccessControl¥bin¥secons-i
secons eTrust Console Utility

Run-Time 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      :    0
Database info  :( record count & First Free Id)
    Classes     :    18 ( CID   0x0012 )
    Properties   :   223 ( PID   0x00df )
    Objects     :   152 ( OID 0x00000a8 )
    PropVals    :   972 ( N/A )
#
```

この出力の説明を以下に示します。

```
INet Statistics:

    Requests Denied    : 0
    Requests Granted   : 17
    Errors found       : 0
```

ここには、クラス HOST がアクティブなときに、eTrust Access Control が受信した受信接続アクティビティの認証要求の数に関する統計が表示されます。これらの行には、許可されないまたは許可された要求の数、および要求の認証時に発生したエラーの数の合計が表示されます。

```
Queues Size:

    Audit Log: 0
    Error Log: 0
```

eTrust 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、一部のイベントがメモリに保持され、少し後でログ ファイルに書き込まれることがあります。これらの値が 10 を超えると、エラーが発生して eTrust Access Control 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 :   0
```

- ACEE(アクセサ エントリ エレメント)は、ログイン プロセスが記録されるテーブルです。
- Protected clients には、キャッシュされたクライアントの数が表示されます。通常、この値は 0 です。
- Trusted Programs には、メモリにキャッシュされた PROGRAM クラスのエントリの数が表示されます。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 には、Untrusted プログラムとして識別されたプログラムの数が表示されます。

```
Access Control Database: Record Count & First Free Id

    Classes           :    18 ( CID   0x0012 )
    Properties        :   223 ( PID   0x00df )
    Objects           :   152 ( OID 0x00000a8 )
    PropVals          :   972 ( N/A )
```

ここには、ローカル 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の数についての全般的な情報が表示されます。

例

操作	コマンド
eTrust Access Control を停止します。	`secons -s`
リモート端末 remoteStat1 および remoteStat2 で実行中の eTrust Access Control を停止します。	`secons -s remoteStat1 remoteStat2` 端末が正常に停止したことがユーザに通知されます。eTrust Access Control で remoteStat1 の停止に失敗した場合でも、remoteStat2 の停止は行われます。
eTrust Access Control のトレース ファイルに文字列「Start Event」を挿入します。	`secons -m 'Start Event'`
実行時の統計情報を表示します。	`secons -i`

segrace

このコマンド ライン ユーティリティは、ユーザのさまざまなログイン設定を表示します。このユーティリティは、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。

segrace 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、ユーザが最後にログオンした日時と端末などを表示するコマンド ライン ユーティリティです。

注:

- segrace を起動する前に、システム管理者は、以下のコマンドを入力して eTrust 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ます。

- パラメータを指定せずに segrace を起動し、ユーザの猶予ログインがない場合は、何も表示されません。

構文

segrace options [userName]

オプション

-d

サーバで設定されているデフォルトの *警告日数* パラメータとは異なる警告日数を設定します。

-h

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 の間にパスワードの有効期限が切れる場合、またはユーザに猶予ログイン回数がある場合、パスワード警告を表示します。

-s

eTrust Access Control データベースが使用されるリモート サーバの名前を示します。

パラメータ

userName

ADMIN 属性がある場合にユーザ名を指定すると、指定したユーザに必要なデータが segrace によって表示されます。

ユーザ名を指定しないと、現在のユーザのログインの詳細が表示されます。

SegraceW

この Windows GUI ユーティリィティは、ユーザのパスワードの有効期限が切れているかどうか、およびユーザに猶予ログイン回数があるかどうかをチェックします。パスワードの有効期限が切れている場合は、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、eTrust Access Control 以外の環境でスタンドアロン モジュールとして実行できます。そのため、このユーティリティは、ドメイン内の任意のワークステーションに適用できます。

SegraceW は、最初に(NT 4.0 環境の)プライマリ ドメイン コントローラへの接続を試みます。接続に失敗した場合にのみ、バックアップ ドメイン コントローラが検索されます。Windows 2000 以降の環境の場合、SegraceW は、検出された最初のドメイン コントローラへの接続を試みます。

注: SegraceW の実行オプションでリモート ホストが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、およびユーザに猶予ログイン回数があるかどうかをチェックします。

ユーザの猶予ログイン回数属性が存在する場合、以下の処理が行われます。

- ユーザの猶予ログインの残り回数が 0 の場合は、ユーザにパスワードを変更するように求めるメッセージが表示されます。
- ユーザの猶予ログインの回数が残っている場合は、ユーザにパスワードの変更を勧めるメッセージが表示されます。

ユーザに猶予ログイン回数がない場合は、パスワードの有効期限のステータスがチェックされます。

- パスワードの有効期限がサーバ側で設定されている*警告日数*パラメータの値よりも長い場合、何の処理も行われません。
- パスワードの有効期限がサーバ側で設定されている*警告日数*パラメータの値と同じか短い場合、パスワードの変更を進めるメッセージが表示されます。
- ユーザのパスワードの有効期限が切れている場合は、ユーザにパスワードを変更するように求めるメッセージが表示されます。

パスワードを変更するときは、ユーザに古いパスワードと新しいパスワードの確認入力を求める[パスワードの変更]ダイアログ ボックスが表示されます。

パスワード確認チェックの後、ドメイン コントローラの SAM データベースでパスワードが更新されます。

注:

ドメイン環境への SegraceW 実装に関する最良の方法を以下に示します。

1. selang から以下のコマンドを入力して、eTrust Access Control のパスワード チェックをアクティブにします。

   ```
   setoptions class+(PASSWORD)
   ```

2. eTrust Access Control のレジストリ ツリーで、レジストリ キー HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥eTrustAccessControl¥SeOSD¥LogonInterceptionMethod の値を 1 に変更し、eTrust Access Control サービスを再起動してログオン インターセプトのサブ認証方法を有効にします。

3. NETLOGON 共有に新しいディレクトリを作成して、以下のファイルをコピーします。

   - %SystemRoot%¥system32¥psapi.dll
   - %SystemRoot%¥system32¥activeds.dll
   - %SystemRoot%¥system32¥adsldpc.dll
   - <eTrust Access Control ルート ディレクトリ>¥Bin¥SegraceW.exe
   - eTrust Access Control 暗号化パッケージ DLL。この名前は、以下のレジストリ キーの値です。

     KEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥eTrustAccessControl¥Encryption Package

     このファイルをコピーした後、ファイル名を defenc.dll に変更します。

4. <新しいディレクトリの名前(上記の 3 番目の項目)>¥SegraceW.exe を呼び出すログオン スクリプトを ¥¥<サーバ名>¥NETLOGON に作成して、Profile セクションでユーザの Logon Script Name を設定し、新しく作成したスクリプトを実行します。

構文

```
segracew options
```

オプション

-d

サーバで設定されているデフォルトの ***警告日数***パラメータとは異なる警告日数を設定します。

-s *remote host*

指定されたリモート ホストに接続して情報を取得します。

selang

selang ユーティリティは、eTrust Access Control データベースおよび Windows 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。selang のコマンドの詳細については、このマニュアルの「eTrust 環境の selang のコマンド」を参照してください。

-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。

ファイル

selang ユーティリティでは以下のファイルを使用します。

- *.selangrc

  *.selangrc ファイルは -r オプションのデフォルト ファイルです。このファイルは、selang を起動するたびに自動的に実行される selang のコマンドのファイルです。

  注: このファイルが必要な場合は利用者が作成する必要があります。

- インデックス ファイルおよびシェル ファイル。これらのファイルは編集しないでください。
  - lang.idx
  - lang.shl

構文

```
selang [-h ] | [-c(command) ] ¥
    [-f ] | [-r ] (filename) ]        ¥
    [-d(dbdirectory)] | [-l ] | [-p(policymodelname)] ¥
    [-o(filename)]           ¥
    [-s ] [-v]
```

オプション

-c(*command*)

command で指定したコマンドを実行して終了します。*command* に空白が含まれる場合は、文字列全体を二重引用符で囲みます。次に例を示します。

```
selang -c "showusr rosa"
```

-d(*dbdirectory*)

指定されたディレクトリにあるデータベースを更新します。このオプションは、seosd が実行されていない場合にのみ有効です。

-f(*fileName*)

端末の標準入力からではなく、指定されたファイルからコマンドを読み込みます。入力ファイルのコマンドが実行された場合は、その時点で実行中のコマンド ラインの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。*fileName* で指定されたコマンドの実行後に、selang が終了します。

-h

ヘルプを表示します。

-l

ローカル データベースを更新します。このオプションは sedlang に取って代わるものです(このコマンドは、シェル スクリプトである sedlang によって呼び出されます)。このオプションは、seosd が実行中でない場合のみ有効で、データベースに ADMIN 属性を持つユーザだけが実行できます。

-o(*fileName*)

指定されたファイルに出力を書き込みます。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(*policyMode/Name*)

指定された PMDB のデータベースを更新します。このデータベースは、ローカル ステーションに存在する必要があります(これは PMDB サブディレクトリです)。データベースに対する変更内容は、サブスクライバに伝達されません。

注: 指定された PMDB 上で sepmdd または seosd のいずれかが実行中の場合、このオプションは無効です。また、このオプションは、*hosts* コマンド(109 ページ)の使用とは異なります。

重要: このモードでは、伝達が必要な変更は行わないでください。更新を行うときにネイティブ モードを使用すると、eTrust Access Control では、(seos.ini ファイルで定義されている)ネイティブ ホスト ファイルだけが更新されます。

-r(*fileName*)

指定されたファイルからコマンドを読み取ります。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。 *fileName* で指定された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。*fileName* を指定しないと、ユーザのホーム ディレクトリにある *.selangrc ファイルが使用されます。

-s

著作権に関するメッセージを表示しません。

-v

出力にコマンド ラインを書き込みます。

使用方法

画面プロンプト

selang 環境では、特別な selang のプロンプトが画面に表示されます。表示されるプロンプトの形式は、作業環境によって異なります。たとえば、以下のように表示されます。

```
eTrustAC>
```

Windows 環境で作業をする場合は、env(nt) コマンドを発行します。以下のプロンプトが表示されます。

```
eTrustAC(nt)>
```

pmdb 環境で作業をする場合には、env(pmd) コマンドを発行します。以下のプロンプトが表示されます。

```
eTrustAC(pmd)>
```

ほかにネイティブ環境および UNIX/Linux 環境を選択できます。

標準のスマート機能

tcsh およびその他のスマート シェルで使用できる多数のコマンド ライン入力機能がサポートされます。

特殊文字

以下の特殊文字がサポートされます。

- *
  行の先頭にある場合、その行がコメント行であることを示します。この行は実行されません。コメント行は、ファイルから selang のコマンドを入力する場合に役立ちます。
- !
  行の先頭にある場合、その行がシェル コマンドであることを示します。そのコマンドは eTrust Access Control では実行されません。コマンドはオペレーティング システムのシェル プログラムに送られて実行されます。
- **上方向の矢印**または**下方向の矢印**または ^
  以下の説明に従って、履歴リストからコマンドを取得します。
- ¥
  行末の円記号は、コマンドが次の行に続くことを示します。
- ;
  1 つのコマンドを終了し、同じ行に別のコマンドを指定します。
- | *パイプ*
  指定された*パイプ*にコマンド出力を送ります。
- **タブ**
  文字列の単語入力を補完します。Ctrl+D キーの説明を参照してください。

- Ctrl+D
  行末にカーソルを置いてこのキーを押すと、コマンド ラインの単語補完文字列に一致する単語のリストが表示されます。

  行末以外の場所にカーソルを置いてこのキーを押すと、カーソルの右側にある文字が削除されます。

- Esc Esc
  コマンド ラインのコマンドのヘルプ テキストが表示されます。コマンド ラインのテキストはすべて保存されるため、入力を中断した位置から続けてコマンドを入力できます。

長い行

1 行につき 1 つのコマンドのみを入力します。次の行に続けてコマンドを入力するには、行末に円記号(¥)を入力します。

履歴

実行したコマンドは***履歴リスト***に保存されます。履歴リストに保存されたコマンド ラインのコマンドを表示するには、上下の矢印キーを使用します。特定の文字で始まるコマンドのみを表示するには、コマンドの先頭文字を入力した後に上方向キーおよび下方向キーを使用します。Enter キーを押すと、コマンド ラインに現在表示されているテキストが実行されます。

selang のコマンド シェルでは、以下のショートカットを使用して、履歴リストに保存されたコマンドを実行できます。

指定する文字	実行されるコマンド
^^ [string]	1 つ前のコマンド。*string* を指定した場合は、*string* が元のコマンドに追加されます。
^n [string]	履歴リストの *n* 番目にあるコマンド(*n* は正の整数)。*string* を指定した場合は、*string* が元のコマンドに追加されます。
^-n [string]	履歴リストの最後から *n* 番目のコマンド(*n* は正の整数)。*string* を指定した場合は、*string* が元のコマンドに追加されます。
^mask [string]	*mask* で指定した文字で始まるコマンドの中で最後に発行したコマンド(*mask* はテキスト文字列)。*string* を指定した場合は、*string* が元のコマンドに追加されます。

コマンド ラインの編集

コマンド ラインのテキストは編集可能です。矢印キーで行内を移動します。コマンド ラインに直接文字を挿入すること、および標準の Backspace キー、Delete キー、または Ctrl+D キーを押して文字を削除することができます。

入力時のショートカット

selang のコマンド シェルでは、入力の手間を省くさまざまなテクニックを使用できます。

コマンド認識

selang コマンド シェルでは、他の使用可能なコマンドと区別できるだけの文字数を入力すると、ただちに目的のコマンドが認識されます。たとえば、「ho」で始まるコマンドは hosts コマンドのみです。「ho」と入力すると、目的のコマンドが hosts であることが認識されます。一方、文字列 new で始まるコマンドはいくつもあります。newusr、newgrp、newfile、および newres を区別するには、識別に必要な文字数を入力する必要があります。

省略形

各コマンドには 1 文字から 4 文字の省略形が関連付けられています。たとえば、文字列 new で始まるコマンドは複数存在するので、newusr コマンドの代わりに省略形の nu も使用できます。省略形については、このマニュアルの「eTrust 環境の selang のコマンド」で、各コマンドのコマンド構文の一部として説明しています。コマンド入力では大文字と小文字は区別されません。ただし、レコード名およびクラス名の大文字と小文字は区別されます。

単語補完

単語の入力途中で Tab キーを押すと、残りの文字が自動的に入力されます。単語補完では状況に応じた処理が行われます。入力した文字列に一致する単語が複数存在する場合は、最も短い単語またはその文字列に一致する単語の一部が表示されます。たとえば、「n」と入力した場合、自動的に ew が追加され、単語 new が表示されます。

new が目的の単語ではない場合、さらに 1 つまたは複数の文字を入力し、Tab キーをもう一度押して文字列を完成します。Ctrl キーを押しながら D キーを押すと、使用できるすべての選択肢が表示されます。この機能は、使用するコマンドが正確にわからない場合に役立ちます。単語「new」の次に「u」と入力して Tab キーを押すと、自動的に「sr」が追加され、newusr コマンドが表示されます。

selang のコマンドの一部ではない単語はメモリに保存され、後で同じセッションの単語補完に使用されます。たとえば、「newusr Mercedes」と入力し、しばらくしてから「showusr Me」と入力して Tab キーを押すと、以下のように「Me」から「Mercedes」に単語が補完されます。

```
showusr Mercedes
```

ここでは、「Me」で始まるユーザ名がほかに入力されていないことを前提としています。

semsgtool

semsgtool は、以下の機能を実行するユーティリティです。

- eTrust 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。
- メッセージを一覧表示します(サブ文字列を含む)。

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保存場所は、*eTrustACDir*¥data¥seos.msg です(*eTrustACDir* は、eTrust Access Control のインストール ディレクトリです)。

構文

```
semsgtool [-h] | [-b |-build] asciiSourcefile outputMessagefile |      ¥
    [-d |-dump] [messagefile ] |
    ¥
    [-l |-list] [messagefile(section) ] |
    ¥
    [-s |-show] messagefile {(hexerrorcode) | (section#msg#)} |          ¥
    [-number | -n] [message-file] <sub-str>
```

メッセージを一覧表示します(サブ文字列を含む)。

```
[-change | -c] [message-file] [0x<error-code> | <section# msg#>] <new-message>
```

メッセージを新しいメッセージに変更します。[message-file].new という形式で新しいメッセージ ファイルを作成します。

オプション

-b *asciiSourceFile outputMessageFile*

ASCII ソース ファイルから新しい eTrust Access Control メッセージ ファイルを作成します。

-c *message-file hexerrorcode section# msg# new-message*

特定のメッセージ コードまたはセクション番号および新しいメッセージ(逆向きカンマで区切られた文字のセット)を指定すると、hexerrorcode に関連付けられたメッセージが新しいメッセージに置き換えられます。この処理で作成された新しいメッセージ ファイルには、「.new」拡張子が付けられます。古いメッセージ ファイルは変更されません。パラメータ messageFile を指定した場合は、レジストリ サブキー HKEY_LOCAL_MACHINE¥Software¥ComputerAssociates¥ eTrustAccessControl¥mqessage のファイル名の値で指定されているメッセージ ファイルが使用されます。メッセージ コードには、16 進数、またはセクション コードおよびメッセージ コードを指定する 2 つのパラメータを指定します。セクション コードまたはメッセージ コードには、10 進数または 16 進数を指定することもできます。16 進数の前には 0x を付けます。

-d *messageFile*

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 eTrust Access Control メッセージ ファイルを作成する際に使用できます。

-l messageFile(*section*)

ファイル *messageFile* の指定され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。パラメータ *messageFile* を指定しないと、レジストリ サブキー HKEY_LOCAL_MACHINE¥Software¥ComputerAssociates¥ eTrustAccessControl¥message のファイル名の値で指定されているメッセージ ファイルが使用されます。セクション番号は 16 進数または 10 進数を指定できます。16 進数の前には 0x(ゼロ x)を付けます。

-n *message-file 〈sub-str〉*

逆向き文字で区切られた文字列を入力すると、その文字列が含まれているすべてのメッセージが一覧表示されます。各メッセージのエラー コードが一覧表示されます(16 進数および 10 進数)。

-s *messageFile hexerrorcode section#msg#*

メッセージ コードまたはセクション番号を指定すると、それに関連付けられたメッセージが表示されます。パラメータ messageFile を指定しないと、レジストリ サブキー HKEY_LOCAL_MACHINE¥Software¥ComputerAssociates¥ eTrustAccessControl¥message のファイル名の値で指定されているメッセージ ファイルが使用されます。メッセージ コードには、16 進数、またはセクション コードおよびメッセージ コードを指定する 2 つのパラメータを指定します。セクション コードまたはメッセージ コードには、10 進数または 16 進数を指定することもできます。16 進数の前には 0x を付けます。

注: eTrust 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 eTrust 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。

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、以下のように入力します。

  ```
  semsgtool -s seos.msg 0x205
  ```

  エラー コード 0x205 に関連付けられたメッセージが一覧表示されます。

- セクション 0x2500 のメッセージを一覧表示するには、以下のように入力します。

  ```
  semsgtool -l seos.msg 0x2500
  ```

  セクション 0x2500 のすべてのメッセージが表示されます。

- 変更済みの eTrust Access Control メッセージ ファイルを作成するには、以下のコマンドを入力します。

  1. cd <*message_file_folder*>

     <*message_file_folder*> は、メッセージ ファイルが存在するディレクトリです。次に例を示します。

     ```
     ¥Program Files¥CA¥eTrustAccessControl¥data
     ```

  2. semsgtool -c seos.msg 0x2501 "This is the new message"

     変更されたメッセージと共に、新しいメッセージ ファイル(seos.msg.new)が作成されます。

  3. copy seos.msg.new seos.msg

     古い seos.msg ファイルに加えて、新しいメッセージ ファイルと変更されたメッセージがコピーされます。

sepmd

sepmd は、PMDB を管理するユーティリティです。このユーティリティは、1 台のホスト上で複数の PMDB をサポートします。

- サブスクライバ データベースのリストの管理
- Policy Model のエラー ログの表示または消去
- PMDB の更新情報が含まれているファイルの消去

重要: Policy Model エンジンは、Windows のタスク マネージャを使用して停止しないでください。

権限

- sepmd を実行するには、ADMIN 属性、および PMDB ディレクトリとファイルに対する書き込み許可が必要です。
- PMDB を停止するには、Policy Model の管理者である必要があります。つまり、PMDB で ADMIN 属性が割り当てられているか、Policy Model が格納されている端末で OPERATOR 属性が割り当てられている必要があります。

ファイル

sepmd では以下のファイルを使用します。

- updates.dat
- error_log
- Windows レジストリ

構文

```
sepmd [-h ] | [-k ] | [-S ] |  ¥
     [-c ] | [-C  ] | [-cl ] |     ¥
     [-dl ] | [-e ] |  ¥
     [-l ] | [-L ] | [-p ] |  ¥
     [-kl ] | [-ri ] | [-n ]  ¥
     [-sl] pmd       ¥
     [-t pmd {auto | offset } ] |  ¥
     [-r ] | [-u ] pmd subscriber |  ¥
     [-s ] pmd subscriber [offset] |   ¥
     [-sm] pmd mfsubscriber mftype mfsysid mfadmin [offset]]
```

スイッチ

-c

Policy Model エラー ログを消去します。

-C

指定した PMDB の更新ファイルにあるコマンドを表示します。

-cl

Policy Model のログ ファイルを消去します。

-dl

Policy Model のログ ファイルを表示します。

-e

Policy Model のエラー ログを表示します。

-k

Policy Model サービスを非アクティブ化(kill)します。UNIX/Linux とは異なり、Windows では、このオプションを使用しても Policy Model サービスを停止できません。

-kl

Policy Model のログ ファイルへの記録を停止します。

-l

Policy Model のサブスクライバを一覧表示します。

-L

Policy Model のサブスクライバ、および更新ファイル内のサブスクライバのオフセットを一覧表示します。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最初の更新情報の位置を示します。

-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的なルールについては、-s オプションの説明を参照してください。このオプションによって、PMDB 全体の内容が新しいサブスクライバに送信されます。

-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ができることを示します。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 eTrust Access Control エンドポイントまたは PMDB から別の PMDB にサブスクライブする場合、新しいサブスクライバにすでに存在するポリシー(POLICY オブジェクト名)を新しい親 PMDB に含めることはできません。ポリシーを新しい親 PMDB にサブスクライブするには、サブスクライバに存在する各ポリシーを展開解除した後に、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する必要があります。

-p

ホストに格納されている Policy Model およびそのステータスを一覧表示します。

-r

Policy Model サービスの 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、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、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、このパラメータを指定した場合、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。

-ri

Policy Model 情報をレジストリからホストに再ロードします。変更したデータを確実にホスト PMDB に送信するには、このスイッチを使用します。

-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。

Policy Model にサブスクライブする場合、サブスクライブされる PMDB の Windows レジストリ サブキーの parent_pmd エントリの値に、親 PMDB の名前が設定されている必要があります。

-S

Policy Model をアクティブ化(起動)します。

-sl

Policy Model のログ ファイルへの記録を開始します。

-sm

メインフレーム コンピュータを Policy Model にサブスクライブします。

-t [*offset*]

更新ファイル updates.dat からエントリを削除して、ファイルを切り捨てます。

-t を指定すると、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。

以前に sepmd -L を実行したことがあり、ファイルを切り捨てるオフセット(ファイルの先頭から特定のサブスクライバまでの距離)がわかっている場合は、*offset* で指定します。指定したオフセットで更新ファイルが切り捨てられます。ただしその前に、指定されたオフセットは更新ファイル内の既存のレコードに一致するように調整されます。

サブスクライバが、指定したオフセットより前にある更新情報を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強制実行するには、以下の操作を行います。

a. 更新されなかった端末のサブスクライブを解除します。

b. ファイルを切り捨てます。

c. 端末を再度 Policy Model にサブスクライブします。

この操作を行った場合、サブスクライバが Policy Model から更新を受け取れないことが 1 回以上発生します。サブスクライバがサブスクライブ解除された状態のときに Policy Model に対して行われた変更は、再度サブスクライブしても伝達されません。

-t auto

すべてのサブスクライバに伝達されたトランザクションを削除し、可能な最大のオフセットで更新ファイルを切り捨てます。

-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(アンサブスクライブ)します。

パラメータ

PolicyModel

Policy Model の名前です。

Subscriber

サブスクライバ端末またはサブスクライバ PMDB のホストのフル ネームまたは IP アドレス。

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。
- ホストを Policy Model にサブスクライブする場合、Policy Model はサブスクライバ端末の親 PMDB である必要があります。つまり、Windows レジストリの HKEY_LOCAL_MACHINE¥Software¥ComputerAssociates¥ eTrustAccessControl¥ eTrustAccessControl サブキーの parent_pmd 値として Policy Model の名前を設定する必要があります。
- Policy Model を他の Policy Model にサブスクライブするには、以下の条件が満たされている必要があります。
  - サブスクライブされる Policy Model が定義済みで、初期化されていること。
  - Policy Model がサブスクライバ PMDB の親 PMDB であること(Windows レジストリ サブキー HKEY_LOCAL_MACHINE¥Software¥ComputerAssociates¥ eTrustAccessControl¥eTrustAccessControl の parent_pmd 値として親 PMDB の名前を設定する必要があります)。

sepropadm

sepropadm は、eTrust Access Control データベースのプロパティを管理するユーティリティです。

sepropadm は、データベースでプロパティの追加、更新、および削除を行うユーティリティです。このユーティリティは、eTrust Access Control デーモンが**実行されていない**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 では、必ず eTrust Access Control テクニカル サポート担当者に認証された説明ファイルを使用してください。

重要: 高度なポリシー ベース管理およびレポートを使用する場合は、eTrust Access Control データベースでクラスを追加または削除するときやクラス プロパティを追加または削除するときに、eTrust Access Control 初期データベース(init_ac_db)で同じ操作を行う必要があります。このデータベースは、ポリシー偏差計算に使用されます。このデータベースは、init_ac_db レジストリ エントリによって指定されているパス(デフォルトでは *<eTrustACDir>*¥data¥devcalc¥init_ac_db)にあります。

構文

```
sepropadm file
```

パラメータ

file

eTrust Access Control サポート担当者が作成する説明ファイルです。説明ファイルには以下の形式を使用します。

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。

シャープ記号(#)で始まる行が 1 行必要です。この行は、記述行より前に配置する必要があります。

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
```

新しいプロパティを更新する記述行は、以下の形式に従う必要があります。

```
CLASS=%s OBJECT=%s PROPERTY=%s VALUE=%s
```

新しい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
```

ファイル

eTrust Access Control データベース ファイルを使用します。

例

説明ファイルのサンプルを以下に示します。

```
; Sample Patch File for the eTrust 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
```

関連項目

この章の dbmgr ユーティリティ、seclassadm ユーティリティ、および lang.ini ユーティリティの説明。

sereport

データベースおよび Policy Model 情報の HTML レポートを作成します。このレポートには Web ブラウザを使用してアクセスできます。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。

構文

sereport -r|-report *number* -f|-file *filename* [-h help] [-host *hostnames*]

スイッチ

-r | report *number*

表示するレポート番号です。

-f | -file *filename*

出力ファイル(レポート)のパスおよび名前です。

注: 指定されたファイルの内容は HTML 形式で構造化されるので、*.html* 拡張子を指定する必要があります。

オプション

-h

ヘルプを表示します。

-host *hostnames*

レポートに含めるホストの名前です。ホスト名はカンマで区切ります。このスイッチは省略できます。指定しない場合、sereport は localhost に適用されます。

注:

- sereport を使用するには、クエリを実行するすべてのデータベースに対する READ 権限が必要です。
- sereport を活用するには、Web ブラウザが必要です。

レポート

sereport のほとんどのパラメータは、以下のレジストリ キーで定義されています。

[HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥eTrustAccessControl¥Report]

このキーには、各レポートのサブキーおよび値が含まれています。レポート、対応するレジストリ キー、および説明を以下の表に示します。

レポート番号	タイトルおよび説明	レジストリ キー	値
1	Administrative Privileges（管理特権） 指定されたユーザの管理特権を表示します。	admin_report	Hostname Object_pattern User_Mode
2	Login Limitation（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	Hostname Object_pattern Properties User_Mode
3	Dormant Accounts（休止状態のアカウント） アクティブでないアカウントを日付（日数）別に表示します。 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	Dormant_account Hostname Object_pattern User_Mode
4	Last Login（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	Hostname Object_pattern User_Mode
5	パスワード変更 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 Hostname Object_pattern User_Mode
6	Warning Mode（警告モード） 警告モードのオブジェクトが含まれているリソースを表示します。	warning_report	Class_Name Hostname Object_pattern
7	Untrusted Programs（Untrusted プログラム） Untrusted モードのプログラムを表示します。	untrust_report	Hostname Object_pattern

レポート番号	タイトルおよび説明	レジストリ キー	値
8	Users' Privilege Access Rights（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	Accessor Class_Name Hostname Object_pattern
9	Compare users/groups in databases（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	Hostname Object_pattern
10	Compare Protected Resources（保護されているリソースの比較） 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 Hostname Object_pattern
11	Compare Access Rights（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 Hostname Object_pattern
12	Compare Users' Information（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	Hostname Object_pattern Properties

レポート番号	タイトルおよび説明	レジストリ キー	値
13	Compare PMDB and Subscriber（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（同一）と報告されます。	pmdb_compare	Class_Name Hostname Object_pattern

上の表に一覧表示されているレジストリ値の意味およびその他の一般的な値の意味を以下に示します。

Accessor

アクセサの選択パターン(マスク)。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。

Days_to_Change

パスワード変更を要求されるまでの残り日数。

Dormant_account

アカウントが休止状態とみなされる期間。

Hostname

データを取得するホストのリスト。

Object_pattern

オブジェクトの選択パターン(マスク)。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。

User_Mode

カンマで区切られたユーザ モードのリスト。

title

レポートのタイトルの色を示します。

class_title

レポートの class_title の色を示します。

logo

ロゴを作成します。ロゴは、完全パスで入力する必要があります。

seretrust

seretrust は、プログラムおよび保護対象ファイルを再度 Trusted 状態にするために必要な selang のコマンドを生成するユーティリティです。

構文

```
seretrust switches path
```

スイッチ

-a

データベース プロパティに関係なく、すべてのレコードに対して retrust コマンドを生成します。

Base_path

指定したディレクトリ内に定義されているレコードのみを処理します。- プレフィクスを指定せずにこのパラメータを使用すると、パスは現在のパスであるとみなされます。Base_path を指定しないと、空のディレクトリであるとみなされます（すべてのレコードが処理されます）。

-h

このユーティリティのヘルプを表示します。

-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取得します（このスイッチは、サービスが実行されている場合は適用されません）。このスイッチを省略すると、このセッションの処理対象となるデータベースは、eTrust Access Control Engine サービスで使用するデータベースと同じになります。

-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。

パラメータ

path

再度 Trusted 状態にするプログラムのパスを示します。指定したディレクトリとそのサブディレクトリがすべて処理されます。

説明

eTrust Access Control データベースには、SECFILE クラスと PROGRAM クラスの 2 つのクラスがあります。これらのクラスにより、eTrust Access Control はリソース（実行可能ファイルおよびファイル）を監視できるようになります。SECFILE クラスおよび PROGRAM クラスのリソースが変更されると、eTrust Access Control 管理者に通知されます。

Watchdog は、指定されたリソースを指定された間隔（レジストリで設定）でチェックし、リソースの整合性に関する判断を行います。変更が検出されると、リソースは Untrusted 状態になり、監査レコードは監査ログに送信されます。

その結果、変更されたリソースが eTrust Access Control データベースで Trusted リソースとして定義されることがあります。これは、リソースが変更された後に Watchdog チェックがまだ行われていない場合に発生します。

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報告します。seretrust では、Watchdog が把握していない場合でも、プログラムが変更されたかどうかを確認できます（したがって、これらのプログラムは、eTrust Access Control データベースで Trusted としてマークが付けられたままです）。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:

- データベースのすべての Trusted プログラムおよび保護対象ファイルを再度 Trusted 状態にするコマンドが含まれているスクリプトが生成されます。
- 出力は、標準出力デバイスに送信されます。ファイルに出力するには、リダイレクト コマンドを実行します。
- -l パラメータを省略すると、seretrust は、再度 Trusted 状態にするプログラムおよびファイルのリストを eTrust Access Control サービスから取得します。

sesudo

あるユーザが別のユーザの権限でコマンドを実行します。

sesudo は、他のユーザ(***ターゲット*** ユーザ)の権限を借りて 1 つまたは複数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、通常のユーザでも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と禁止されているユーザの両方を指定できます。

構文

sesudo {-h | -list | -do *record* [*parameters*]}

オプション

-h

ヘルプ画面を表示します。

-list

sesudo に使用可能なコマンドを一覧表示します。これは、eTrust Access Control データベースで定義されている SUDO レコードのリストです。

-do *record* [*parameters*]

指定されたコマンドを sesudo ユーティリティを使用して実行します。コマンドの名前は、SUDO クラス(420 ページ)内のレコードの名前です。SUDO レコードで許可されている場合は、コマンドに追加パラメータを渡すこともできます。

注: SUDO レコードの定義については、「**管理者ガイド**」を参照してください。

サービスの詳細

このセクションでは、eTrust Access Control のサービスをアルファベット順に示し、各サービスについて詳しく説明します。

sepmdd

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 eTrust 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。Windows では、sepmdd は「eTrust Access Control Policy Model」というサービスとして実行されます。各 Policy Model は、開始または停止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。HKEY_LOCAL_MACHINE¥Software¥ ComputerAssociates¥eTrustAccessControl¥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 eTrust Access Control エージェントを使用して 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。Policy Model のエラー ログに関する詳細については、「**管理者ガイド**」の「Policy Model の管理」を参照してください。

eTrust Access Control は、Policy Model に追加されたサブスクライバまたは Policy Model から削除されたサブスクライバを完全に修飾しようとします。

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するには、以下のように入力します。

```
sepmd -r policyModel subscriber
```

サブスクライバ データベースで更新が拒否された場合（サブスクライバ データベースと PMDB が異なる場合など）、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んで処理を続行します。

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
```

Policy Model サービスを非アクティブ化するには、以下のコマンドを入力します。

```
sepmd -k policyModel
```

フィルタ メカニズム

PMDB では、以下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、以下のレジストリ 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。次に例を示します。

```
HKEY_LOCAL_MACHINE¥Software¥ComputerAssociates¥eTrustAccessControl¥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、ETRUST、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 eTrust 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に GROUPS および FULLNAME を含めた場合、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ます。各プロパティは、「eTrust 環境のクラスとプロパティ」に記載されているとおり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 および NOPASS です。

注: 任意のフィールドで、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以下に示します。

CREATE	eTrust	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）	プロパティ	処理方法

たとえば、この行が含まれているファイルの名前が Printer1_Filter.flt で、レジストリ キー HKEY_LOCAL_MACHINE¥Software¥ComputerAssociates¥ eTrustAccessControl¥Pmd¥PM-¥Filter に「D:¥Program Files¥CA¥eTrustAccessControl¥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、監査者など）を持つ eTrust Access Control の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/Linux）
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/Linux）
READ	list
START	start devcalc
UNDEPLOY	deploy-（展開解除）

注: eTrust 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 には、以下のレジストリ キーに独自のサブキーがあります。
HKEY_LOCAL_MACHINE¥Software¥ComputerAssociates¥ eTrustAccessControl¥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。

sepmdd ユーティリティでは、Policy Model が格納されている端末で以下のレジストリ サブキーの値が使用されます。

値	説明	デフォルト
Min_Retrys	使用不可のサブスクライバに対する最小アクセス試行回数。アクセス試行がこの回数を超えると、sepmdd は非アクティブ状態になります。実際の試行回数は、ここで指定した回数より多くなる場合があります。サブスクライバを更新せずに sepmdd の実行を停止した場合、次回起動時に、そのサブスクライバの更新が試行されます。	4
Active_Policy	アクティブな Policy Model の名前。	*Policymode lName*
Always_Propagate	Policy Model で実行できないトランザクションを Policy Model からサブスクライバに伝達するかどうかを決定します。たとえば、Windows で失敗したトランザクションが UNIX/Linux ホストに伝達されたときに実行することがあります。この値に no を設定した場合、実行に失敗したコマンドは伝達されません。	yes
Auto_Truncate	伝達されたエントリを更新ファイルから切り捨てます。この値を no に設定すると、更新ファイルを手動で切り捨てることができます。詳細については、このマニュアルに記載されている sepmd ユーティリティの -t スイッチの説明を参照してください。	yes
Filterj	フィルタ ファイルのディレクトリ パス。	
Parent_PMD	親 PMD(存在する場合)のディレクトリ パス。	

その他のファイル

その他の特別なファイルは使用されません。

注:

- selang を使用し、(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てください。PMDB がそれ自体にサブスクライブされた場合、Policy Model がブロックされるか、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/Linux 環境で selang を使用して 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。
- UNIX/Linux 環境で selang を使用して Policy Model を更新する場合は、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/Linux 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。

関連項目

「eTrust Access Control for UNIX and Linux ユーティリティ ガイド」の seagent ユーティリティ、sepmd ユーティリティ、および sepmdadm ユーティリティの説明。

第 6 章: eTrust 環境のクラスとプロパティ

このセクションには、以下のトピックが含まれます。

クラスとプロパティの情報

この章では、eTrust Access Control データベースで定義されているクラスの各プロパティについて説明します。変更可能なプロパティ、それらのプロパティを更新する際に使用する selang のパラメータ、およびそれらのパラメータを指定するコマンドに関する情報をクラス別にまとめてアルファベット順に示します。

注: USER クラス、GROUP クラス、または FILE クラスのように、eTrust 環境とネイティブ環境の両方にあるクラスもあります。両方の環境で同じプロパティ名が使用されている場合は、それらのプロパティが同一のものか、別々のものかが明記されています。

変更できるプロパティと変更できないプロパティのすべてが、クラス別に一覧表示されます。どちらのプロパティについても、以下の情報が示されます。

- **プロパティ名** – eTrust Access Control データベースに登録されているプロパティの名前。
- **説明** – プロパティの機能および目的の説明。

さらに、変更可能なプロパティの説明では、プロパティを変更するために使用する selang のコマンドおよびパラメータを示します。

注: マイナス記号(-)を付けてパラメータを入力すると、データベースからそのパラメータが削除されます。たとえば、comment で適切なテキストを指定すると、データベースレコードにコメントが追加されますが、comment- を指定すると、データベースからコメントが削除されます。レコードを作成する場合は、パラメータにマイナス記号を付けることはできません。

各プロパティ リストの最初に記載される説明部分では、クラスのレコードの**キー**を定義します。キーは、新しいレコードの作成時に指定するレコード識別子です。レコードの作成が完了すると、キーは変更できないプロパティになります。

データベースには、アクセサ クラスとリソース クラスという 2 種類のクラスがあります。アクセサ クラス(USER および GROUP)のレコードを操作する場合は、リソース クラスに対して使用する selang のコマンド セットとは異なるコマンド セットを使用します(ポリシー マネージャでは、異なるワークスペースを使用します)。

- USER クラスのレコードを操作するには、chusr、editusr、および newusr を使用します。
- GROUP クラスのレコードを操作するには、chgrp、editgrp、および newgrp を使用します。
- リソース クラスのレコードを操作するには、chres、editres、および newres を使用します。リソースがファイルの場合は、chfile コマンドまたは editfile コマンドを使用することもできます。
- レコードのプロパティを一覧表示するには、showgrp、showres、showfile、または showusr を使用します。

- リソース レコードの ACL を追加、変更、または削除するには、authorize および authorize- を使用します。

注: edit(編集)では、new(新規作成)と change(変更)の操作を実行できます。つまり、chusr または newusr の代わりに editusr を使用できます。

selang のコマンドの詳細については、このマニュアルの「eTrust 環境の selang のコマンド」を参照してください。

アクセサ クラス

このセクションでは、eTrust AC データベースのアクセサ クラスである USER クラスおよび GROUP クラスについて説明します。

USER クラス

USER クラスの各レコードは、データベース内でユーザを定義します。

USER レコードのキーは、ユーザがシステムへのログイン時に入力するユーザ名です。USER クラスのレコードの変更可能なプロパティについて以下に説明します。

変更可能なプロパティ

APPLIST

eTrust Single Sign-On および eTrust Web Access Control で使用されます。

APPLIST_TIME

eTrust Single Sign-On および eTrust Web Access Control で使用されます。

APPLS

ユーザが明示的にアクセスを許可されているアプリケーションのリストです。eTrust Single Sign-On および eTrust Web Access Control で使用されます。

AUDIT_MODE

eTrust AC が監査ログに記録するアクティビティを識別します。以下のアクティビティの任意の組み合わせを指定できます。

- ログへの記録を行わない
- トレース ファイルに記録されたすべてのアクティビティ(UNIX/Linux のみ)
- 失敗したログイン
- 成功したログイン
- eTrust AC によって保護されているリソースに対する失敗したアクセス
- eTrust AC によって保護されているリソースに対する成功したアクセス

USER クラスのレコードの AUDIT_MODE プロパティの値は、GROUP クラスのレコードの値よりも優先されます。

このプロパティを変更するには、chusr コマンド、editusr コマンド、または newusr コマンドで audit パラメータを使用します。

AUTHNMTHD

ユーザに対して使用する 1 つまたは複数の認証方法(method 1 から method 32、または none)です。eTrust Single Sign-On および eTrust Web Access Control で使用されます。

BADPASSWD

eTrust Single Sign-On および eTrust Web Access Control で使用されます。

CALENDAR

eTrust AC のユーザ、グループ、およびリソース制限の Unicenter TNG カレンダ オブジェクトを表します。eTrust AC は、一定の間隔で Unicenter TNG のアクティブなカレンダを取得します。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで calendar パラメータと calendar- パラメータを使用します。

CATEGORY

ユーザに割り当てる 1 つまたは複数のセキュリティ カテゴリです。CATEGORY クラスに定義されている任意のセキュリティ カテゴリを指定できます。リソースに 1 つまたは複数のセキュリティ 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。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで category[-] パラメータを使用します。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。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。このプロパティで指定する情報は、ネイティブ環境の COMMENT プロパティで指定する情報と同じです。個別に情報を変更することはできません。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで comment[-] パラメータを使用します。

COUNTRY

ユーザの国記述子を指定する文字列です。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。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで country パラメータを使用します。

DAYTIME

ユーザがリソースにアクセスできる日時を管理する、曜日と時刻の制限です。USER クラスのレコードの DAYTIME プロパティの値は、GROUP クラスのレコードの値よりも優先されます。このプロパティの情報は、eTrust AC のデータベースでは分単位を含む時間が使用できること以外は、ネイティブ環境の DAYTIME プロパティの情報と同じです。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで restrictions(days and time) パラメータを使用します。

EMAIL

最大 128 文字のユーザの電子メール アドレスを示します。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで email パラメータを使用します。

EXPIRE_DATE

USER クラスのレコードが失効して無効になる日付です。USER クラスのレコードの EXPIRE_DATE プロパティの値は、GROUP クラスのレコードの値よりも優先されます。失効したレコードを元に戻すには、chusr コマンドで expire- パラメータを使用します。失効したユーザを再開することはできません。一時停止したユーザは、再開日を指定することで再開できます。

このプロパティを変更するには、chusr コマンド、editusr コマンド、または newusr コマンドで expire パラメータか expire- パラメータを使用します。

FULLNAME

ユーザに関連付けられたフル ネームであり、最大 256 文字の英数字からなる文字列です。フル ネームは、eTrust AC の監査ログ メッセージでユーザを識別するために使用されますが、権限付与に使用されることはありません。

このプロパティを変更するには、chusr コマンド、editusr コマンド、または newusr コマンドで name パラメータを使用します。

GAPPLS

ユーザがアクセスを許可されているアプリケーション グループのリストです。eTrust Single Sign-On および eTrust Web Access Control で使用されます。

GRACELOGIN

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に達するとユーザはシステムへのアクセスを許可されないため、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。

猶予ログイン回数には、0 から 255 までの値を設定する必要があります。**この値が 0 の場合、ユーザはログインできません。**

USER クラスのレコードの GRACELOGIN プロパティの値は、SEOS クラスのレコードの PASSWDRULES プロパティよりも優先されます。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで grace[-] パラメータを使用します。

GROUPS

USER クラスのレコードが属するユーザ グループ（GROUP クラスのレコード）のリストです。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。

このプロパティを変更するには、join[-] コマンドで group パラメータを使用します。

HOMEDIR

(UNIX/Linux のみ)ユーザのホーム ディレクトリを指定する文字列です。ユーザは、自分のホーム ディレクトリに自動的にログインできます。eTrust Single Sign-On および eTrust Web Access Control で使用されます。

このプロパティを変更するには、chusr コマンド、editusr コマンド、または newusr コマンドで homedir パラメータを使用します。

INACTIVE

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、ユーザのアクティビティがない状態の経過日数です。指定日数を経過すると、アカウントは非アクティブとしてマークが設定され、ユーザはログインできません。

USER クラスのレコードの INACTIVE プロパティの値は、GROUP クラスのレコードの値よりも優先されます。これらの両方のプロパティ値は、SEOS クラスのレコードの INACT プロパティよりも優先されます。

注: ユーザ レコードでは、アクティブでないユーザのマークが設定されません。アクティブでないユーザを識別するには、Inactive Days 値と Last Accessed Time 値を比較する必要があります。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで inactive パラメータを使用します。

LOCALAPPS

eTrust Single Sign-On および eTrust Web Access Control で使用されます。

LOCATION

ユーザの所在地を格納するために使用する文字列です。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。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで location パラメータを使用します。

LOGININFO

レコードで、ユーザが特定のアプリケーションおよび監査データにログインするために必要な情報を格納しているセクションです。LOGININFO には、ユーザがアクセスを許可されているアプリケーションごとに、個別にリストが保存されています。eTrust Single Sign-On および eTrust Web Access Control で使用されます。

LOGSHIFT

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、eTrust AC によって監査ログに書き込まれます。

MAXLOGINS

ユーザに許可される同時ログインの最大数(端末セッション数)です。この値を超えると、ユーザのアクセスは拒否されます。値が 0 の場合は、最大数を設定しないことを意味します。ユーザは任意の数の端末セッションに同時にログインできます。eTrust AC では、ログイン、selang、GUI などの個々のタスクが 1 つの端末セッションとみなされます。そのため、ログインした後に selang のコマンドを実行したり、データベースの管理タスクを実行する必要があるユーザについては、0 を指定するか、1 より大きい値を指定する必要があります。

USER クラスのレコードの MAXLOGINS プロパティの値は、GROUP クラスのレコードの値よりも優先されます。これらの両方のプロパティ値は、SEOS クラスのレコードの MAXLOGINS プロパティよりも優先されます。SEOS クラスのレコードの値は、アクセサ レコードに明示的な値の指定がない場合に使用されるデフォルト値です。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで maxlogins パラメータを使用します。

MIN_TIME

ユーザのパスワード変更間隔として許可する最短期間(日数)です。

USER クラスのレコードの MIN_TIME プロパティの値は、GROUP クラスのレコードの値よりも優先されます。これらの両方のプロパティ値は、SEOS クラスのレコードの PASSWDRULES プロパティよりも優先されます。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで min_life[-] パラメータを使用します。

NOTIFY

リソースの監査イベントが生成された場合に通知を受け取るユーザです。selogrd を使用して指定の電子メール アドレスに送信できる特別な監査レコードを作成することもできます。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで notify[-] パラメータを使用します。

制限: 30 文字。

OBJ_TYPE

ユーザの権限属性を示します。以下の権限属性を 1 つまたは複数指定できます。

ADMIN

UNIX/Linux 環境の root ユーザと同様に、ほとんどの管理機能の実行をユーザに許可します。

AUDITOR

システムの監視、データベース情報の一覧表示、および既存のレコードに対する監査モードの設定をユーザに許可します。

IGN_HOL

HOLIDAY クラスのレコードに定義されている時間帯のログインをユーザに許可します。

OPERATOR

データベース内のすべての情報の一覧表示、および secons ユーティリティの使用をユーザに許可します。

PWMANAGER

他のユーザのパスワード設定の変更、および serevu によって無効化されたユーザ アカウントの有効化をユーザに許可します。

SERVER

ユーザの権限を照会するプロセスを許可し、SEOSROUTE_VerifyCreate API コールを発行できます。

1 ユーザに対して複数の属性を指定できます。

ユーザに割り当てることのできる特別な属性の詳細については、「管理者ガイド」を参照してください。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで admin[-]、auditor[-]、ign_hol[-]、operator[-]、pwmanager[-]、または server[-]の各パラメータを使用します。

OIDCRDDATA

eTrust Single Sign-On および eTrust Web Access Control で使用されます。

ORG_UNIT

ユーザが所属する組織単位に関する情報を格納する文字列です。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。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで org-unit パラメータを使用します。

ORGANIZATION

ユーザが所属する組織に関する情報を格納する文字列です。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。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで organization パラメータを使用します。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで owner パラメータを使用します。

PASSWD_INT

ユーザのパスワード変更間隔として許可する最長期間（日数）です。

USER クラスのレコードの PASSWD_INT プロパティの値は、GROUP クラスのレコードの値よりも優先されます。これらの両方のプロパティ値は、SEOS クラスのレコードの PASSWDRULES プロパティよりも優先されます。

このプロパティを変更するには、chusr コマンド、editusr コマンド、または newusr コマンドで interval[-] パラメータを使用します。

PHONE

ユーザの電話番号を格納するために使用できる文字列。この情報が権限付与に使用されることはありません。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで phone パラメータを使用します。

POLICYMODEL

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に、新しいパスワードを受け取る PMDB です。このプロパティの値を入力した場合、Windows レジストリの parent_pmd または passwd_pmd のサブキー エントリで定義されている Policy Model にパスワードは送信されません。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで pmdb[-] パラメータを使用します。

PROFILE

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。

このプロパティを変更するには、chusr コマンド、editusr コマンド、または newusr コマンドで profile[-] パラメータを使用します。

PWD_AUTOGEN

ユーザ パスワードを自動的に生成するかどうかを指定します。eTrust Single Sign-On および eTrust Web Access Control で使用されます。デフォルトは「no」です。

PWD_SYNC

すべてのユーザ アプリケーションでユーザ パスワードを自動的に同一にするかどうかを示します。eTrust Single Sign-On および eTrust Web Access Control で使用されます。デフォルトは「no」です。

RESUME_DATE

一時停止した USER アカウントが有効になる日付です。

RESUME_DATE および SUSPEND_DATE を組み合わせて指定する方法については、SUSPEND_DATE を参照してください。

REVOKE_COUNT

eTrust Single Sign-On および eTrust Web Access Control で使用されます。

SCRIPT_VARS

eTrust Single Sign-On および eTrust 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が含まれる変数リストです。

SECLABEL

ユーザのセキュリティ ラベルです。セキュリティ ラベルは、セキュリティ レベルをセキュリティ カテゴリに関連付けます。

適用する場合、セキュリティ ラベルは、レコードに設定された特定のセキュリティ レベルおよびセキュリティ カテゴリよりも優先されます。セキュリティ ラベルを割り当てることは、ラベルのレベルとカテゴリをユーザに明示的に割り当てることと同じです。指定されたセキュリティ ラベルは、SECLABEL クラスのレコードとして定義する必要があります。USER クラスのレコードにセキュリティ ラベルが設定されている場合は、以下の条件が両方とも満たされている場合にのみ、リソースへのアクセス権がユーザに与えられます。

- セキュリティ ラベルに指定されたユーザのセキュリティ レベルが、リソースのセキュリティ レベル以上であること。
- リソース レコードに指定されたすべてのセキュリティ カテゴリが、ユーザのセキュリティ ラベルのセキュリティ カテゴリ リストに含まれていること。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで label[-] パラメータを使用します。

SECLEVEL

ユーザのセキュリティ レベルです。セキュリティ レベルは 0 から 255 までの正の整数です。値 0 は、セキュリティ レベルを割り当てないことを意味します。リソースにセキュリティ レベルを割り当てた場合は、ユーザのセキュリティ レベルがリソースのセキュリティ レベル以上である場合にのみ、リソースへのアクセス権がユーザに与えられます。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで level[-] パラメータを使用します。

SESSION_GROUP

eTrust 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。

Windows では、該当する名前がドロップダウン リストに存在しない場合、管理者がセッション グループの新しい名前を入力できます。

SHIFT

eTrust Single Sign-On および eTrust Web Access Control で使用されます。

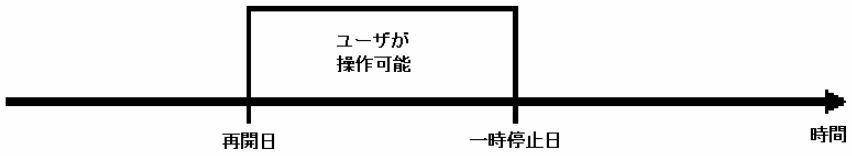
SUSPEND_DATE

ユーザ アカウントが一時停止されて無効になる日付です。

ユーザの再開日（RESUME_DATE を参照）が一時停止日より前の日付である場合は、再開日の前でもユーザ レコードは無効です。

レコードの一時停止日が再開日より前の日付である場合、ユーザは一時停止日より前および再開日より後に操作を実行できます。

レコードの再開日が一時停止日より前の日付である場合、ユーザは再開日と一時停止日の間のみ操作を実行できます。



USER クラスのレコードの SUSPEND_DATE プロパティの値は、GROUP クラスのレコードの値よりも優先されます。

このプロパティを変更するには、chusr コマンド、editusr コマンド、または newusr コマンドで suspend[-] パラメータを使用します。

変更できないプロパティ

このレコードに含まれている以下のプロパティは、eTrust AC によって自動的に変更されるため、selang またはポリシー マネージャ インターフェースを使用して変更することはできません。

CREATE_TIME

レコードが作成された日時です。

LAST_ACC_TERM

最後にログインが実行された端末です。

LAST_ACC_TIME

最後にログインが実行された日時です。

OLD_PASSWD

ユーザに割り当てられていた以前のパスワードのリストです。ユーザは、このリストから新しいパスワードを選択することはできません。このリストに保存されるパスワードの最大数は、setoptions コマンドによって指定します。このデータは暗号化されます。

PASSWD_A_C_W

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。

PASSWD_L_A_C

管理者が最後にパスワードを更新した日時です。

PASSWD_L_C

ユーザが最後にパスワードを更新した日時です。

REVACL

アクセサの ACL（アクセス制御リスト）を一覧表示します。

SUSPEND_WHO

一時停止日をアクティブにした管理者です。

UALIAS

1 つまたは複数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。eTrust Single Sign-On および eTrust Web Access Control で使用されます。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

GROUP クラス

GROUP クラスの各レコードは、データベース内でユーザのグループを定義します。グループのプロパティ(権限および制限)は、USER クラスのレコードのプロパティに指定されていない限り、各メンバに適用されます。この場合、ユーザは再開日と一時停止日の間のみ操作を実行できます。

GROUP クラスのレコードのキーは、グループ名です。eTrust AC では、GROUP クラスのレコードはグループ名によって識別されます。GROUP クラスのレコードの変更できるプロパティについて以下に説明します。

変更可能なプロパティ

APPLS

グループがアクセスを許可されているアプリケーションのリストです。eTrust Single Sign-On および eTrust Web Access Control で使用されます。

AUDIT_MODE

eTrust AC が監査ログに記録するアクティビティを識別します。以下のアクティビティの任意の組み合わせを指定できます。

- ログへの記録を行わない
- トレース ファイルに記録されたすべてのアクティビティ(UNIX/Linux のみ)
- 失敗したログイン
- 成功したログイン
- eTrust AC によって保護されているリソースに対する失敗したアクセス
- eTrust AC によって保護されているリソースに対する成功したアクセス

USER クラスのレコードの AUDIT_MODE プロパティの値は、GROUP クラスのレコードの値よりも優先されます。

このプロパティを変更するには、chgrp コマンド、editgrp コマンド、または newgrp コマンドで audit パラメータを使用します。

AUTHNMTHD

グループ レコードに対して使用する 1 つまたは複数の認証方法(method 1 から method 32、または none)です。eTrust Single Sign-On および eTrust Web Access Control で使用されます。

CALENDAR

eTrust AC のユーザ、グループ、およびリソース制限の Unicenter TNG カレンダオブジェクトを表します。eTrust AC は、一定の間隔で Unicenter TNG のアクティブなカレンダを取得します。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで calendar パラメータと calendar- パラメータを使用します。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。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。このプロパティで指定する情報は、ネイティブ環境の COMMENT プロパティで指定する情報と同じです。個別に情報を変更することはできません。

このプロパティを変更するには、chgrp コマンド、editgrp コマンド、および newgrp コマンドで comment[-] パラメータを使用します。

DAYTIME

プロファイル機能の一部です。ユーザがリソースにアクセスできる日時を管理する、曜日と時刻の制限です。USER クラスのレコードの DAYTIME プロパティの値は、GROUP クラスのレコードの値よりも優先されます。このプロパティの情報は、eTrust AC のデータベースでは分単位を含む時間が使用できること以外は、ネイティブ環境の DAYTIME プロパティの情報と同じです。

このプロパティを変更するには、chgrp コマンド、editgrp コマンド、および newgrp コマンドで restrictions(days and time) パラメータを使用します。

EXPIRE_DATE

USER クラスのレコードが失効して無効になる日付です。USER クラスのレコードの EXPIRE_DATE プロパティの値は、GROUP クラスのレコードの値よりも優先されます。

失効したレコードを元に戻すには、chgrp コマンドで expire- パラメータを使用します。失効したグループを再開することはできません。一時停止したグループは、再開日を指定することで再開できます。

このプロパティを変更するには、chgrp コマンド、editgrp コマンド、または newgrp コマンドで expire[-] パラメータを使用します。

FULLNAME

グループに関連付けられたフル ネームであり、最大 256 文字の英数字からなる文字列です。 フル ネームは、eTrust AC の監査ログ メッセージでユーザを識別するために使用されますが、権限付与に使用されることはありません。

このプロパティを変更するには、chgrp コマンド、editgrp コマンド、または newgrp コマンドで name パラメータを使用します。

GAPPLS

グループがアクセスを許可されているアプリケーション グループのリストです。eTrust Single Sign-On および eTrust Web Access Control で使用されます。

GROUP_MEMBER

このグループに属するグループです。

HOMEDIR

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。最大 255 文字の英数字で完全パスを指定します。

このプロパティを変更するには、chgrp コマンド、editgrp コマンド、または newgrp コマンドで homedir パラメータを使用します。

INACTIVE

プロファイル機能の一部です。グループ メンバのステータスが非アクティブに変更されるまでの、ユーザのアクティビティがない状態の経過日数です。指定日数を経過すると、アカウントは非アクティブとしてマークが付けられ、グループ メンバはログインできません。

USER クラスのレコードの INACTIVE プロパティの値は、GROUP クラスのレコードの値よりも優先されます。これらの両方のプロパティ値は、SEOS クラスのレコードの INACT プロパティよりも優先されます。

注: ユーザ レコードでは、アクティブでないユーザのマークが設定されません。アクティブでないユーザを識別するには、Inactive Days 値と Last Accessed Time 値を比較する必要があります。

このプロパティを変更するには、chgrp コマンド、editgrp コマンド、および newgrp コマンドで inactive パラメータを使用します。

MAXLOGINS

プロファイル機能の一部です。グループ内のユーザに許可される同時ログインの最大数(端末セッション数)です。この値を超えると、ユーザのアクセスは拒否されます。値が 0 の場合は、最大数を設定しないことを意味します。グループ内のユーザは、任意の数の端末セッションに同時にログインできます。eTrust AC では、ログイン、selang、GUI などの個々のタスクが 1 つの端末セッションとみなされます。そのため、ログインした後に selang を実行したり、データベースの管理タスクを実行する必要があるグループ内のユーザについては、0 を指定するか、1 より大きい値を指定する必要があります。

USER クラスのレコードの MAXLOGINS プロパティの値は、GROUP クラスのレコードの値よりも優先されます。これらの両方のプロパティ値は、SEOS クラスのレコードの MAXLOGINS プロパティよりも優先されます。SEOS クラスのレコードの値は、アクセサ レコードに明示的な値の指定がない場合に使用されるデフォルト値です。

このプロパティを変更するには、chgrp コマンド、editgrp コマンド、および newgrp コマンドで maxlogins パラメータを使用します。

MEMBER_OF

このグループが属するグループです。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chgrp コマンド、editgrp コマンド、および newgrp コマンドで owner パラメータを使用します。

PASSWDRULES

プロファイル機能の一部です。パスワード ルールを示します。このプロパティには、eTrust AC 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。

このプロパティを変更するには、setoptions コマンドで password パラメータおよび rules オプションまたは rules- オプションを使用します。

POLICYMODEL

プロファイル機能の一部です。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に、新しいパスワードを受け取る PMDB です。このプロパティの値を入力した場合、Windows レジストリの parent_pmd または passwd_pmd のサブキー エントリで定義されている Policy Model にパスワードは送信されません。

このプロパティを変更するには、chgrp コマンド、editgrp コマンド、および newgrp コマンドで pmdb[-] パラメータを使用します。

PWD_AUTOGEN

グループ パスワードを自動的に生成するかどうかを指定します。デフォルトは「no」です。eTrust Single Sign-On および eTrust Web Access Control で使用されます。

PWD_SYNC

すべてのグループ アプリケーションでグループ パスワードを自動的に同一にするかどうかを示します。デフォルトは「no」です。eTrust Single Sign-On および eTrust Web Access Control で使用されます。

PWPOLICY

グループに適用するパスワード ポリシーのレコード名です。パスワード ポリシーは、新しいパスワードの妥当性をチェックし、パスワードの有効期限を定義する一連のルールです。デフォルトでは、妥当性チェックは行われません。eTrust Single Sign-On および eTrust Web Access Control で使用されます。

RESUME_DATE

プロファイル機能の一部です。USER クラスのレコードが有効になる日付です。USER クラスのレコードの RESUME_DATE プロパティの値は、GROUP クラスのレコードの値よりも優先されます。

RESUME_DATE および SUSPEND_DATE を組み合わせて指定する方法については、SUSPEND_DATE を参照してください。

このプロパティを変更するには、chgrp コマンド、editgrp コマンド、および newgrp コマンドで resume[-] パラメータを使用します。

SHELL

(UNIX/Linux のみ)このグループのメンバである新しい UNIX/Linux ユーザに割り当てられるシェル プログラムです。

このプロパティを変更するには、chgrp コマンド、editgrp コマンド、または newgrp コマンドで shellprog パラメータを使用します。

SUPGROUP

親グループ(「上位」グループ)の名前です。

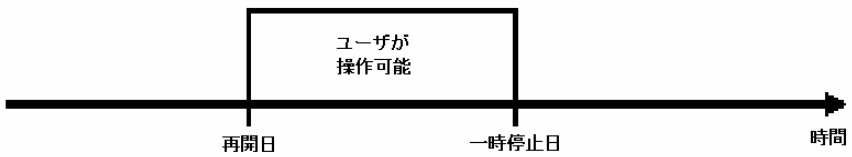
このプロパティを変更するには、chgrp コマンド、editgrp コマンド、または newgrp コマンドで parent[-] パラメータを使用します。

SUSPEND_DATE

グループ メンバ レコードが一時停止されて無効になる日付です。グループの再開日(RESUME_DATE を参照)が一時停止日より前の日付である場合は、再開日より前でもユーザ レコードは無効です。

レコードの一時停止日が再開日より前の日付である場合、ユーザは一時停止日より前および再開日より後に操作を実行できます。

レコードの再開日が一時停止日より前の日付である場合、ユーザは再開日と一時停止日の間のみ操作を実行できます。



USER クラスのレコードの SUSPEND_DATE プロパティの値は、GROUP クラスのレコードの値よりも優先されます。

このプロパティを変更するには、chgrp コマンド、editgrp コマンド、または newgrp コマンドで suspend[-] パラメータを使用します。

USERLIST

グループに属するユーザのリストです。

このプロパティで設定するユーザ リストは、ネイティブ環境の USERS 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。

このプロパティを変更するには、join[-] コマンドで username パラメータを使用します。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

PROFUSR

このプロファイル グループに関連付けられているユーザのリストです。

REVACL

アクセサの ACL(アクセス制御リスト)を一覧表示します。

SUBGROUP

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。

SUSPEND_WHO

一時停止日をアクティブにした管理者です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

注: 旧バージョンの eTrust AC の MIN_TIME プロパティ、NGRACE プロパティ、および PASSWD_INT プロパティは、現在では PASSWDRULES プロパティの一部になっています。

リソース クラス

このセクションでは、eTrust AC データベースの各リソース クラスをアルファベット順に示し、クラス別に概要を説明します。ほとんどのクラスは、UNIX/Linux 版と Windows 版の両方の eTrust AC に実装されています。

ADMIN クラス

ADMIN クラスの各レコードには、ADMIN 以外のユーザに対して特定のクラスの管理を許可するための定義が含まれます。委任されたユーザが管理する eTrust AC の各クラスを表す ADMIN レコードを作成する必要があります。ADMIN レコードには、各クラスのアクセス権限を持つアクセサのリストが格納されます。条件付きアクセス制御リスト(CACL)もサポートされます。

ADMIN クラスのレコードのキーは、保護されるクラスの名前です。ADMIN クラスのレコードの変更できるプロパティについて以下に説明します。

変更可能なプロパティ

ACL

リソースへのアクセスを許可されているアクセサ(ユーザおよびグループ)およびアクセス タイプのリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。ADMIN クラスの有効なアクセス権限は、以下のとおりです。
  - all - そのクラスに対して許可されるすべての操作の実行をアクセサに許可します。
  - create - ADMIN レコードの作成をアクセサに許可します。
  - delete - ADMIN レコードの削除をアクセサに許可します。
  - join - USER レコードにグループを追加する操作、およびグループとユーザのリンクを作成する操作をアクセサに許可します。ただし、アクセサには modify アクセス権も必要です。
  - modify - GROUP レコードへのユーザ名の追加を含む、既存のレコードを変更する操作をアクセサに許可します。ただし、グループとユーザのリンクを作成するには、join アクセス権も必要です。
  - none - どの操作の実行もアクセサに許可しません。
  - password - 他のユーザのパスワードを変更する操作をアクセサに許可します(このアクセス タイプは USER クラスにのみ適用されます)。
  - read - すべてのクラスのレコードを一覧表示する操作をアクセサに許可します。

ACL プロパティを変更するには、authorize コマンドで access(*authority*) パラメータ、または authorize- コマンドを使用します。

AUDIT

eTrust AC の監査ログに記録されるアクセス イベントのタイプです。有効な値は以下のとおりです。

- all - すべてのアクセス要求が監査されます。
- success - 許可されたすべてのアクセス要求が監査されます。
- failure - 拒否されたアクセス要求のみが監査されます。この値がデフォルト値です。
- none - アクセス要求の監査は行われません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで audit パラメータを使用します。

CALACL

カレンダ アクセス制御リストです。これは、Unicenter TNG カレンダ ステータスに基づいてリソースへのアクセスが許可されているアクセサ(ユーザおよびグループ)のリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **カレンダ参照** - Unicenter TNG のカレンダへの参照。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。ADMIN クラスの有効なアクセス権限は、以下のとおりです。
  - all - そのクラスに対して許可されるすべての操作の実行をアクセサに許可します。
  - create - ADMIN レコードの作成をアクセサに許可します。
  - delete - ADMIN レコードの削除をアクセサに許可します。
  - join - USER レコードにグループを追加する操作、およびグループとユーザのリンクを作成する操作をアクセサに許可します。ただし、アクセサには modify アクセス権も必要です。
  - modify - GROUP レコードへのユーザ名の追加を含む、既存のレコードを変更する操作をアクセサに許可します。ただし、グループとユーザのリンクを作成するには、join アクセス権も必要です。
  - none - どの操作の実行もアクセサに許可しません。
  - password - 他のユーザのパスワードを変更する操作をアクセサに許可します(このアクセス タイプは USER クラスにのみ適用されます)。
  - read - すべてのクラスのレコードを一覧表示する操作をアクセサに許可します。

カレンダが有効な場合にのみアクセスが許可されます。その他の場合はすべてのアクセスが拒否されます。

ACL アクセスに基づいて、ユーザまたはグループにリソースへのアクセスを許可するには、authorize コマンドで calendar パラメータを使用します。

CALENDAR

eTrust AC のユーザ、グループ、およびリソース制限の Unicenter TNG カレンダオブジェクトを表します。eTrust AC は、一定の間隔で Unicenter TNG のアクティブなカレンダを取得します。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで calendar パラメータと calendar- パラメータを使用します。

CATEGORY

リソースに割り当てる 1 つまたは複数のセキュリティ カテゴリです。CATEGORY クラスに定義されている任意のセキュリティ カテゴリを指定できます。リソースに 1 つまたは複数のセキュリティ 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**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。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで category[-] パラメータを使用します。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。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。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

DAYTIME

ユーザがリソースにアクセスできる日時を管理する、日付と時刻の制限です。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで restrictions(days and time) パラメータを使用します。

NACL

リソースへのアクセスが許可されないアクセサ(ユーザおよびグループ)と、許可されないアクセス タイプのリストです。NACL の各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを NACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されないアクセス** - アクセサが明示的にアクセスを許可されないリソースへのアクセスのタイプです。ADMIN クラスの有効なアクセス権限は、以下のとおりです。

- all - アクセサがそのクラスに対してすべての操作を実行できないようにします。
- create - アクセサが ADMIN レコードを作成できないようにします。
- delete - アクセサが ADMIN レコードを削除できないようにします。
- join - アクセサが USER レコードにグループを追加できないようにします。
- modify - アクセサが既存のレコードを変更（GROUP レコードへのユーザ名の追加を含む）できないようにします。
- none - すべての操作の実行をアクセサに許可します。
- password - アクセサが他のユーザのパスワードを変更できないようにします。
- read - アクセサがすべてのクラスのレコードを一覧表示できないようにします。

NACL プロパティを変更するには、authorize コマンドで deniedaccess(*accesstype*) パラメータ、または authorize- コマンドで deniedaccess- パラメータを使用します。

NOTIFY

リソースの監査イベントが生成された場合に通知を受け取るユーザです。selogrd を使用して指定の電子メール アドレスに送信できる特別な監査レコードを作成することもできます。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで notify[-] パラメータを使用します。

制限: 30 文字。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

PACL

プログラム アクセス制御リストです。特定のプログラムから、またはプログラム名のパターンに一致するプログラムからアクセス要求が行われた場合に、アクセサに適用される ACL です。-名前パターン

パターンを指定すると、PACL によって保護されているリソースは、指定したパターンに一致するプログラムを使用しないとアクセスできません。プログラムが複数のパターンと一致する場合は、文字数が最も多いパターンが優先されます。

プログラム アクセス制御リストの各要素には、以下の情報が含まれています。

- **プログラム参照** - 指定または名前パターン一致による PROGRAM クラスのレコードへの参照。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。
- **許可されたアクセス** - 指定されたプログラムを使用している場合にアクセサに許可されるアクセス権。有効な値については、ACL プロパティを参照してください。

ACL プロパティにプログラム、アクセサ、およびアクセス タイプを追加するには、authorize コマンドで via(pgm) パラメータを使用します。ACL プロパティからこれらを削除するには、authorize- コマンドで via(pgm) パラメータを使用します。

SECLABEL

リソースのセキュリティ ラベルです。セキュリティ ラベルは、セキュリティ レベルをセキュリティ カテゴリに関連付けます。

適用する場合、セキュリティ ラベルは、レコードに設定された特定のセキュリティ レベルおよびセキュリティ カテゴリよりも優先されます。セキュリティ ラベルを割り当てることは、ラベルのレベルとカテゴリをユーザに明示的に割り当てることと同じです。指定されたセキュリティ ラベルは、SECLABEL クラスのレコードとして定義する必要があります。USER クラスのレコードにセキュリティ ラベルが設定されている場合は、以下の条件が両方とも満たされている場合にのみ、リソースへのアクセス権がユーザに与えられます。

- セキュリティ ラベルに指定されたユーザのセキュリティ レベルが、リソースのセキュリティ レベル以上であること。
- リソース レコードに指定されたすべてのセキュリティ カテゴリが、ユーザのセキュリティ ラベルのセキュリティ カテゴリ リストに含まれていること。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで label[-] パラメータを使用します。

SECLEVEL

ユーザまたはリソースのセキュリティ レベルです。セキュリティ レベルは 0 から 255 までの正の整数です。値 0 は、セキュリティ レベルを割り当てないことを意味します。リソースにセキュリティ レベルを割り当てた場合は、ユーザのセキュリティ レベルがリソースのセキュリティ レベル以上である場合にのみ、リソースへのアクセス権がユーザに与えられます。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで level[-] パラメータを使用します。

UACC

リソースに対するデフォルトのアクセス権です。eTrust AC に定義されていないアクセサ、またはリソースの ACL に登録されていないアクセサに与えるアクセス権を示します。有効な値については、リソースの ACL プロパティを参照してください。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで defaccess パラメータを使用します。

WARNING

警告モードを有効にするかどうかを示します。警告モードを有効にすると、すべてのアクセス要求が許可されます。アクセス要求がアクセス ルールに違反する場合は、レコードが監査ログに書き込まれます。

注: 警告モードの場合、eTrust Access Control では、リソース グループに対する警告メッセージは作成されません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで warning[-] パラメータを使用します。

変更できないプロパティ

AAUDIT

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。

CREATE_TIME

レコードが作成された日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

AGENT クラス

AGENT クラスの各レコードは、eTrust Single Sign-On または eTrust Web Access Control でエージェントとして使用されるオブジェクトを定義します。

AGENT クラスのレコードのキーは、エージェントの名前です。AGENT クラスのレコードの変更できるプロパティについて以下に説明します。

変更可能なプロパティ

AGENT_TYPE

エージェントのタイプです。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。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。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

AGENT_TYPE クラス

AGENT_TYPE クラスの各レコードは、eTrust Single Sign-On または eTrust Web Access Control で使用されるエージェント タイプを定義します。

AGENT_TYPE クラスのレコードのキーは、エージェントのタイプです。AGENT_TYPE クラスのレコードの変更できるプロパティについて以下に説明します。

変更可能なプロパティ

AGENT_FLAG

属性に関する情報が含まれています。フラグには、以下の値を指定できます。

- aznchk - この属性が権限付与に使用されるかどうかを示します。
- predef（事前に定義済み）、freetext（自由形式のテキスト）、または userdir（ユーザ ディレクトリ） - これらの値を使用して、ユーザ属性のソースを示します。
- user または group - これらの値を使用して、属性（アクセサ）がユーザかグループかを示します。

AGENT_LIST

agent_type パラメータの値として AGENT_TYPE オブジェクトを指定して作成された AGENT クラスのオブジェクトのリストです。たとえば、このプロパティは、AGENT クラスのオブジェクトの作成時に暗黙的に更新されます。

CLASSES

このエージェントに関連するクラスまたはリソースの複数文字列リストです。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。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。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

APPL クラス

APPL クラスの各レコードは、eTrust Single Sign-On または eTrust Web Access Control で使用されるアプリケーションを定義します。

APPL クラスのレコードのキーは、アプリケーションの名前です。APPL クラスのレコードの変更できるプロパティについて以下に説明します。

変更可能なプロパティ

ACL

リソースへのアクセスを許可されているアクセサ(ユーザおよびグループ)およびアクセス タイプのリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。APPL クラスの有効なアクセス権限は、以下のとおりです。
  - execute - プログラムの実行をアクセサに許可します。このアクセス タイプを使用するには、読み取りアクセス権限も必要です。
  - none - どの操作の実行もアクセサに許可しません。
  - read - ファイルまたはディレクトリを変更せずに使用することをアクセサに許可します。

ACL プロパティを変更するには、authorize コマンドで access(*authority*) パラメータ、または authorize- コマンドを使用します。

APPLTYPE

eTrust Single Sign-On および eTrust Web Access Control で使用されます。

AZNACL

権限 ACL です。リソースの説明に基づいてリソースへのアクセスを許可できます。説明は、オブジェクトではなく認証エンジンに送信されます。オブジェクトは、ほとんどの場合データベースに存在しません。

AUDIT

eTrust AC の監査ログに記録されるアクセス イベントのタイプです。有効な値は以下のとおりです。

- all - すべてのアクセス要求が監査されます。
- success - 許可されたすべてのアクセス要求が監査されます。
- failure - 拒否されたアクセス要求のみが監査されます。この値がデフォルト値です。

- none - アクセス要求の監査は行われません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで audit パラメータを使用します。

CALACL

カレンダ アクセス制御リストです。これは、Unicenter TNG カレンダ ステータスに基づいてリソースへのアクセスが許可されているアクセサ(ユーザおよびグループ)のリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **カレンダ参照** - Unicenter TNG のカレンダへの参照。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。APPL クラスの有効なアクセス権限は、以下のとおりです。
  - execute - プログラムの実行をアクセサに許可します。このアクセス タイプを使用するには、読み取りアクセス権限も必要です。
  - none - どの操作の実行もアクセサに許可しません。
  - read - ファイルまたはディレクトリを変更せずに使用することをアクセサに許可します。

カレンダが有効な場合にのみアクセスが許可されます。その他の場合はすべてのアクセスが拒否されます。

ACL アクセスに基づいて、ユーザまたはグループにリソースへのアクセスを許可するには、authorize コマンドで calendar パラメータを使用します。

CALENDAR

eTrust AC のユーザ、グループ、およびリソース制限の Unicenter TNG カレンダ オブジェクトを表します。eTrust AC は、一定の間隔で Unicenter TNG のアクティブなカレンダを取得します。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで calendar パラメータと calendar- パラメータを使用します。

CAPTION

デスクトップのアプリケーション アイコンの下に表示されるテキストです。最大 47 文字の英数字を指定できます。デフォルトは APPL クラスのレコードの名前です。

CMDLINE

アプリケーション実行可能ファイルのファイル名です。eTrust Single Sign-On および eTrust Web Access Control で使用されます。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。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。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

CONTAINED_ITEMS

レコードがコンテナである場合に、コンテナに含まれるアプリケーションのレコード名です。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで item[-](*app/Name*) パラメータを使用します。

CONTAINER

アプリケーションがコンテナかどうかを示します。デフォルトは「no」です。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで container[-]パラメータを使用します。

DAYTIME

ユーザがリソースにアクセスできる日時を管理する、曜日と時刻の制限です。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで restrictions(days and time) パラメータを使用します。

DIALOG_FILE

アプリケーションのログイン シーケンスが含まれているディレクトリ内の eTrust Web Access Control スクリプトの名前です。デフォルトのディレクトリの場所は、/usr/sso/scripts です。デフォルト値は「no script」です。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで script[-](*fileName*) パラメータを使用します。

GROUPS

アプリケーションの使用を許可されているユーザ グループのリストです。

HOST

アプリケーションが存在するホストの名前です。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで host[-](hostName) パラメータを使用します。

ICONFILE

デスクトップに表示するアプリケーションのアイコンが保存されているファイルのファイル名または完全パスです。eTrust AC では、エンド ユーザのワークステーションにアイコン ファイルが存在することを前提としています。ファイル名のみを入力した場合は、以下の順序でファイルが検索されます。

1. 現在のディレクトリ
2. 環境変数 PATH に指定されているディレクトリ

デフォルトは、ワークステーションのデフォルト アイコンです。

ICONID

アイコン ファイル内のアイコンの(必要に応じた)ID 番号です。ICONID が指定されない場合は、デフォルト アイコンが使用されます。

IS_CONTAINER

アプリケーションがコンテナかどうかを示します。デフォルトは「no」です。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで container[-] パラメータを使用します。

IS_DISABLED

アプリケーションが無効化された状態かどうかを示します。アプリケーションが無効化された状態である場合、ユーザはアプリケーションにログインできません。この機能は、ユーザがアプリケーションを変更しているときに、他のユーザがアプリケーションにログインできないようにする場合に役立ちます。無効化された状態のアプリケーションはアプリケーション メニュー リストに表示されますが、ユーザがそのアプリケーションを選択すると、メッセージが表示され、ログインは中止されます。デフォルトは「not disabled」です。

IS_HIDDEN

アプリケーションを起動できるユーザのデスクトップにもアプリケーション アイコンを表示するかどうかを示します。たとえば、他のアプリケーションにパスワードを提供する目的のみを果たすアプリケーションなどのマスタ アプリケーションを非表示にすることができます。デフォルトは「not hidden」です。

1. このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで hidden[-] パラメータを使用します。

IS_SENSITIVE

事前設定された時間が経過した後にユーザがアプリケーションを開いた場合に、再認証が必要かどうかを示します。デフォルトは「not sensitive」です。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで sensitive[-]パラメータを使用します。

LOGIN_TYPE

ユーザ パスワードの指定方法です。値は、pwd（平文パスワード）、otp（ワンタイム パスワード）、appticket（メインフレーム アプリケーション認証専用チケット）、none（パスワード不要）、または passticket（IBM が開発したワンタイム パスワード置換形式。メインフレームのセキュリティ パッケージで使用される）です。デフォルトは pwd です。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで *login_type(value)* パラメータを使用します。

MASTER_APPL

他のアプリケーションにパスワードを提供するアプリケーションのレコード名です。デフォルトは「no master」です。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで master[-](*applName*) パラメータを使用します。

MON_RULES_FILE

UNIX/Linux の dbdump でのみ使用されます。

NACL

リソースへのアクセスが許可されないアクセサ（ユーザおよびグループ）と、許可されないアクセス タイプのリストです。NACL の各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ（ユーザまたはグループ）への参照。eTrust AC に定義されているすべてのユーザを NACL に指定するには、アクセサ参照としてアスタリスク（*）を入力します。
- **許可されないアクセス** - アクセサが明示的にアクセスを許可されないリソースへのアクセスのタイプです。APPL クラスの有効なアクセス権限は、以下のとおりです。
  - execute - アクセサがプログラムを実行できないようにします。このアクセス タイプを使用するには、読み取りアクセス権限も必要です。
  - none - すべての操作の実行をアクセサに許可します。
  - read - アクセサがファイルを表示できないようにします。

NACL プロパティを変更するには、authorize コマンドで deniedaccess(*accesstype*) パラメータ、または authorize- コマンドで deniedaccess- パラメータを使用します。

NOTIFY

リソースの監査イベントが生成された場合に通知を受け取るユーザです。selogrd を使用して指定の電子メール アドレスに送信できる特別な監査レコードを作成することもできます。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで notify[-] パラメータを使用します。

制限: 30 文字。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

PGMDIR

アプリケーションの実行可能ファイルが格納されているディレクトリまたはディレクトリのリストです。eTrust Single Sign-On および eTrust Web Access Control で使用されます。

PWD_AUTOGEN

アプリケーション パスワードを eTrust Web Access Control で自動的に生成するかどうかを示します。デフォルトは「no」です。

PWD_SYNC

アプリケーション パスワードを自動的に他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示します。デフォルトは「no」です。

PWPOLICY

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です。パスワード ポリシーは、新しいパスワードの妥当性をチェックし、パスワードの有効期限を定義する一連のルールです。デフォルトでは、妥当性チェックは行われません。

SCRIPT_POSTCMD

ログイン スクリプトの後に 1 つまたは複数のコマンドを実行するかどうかを示します。

SCRIPT_PRECMD

ログイン スクリプトの前に 1 つまたは複数のコマンドを実行するかどうかを示します。

SCRIPT_VARS

eTrust Single Sign-On および eTrust 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が含まれる変数リストです。

TKTKEY

eTrust Single Sign-On でのみ使用されます。

TKTPROFILE

eTrust Single Sign-On でのみ使用されます。

UACC

リソースに対するデフォルトのアクセス権です。eTrust AC に定義されていないアクセサ、またはリソースの ACL に登録されていないアクセサに与えるアクセス権を示します。有効な値については、リソースの ACL プロパティを参照してください。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで defaccess パラメータを使用します。

WARNING

警告モードを有効にするかどうかを示します。警告モードを有効にすると、すべてのアクセス要求が許可されます。アクセス要求がアクセス ルールに違反する場合は、レコードが監査ログに書き込まれます。

注: 警告モードの場合、eTrust Access Control では、リソース グループに対する警告メッセージは作成されません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで warning[-] パラメータを使用します。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

AUTHHOST クラス

AUTHHOST クラスの各レコードは、eTrust Single Sign-On および eTrust Web Access Control の認証ホストを定義します。

AUTHHOST クラスのレコードのキーは、認証ホストの名前です。AUTHHOST クラスのレコードの変更できるプロパティについて以下に説明します。

変更可能なプロパティ

ACL

リソースへのアクセスを許可されているアクセサ(ユーザおよびグループ)およびアクセス タイプのリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。AUTHHOST クラスの有効なアクセス権限は、以下のとおりです。
  - none - どの操作の実行もアクセサに許可しません。
  - read - 認証されたホストからのログインをアクセサに許可します。

ACL プロパティを変更するには、authorize コマンドで access(*authority*) パラメータ、または authorize- コマンドを使用します。

AUDIT

eTrust AC の監査ログに記録されるアクセス イベントのタイプです。有効な値は以下のとおりです。

- all - すべてのアクセス要求が監査されます。
- success - 許可されたすべてのアクセス要求が監査されます。
- failure - 拒否されたアクセス要求のみが監査されます。この値がデフォルト値です。
- none - アクセス要求の監査は行われません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで audit パラメータを使用します。

AUTH_METHOD

UNIX/Linux の dbdump でのみ使用されます。

AZNACL

権限 ACL です。リソースの説明に基づいてリソースへのアクセスを許可できます。説明は、オブジェクトではなく認証エンジンに送信されます。オブジェクトは、ほとんどの場合データベースに存在しません。

CALACL

カレンダ アクセス制御リストです。これは、Unicenter TNG カレンダ ステータスに基づいてリソースへのアクセスが許可されているアクセサ(ユーザおよびグループ)のリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **カレンダ参照** - Unicenter TNG のカレンダへの参照。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。AUTHHOST クラスの有効なアクセス権限は、以下のとおりです。
  - none - どの操作の実行もアクセサに許可しません。
  - read - 認証されたホストからのログインをアクセサに許可します。

カレンダが有効な場合にのみアクセスが許可されます。その他の場合はすべてのアクセスが拒否されます。

ACL アクセスに基づいて、ユーザまたはグループにリソースへのアクセスを許可するには、authorize コマンドで calendar パラメータを使用します。

CALENDAR

eTrust AC のユーザ、グループ、およびリソース制限の Unicenter TNG カレンダ オブジェクトを表します。eTrust AC は、一定の間隔で Unicenter TNG のアクティブなカレンダを取得します。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで calendar パラメータと calendar- パラメータを使用します。

CATEGORY

リソースに割り当てる 1 つまたは複数のセキュリティ カテゴリです。CATEGORY クラスに定義されている任意のセキュリティ カテゴリを指定できます。リソースに 1 つまたは複数のセキュリティ 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**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。

リソースのこのプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで category[-] パラメータを使用します。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。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。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

CONT_FORMAT

UNIX/Linux の dbdump でのみ使用されます。

DAYTIME

ユーザがリソースにアクセスできる日時を管理する、曜日と時刻の制限です。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで restrictions(days and time) パラメータを使用します。

ETHINFO

ホストのイーサネット情報です。

GROUPS

リソース レコードが属する GAUTHHOST クラスまたは CONTAINER クラスのレコードのリストです。

AUTHHOST クラスのレコードのこのプロパティを変更するには、該当する CONTAINER クラスまたは GAUTHHOST クラスのレコードの MEMBERS プロパティを変更する必要があります。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで mem+ か mem- パラメータを使用します。

KEY

eTrust Single Sign-On でのみ使用されます。

NACL

リソースへのアクセスが許可されないアクセサ(ユーザおよびグループ)と、許可されないアクセス タイプのリストです。NACL の各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを NACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されないアクセス** - アクセサが明示的にアクセスを許可されないリソースへのアクセスのタイプです。AUTHHOST クラスの有効なアクセス権限は、以下のとおりです。
  - none - すべての操作の実行をアクセサに許可します。
  - read - 認証されたホストからアクセサがログインできないようにします。

NACL プロパティを変更するには、authorize コマンドで deniedaccess(*accesstype*) パラメータ、または authorize- コマンドで deniedaccess- パラメータを使用します。

NOTIFY

リソースの監査イベントが生成された場合に通知を受け取るユーザです。selogrd を使用して指定の電子メール アドレスに送信できる特別な監査レコードを作成することもできます。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで notify[-] パラメータを使用します。

制限: 30 文字。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

PATH

eTrust Single Sign-On でのみ使用されます。

PROPERTIES

UNIX/Linux の dbdump でのみ使用されます。

SECLABEL

リソースのセキュリティ ラベルです。セキュリティ ラベルは、セキュリティ レベルをセキュリティ カテゴリに関連付けます。

適用する場合、セキュリティ ラベルは、レコードに設定された特定のセキュリティ レベルおよびセキュリティ カテゴリよりも優先されます。セキュリティ ラベルを割り当てることは、ラベルのレベルとカテゴリをユーザに明示的に割り当てることと同じです。指定されたセキュリティ ラベルは、SECLABEL クラスのレコードとして定義する必要があります。USER クラスのレコードにセキュリティ ラベルが設定されている場合は、以下の条件が両方とも満たされている場合にのみ、リソースへのアクセス権がユーザに与えられます。

- セキュリティ ラベルに指定されたユーザのセキュリティ レベルが、リソースのセキュリティ レベル以上であること。
- リソース レコードに指定されたすべてのセキュリティ カテゴリが、ユーザのセキュリティ ラベルのセキュリティ カテゴリ リストに含まれていること。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで label[-] パラメータを使用します。

SECLEVEL

ユーザまたはリソースのセキュリティ レベルです。セキュリティ レベルは 0 から 255 までの正の整数です。値 0 は、セキュリティ レベルを割り当てないことを意味します。リソースにセキュリティ レベルを割り当てた場合は、ユーザのセキュリティ レベルがリソースのセキュリティ レベル以上である場合にのみ、リソースへのアクセス権がユーザに与えられます。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで level[-] パラメータを使用します。

SEED

eTrust Single Sign-On でのみ使用されます。

SERNUM

認証ホストのシリアル番号です。

UACC

リソースに対するデフォルトのアクセス権です。eTrust AC に定義されていないアクセサ、またはリソースの ACL に登録されていないアクセサに与えるアクセス権を示します。有効な値については、リソースの ACL プロパティを参照してください。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで defaccess パラメータを使用します。

UNTRUST

プログラムが trusted かどうかを示します。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他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、eTrust AC によって UNTRUST プロパティが自動的に設定されます。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで trust[-] パラメータを使用します。

USER_FORMAT

eTrust Single Sign-On でのみ使用されます。

USERALIAS

特定の認証ホストに定義されているユーザのすべての別名を示します。

WARNING

警告モードを有効にするかどうかを示します。警告モードを有効にすると、すべてのアクセス要求が許可されます。アクセス要求がアクセス ルールに違反する場合は、レコードが監査ログに書き込まれます。

注: 警告モードの場合、eTrust Access Control では、リソース グループに対する警告メッセージは作成されません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで warning[-] パラメータを使用します。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

USER_DIR_PROP

ユーザのディレクトリの名前です。

CALENDAR クラス

CALENDAR クラスの各レコードは、eTrust AC で時刻制限が適用されたユーザ、グループ、およびリソースの Unicenter TNG カレンダ オブジェクトを定義します。eTrust AC は、指定された間隔で Unicenter TNG のアクティブなカレンダを取得して適用します。

以下のクラスには、そのクラスのレコード内に CALENDAR プロパティがあります。これらのリソース クラスの各オブジェクトには、CALENDAR クラス オブジェクトを 1 つのみ割り当てることができます。

- ADMIN
- APPL
- AUTHHOST
- CONNECT
- CONTAINER
- DOMAIN(Windows のみ)
- FILE
- GFILE
- GHOST
- GROUP
- GSUDO
- GTERMINAL
- HOST
- HOSTNET
- HOSTNP
- LOGINAPPL(UNIX/Linux のみ)
- MFTERMINAL
- PROCESS
- PROGRAM
- REGKEY(Windows のみ)
- SUDO
- SURROGATE
- TCP
- TERMINAL

- USER

CALENDAR クラスのキーは、Unicenter TNG カレンダの名前です。CALENDAR クラスのレコードの変更できるプロパティについて以下に説明します。

変更可能なプロパティ

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。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。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment パラメータを使用します。このプロパティを削除するには、comment- パラメータを使用します。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

selang の構文

CALENDAR クラスのレコードを作成または変更するには、以下の構文を使用します。

```
{chres | editres | newres} calendar(calendarName) ¥
{comment(string) owner(ownerName)}
```

CALENDAR クラスのレコードをリソースに割り当てるには、以下の構文を使用します。

```
{chgrp | chres | chusr | editgrp | editres | editusr | newgrp | newres | newusr} ¥
{className resourceName calendar(calendarName) ¥
groupName calendar(calendarName) ¥
userName calendar(calendarName) }
```

CALENDAR クラスのレコードをリソースから削除するには、以下の構文を使用します。

```
{className resourceName calendar-(calendarName) ¥
groupName calendar-(calendarName) ¥
```

userName calendar-(*calendarName*) }

CATEGORY クラス

CATEGORY クラスの各レコードは、データベース内のセキュリティ カテゴリを定義します。1 つまたは複数のセキュリティ カテゴリが割り当てられたリソースに対してユーザがアクセス要求をすると、eTrust AC は、そのユーザ レコードのセキュリティ カテゴリのリストと、リソース レコードのセキュリティ カテゴリのリストを比較します。リソース レコードに指定されているセキュリティ カテゴリがユーザ レコードに含まれていない場合、eTrust AC はそのリソースへのアクセスを許可しません。リソース レコードに指定されたすべてのセキュリティ カテゴリがユーザ レコードに含まれている場合は、引き続き他の権限チェックが行われます。

CATEGORY クラスのレコードのキーは、セキュリティ カテゴリの名前です。
CATEGORY クラスのレコードの変更できるプロパティについて以下に説明します。

変更可能なプロパティ

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。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。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

CONNECT クラス

CONNECT クラスの各レコードは、接続先(リモート ホスト)を定義し、指定されたリモート ホストにローカル ホストから TCP 接続できるユーザを制御します。

CONNECT クラスのレコードのキーは、接続先リモート ホストの名前です。CONNECT クラスのレコードの変更できるプロパティについて以下に説明します。

注: レコードに TCP クラスを使用する場合、CONNECT クラスを使用しないでください。

変更可能なプロパティ

ACL

リソースへのアクセスを許可されているアクセサ(ユーザおよびグループ)およびアクセス タイプのリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。CONNECT クラスの有効なアクセス権限は、以下のとおりです。
  - none - どの操作の実行もアクセサに許可しません。
  - read - リモート ホストへの接続をアクセサに許可します。

ACL プロパティを変更するには、authorize コマンドで access(*authority*) パラメータ、または authorize- コマンドを使用します。

AUDIT

eTrust AC の監査ログに記録されるアクセス イベントのタイプです。有効な値は以下のとおりです。

- all - すべてのアクセス要求が監査されます。
- success - 許可されたすべてのアクセス要求が監査されます。
- failure - 拒否されたアクセス要求のみが監査されます。この値がデフォルト値です。
- none - アクセス要求の監査は行われません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで audit パラメータを使用します。

CALACL

カレンダ アクセス制御リストです。これは、Unicenter TNG カレンダ ステータスに基づいてリソースへのアクセスが許可されているアクセサ(ユーザおよびグループ)のリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **カレンダ参照** - Unicenter TNG のカレンダへの参照。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。CONNECT クラスの有効なアクセス権限は、以下のとおりです。
  - none - どの操作の実行もアクセサに許可しません。
  - read - リモート ホストへの接続をアクセサに許可します。

カレンダが有効な場合にのみアクセスが許可されます。その他の場合はすべてのアクセスが拒否されます。

ACL アクセスに基づいて、ユーザまたはグループにリソースへのアクセスを許可するには、authorize コマンドで calendar パラメータを使用します。

CALENDAR

eTrust AC のユーザ、グループ、およびリソース制限の Unicenter TNG カレンダ オブジェクトを表します。eTrust AC は、一定の間隔で Unicenter TNG のアクティブなカレンダを取得します。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで calendar パラメータと calendar- パラメータを使用します。

CATEGORY

リソースに割り当てる 1 つまたは複数のセキュリティ カテゴリです。CATEGORY クラスに定義されている任意のセキュリティ カテゴリを指定できます。リソースに 1 つまたは複数のセキュリティ 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**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。

リソースのこのプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで category[-] パラメータを使用します。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。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。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

DAYTIME

ユーザがリソースにアクセスできる日時を管理する、曜日と時刻の制限です。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで restrictions(days and time) パラメータを使用します。

GROUPS

リソース レコードが属する CONTAINER クラスのレコードのリストです。

CONNECT クラスのレコードのこのプロパティを変更するには、該当する CONTAINER クラスのレコードの MEMBERS プロパティを変更する必要があります。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで mem+ か mem- パラメータを使用します。

NACL

リソースへのアクセスが許可されないアクセサ(ユーザおよびグループ)と、許可されないアクセス タイプのリストです。NACL の各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを NACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されないアクセス** - アクセサが明示的にアクセスを許可されないリソースへのアクセスのタイプです。CONNECT クラスの有効なアクセス権限は、以下のとおりです。
  - none - すべての操作の実行をアクセサに許可します。
  - read - アクセサがリモート ホストに接続できないようにします。

NACL プロパティを変更するには、authorize コマンドで deniedaccess(*accesstype*) パラメータ、または authorize- コマンドで deniedaccess- パラメータを使用します。

NOTIFY

リソースの監査イベントが生成された場合に通知を受け取るユーザです。selogrd を使用して指定の電子メール アドレスに送信できる特別な監査レコードを作成することもできます。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで notify[-] パラメータを使用します。

制限: 30 文字。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

PACL

プログラム アクセス制御リストです。特定のプログラムから、またはプログラム名のパターンに一致するプログラムからアクセス要求が行われた場合に、アクセサに適用される ACL です。-名前パターン

パターンを指定すると、PACL によって保護されているリソースは、指定したパターンに一致するプログラムを使用しないとアクセスできません。プログラムが複数のパターンと一致する場合は、文字数が最も多いパターンが優先されます。

プログラム アクセス制御リストの各要素には、以下の情報が含まれています。

- **プログラム参照** - 指定または名前パターン一致による PROGRAM クラスのレコードへの参照。
- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。
- **許可されたアクセス** - 指定されたプログラムを使用している場合にアクセサに許可されるアクセス権。有効な値については、ACL プロパティを参照してください。

ACL プロパティにプログラム、アクセサ、およびアクセス タイプを追加するには、authorize コマンドで via(pgm) パラメータを使用します。ACL プロパティからこれらを削除するには、authorize- コマンドで via(pgm) パラメータを使用します。

SECLABEL

リソースのセキュリティ ラベルです。セキュリティ ラベルは、セキュリティ レベルをセキュリティ カテゴリに関連付けます。

適用する場合、セキュリティ ラベルは、レコードに設定された特定のセキュリティ レベルおよびセキュリティ カテゴリよりも優先されます。セキュリティ ラベルを割り当てることは、ラベルのレベルとカテゴリをユーザに明示的に割り当てることと同じです。指定されたセキュリティ ラベルは、SECLABEL クラスのレコードとして定義する必要があります。USER クラスのレコードにセキュリティ ラベルが設定されている場合は、以下の条件が両方とも満たされている場合にのみ、リソースへのアクセス権がユーザに与えられます。

- セキュリティ ラベルに指定されたユーザのセキュリティ レベルが、リソースのセキュリティ レベル以上であること。
- リソース レコードに指定されたすべてのセキュリティ カテゴリが、ユーザのセキュリティ ラベルのセキュリティ カテゴリ リストに含まれていること。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで label[-] パラメータを使用します。

SECLEVEL

ユーザまたはリソースのセキュリティ レベルです。セキュリティ レベルは 0 から 255 までの正の整数です。値 0 は、セキュリティ レベルを割り当てないことを意味します。リソースにセキュリティ レベルを割り当てた場合は、ユーザのセキュリティ レベルがリソースのセキュリティ レベル以上である場合にのみ、リソースへのアクセス権がユーザに与えられます。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで level[-] パラメータを使用します。

UACC

リソースに対するデフォルトのアクセス権です。eTrust AC に定義されていないアクセサ、またはリソースの ACL に登録されていないアクセサに与えるアクセス権を示します。有効な値については、リソースの ACL プロパティを参照してください。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで defaccess パラメータを使用します。

WARNING

警告モードを有効にするかどうかを示します。警告モードを有効にすると、すべてのアクセス要求が許可されます。アクセス要求がアクセス ルールに違反する場合は、レコードが監査ログに書き込まれます。

注: 警告モードの場合、eTrust Access Control では、リソース グループに対する警告メッセージは作成されません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで warning[-] パラメータを使用します。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

CONTAINER クラス

CONTAINER クラスの各レコードは、他のリソース クラスにあるオブジェクトのグループを定義します。これにより、複数の異なるオブジェクトのクラスに 1 つのルールを適用する場合に、アクセス ルールを定義する作業が簡略化されます。CONTAINER クラス レコードのメンバは、以下のいずれかのクラスのオブジェクトになることができます。

- APPL
- AUTHHOST
- CONNECT
- CONTAINER
- DICTIONARY
- DOMAIN
- FILE
- GAPPL
- GAUTHHOST
- GFILE
- GHOST
- GSUDO
- GTERMINAL
- HOLIDAY
- HOST
- MFTERMINAL
- PARAM_DESC
- PROCESS
- PROGRAM
- REGKEY(Windows のみ)
- SPECIALPGM
- SUDO
- SURROGATE
- TCP
- TERMINAL
- WEBSERVICE

注: CONTAINER レコードは、他の CONTAINER レコードにネストすることができます。

オブジェクトを CONTAINER レコードのメンバとして指定する前に、該当するクラスにそのオブジェクトのレコードを作成する必要があります。

コンテナ内のオブジェクトが、その該当するクラス レコード内に ACL を持たない場合、そのオブジェクトは、所属している CONTAINER レコードの ACL を継承します。

CONTAINER クラスのキーは、CONTAINER レコードの名前です。CONTAINER クラスのレコードの変更できるプロパティについて以下に説明します。

変更可能なプロパティ

ACL

リソースへのアクセスを許可されているアクセサ(ユーザおよびグループ)およびアクセス タイプのリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。CONTAINER クラスに対する有効なアクセス権限は、そのクラスに含まれるオブジェクトに対する有効なアクセス タイプとなります。該当するクラスに記載されている一覧を参照してください。

ACL プロパティを変更するには、authorize コマンドで access(*authority*) パラメータ、または authorize- コマンドを使用します。

AUDIT

eTrust AC の監査ログに記録されるアクセス イベントのタイプです。有効な値は以下のとおりです。

- all - すべてのアクセス要求が監査されます。
- success - 許可されたすべてのアクセス要求が監査されます。
- failure - 拒否されたアクセス要求のみが監査されます。この値がデフォルト値です。
- none - アクセス要求の監査は行われません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで audit パラメータを使用します。

CALACL

カレンダ アクセス制御リストです。これは、Unicenter TNG カレンダ ステータスに基づいてリソースへのアクセスが許可されているアクセサ(ユーザおよびグループ)のリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **カレンダ参照** - Unicenter TNG のカレンダへの参照。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。CONTAINER クラスに対する有効なアクセス権限は、そのクラスに含まれるオブジェクトに対する有効なアクセス タイプとなります。該当するクラスに記載されている一覧を参照してください。

カレンダが有効な場合にのみアクセスが許可されます。その他の場合はすべてのアクセスが拒否されます。

ACL アクセスに基づいて、ユーザまたはグループにリソースへのアクセスを許可するには、authorize コマンドで calendar パラメータを使用します。

CALENDAR

eTrust AC のユーザ、グループ、およびリソース制限の Unicenter TNG カレンダオブジェクトを表します。eTrust AC は、一定の間隔で Unicenter TNG のアクティブなカレンダを取得します。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで calendar パラメータと calendar- パラメータを使用します。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。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。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

DAYTIME

ユーザがリソースにアクセスできる日時を管理する、曜日と時刻の制限です。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで restrictions(days and time) パラメータを使用します。

GROUPS

コンテナ レコードが属する CONTAINER クラスのレコードのリストです。

このプロパティを変更するには、該当する CONTAINER クラスのレコードの MEMBERS プロパティを変更する必要があります。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで mem+ か mem- パラメータを使用します。

MEMBERS

任意のクラスにある、グループのメンバとなるオブジェクトのリストです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで mem+ か mem- パラメータを使用します。

NACL

リソースへのアクセスが許可されないアクセサ(ユーザおよびグループ)と、許可されないアクセス タイプのリストです。NACL の各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを NACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されないアクセス** - アクセサが明示的にアクセスを許可されないリソースへのアクセスのタイプです。CONTAINER クラスに対する有効なアクセス権限は、そのクラスに含まれるオブジェクトに対する有効なアクセス タイプとなります。該当するクラスに記載されている一覧を参照してください。

NACL プロパティを変更するには、authorize コマンドで deniedaccess(*accesstype*) パラメータ、または authorize- コマンドで deniedaccess- パラメータを使用します。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

PACL

プログラム アクセス制御リストです。特定のプログラムから、またはプログラム名のパターンに一致するプログラムからアクセス要求が行われた場合に、アクセサに適用される ACL です。

パターンを指定すると、PACL によって保護されているリソースは、指定したパターンに一致するプログラムを使用しないとアクセスできません。プログラムが複数のパターンと一致する場合は、文字数が最も多いパターンが優先されます。

プログラム アクセス制御リストの各要素には、以下の情報が含まれています。

- **プログラム参照** - 指定または名前パターン一致による PROGRAM クラスのレコードへの参照。
- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。
- **許可されたアクセス** - 指定されたプログラムを使用している場合にアクセサに許可されるアクセス権。有効な値については、ACL プロパティを参照してください。

ACL プロパティにプログラム、アクセサ、およびアクセス タイプを追加するには、authorize コマンドで via(pgm) パラメータを使用します。ACL プロパティからこれらを削除するには、authorize- コマンドで via(pgm) パラメータを使用します。

WARNING

警告モードを有効にするかどうかを示します。警告モードを有効にすると、すべてのアクセス要求が許可されます。アクセス要求がアクセス ルールに違反する場合は、レコードが監査ログに書き込まれます。

注: 警告モードの場合、eTrust Access Control では、リソース グループに対する警告メッセージは作成されません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで warning[-] パラメータを使用します。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

selang の構文

CONTAINER オブジェクトにメンバを追加するには、以下の構文を使用します。

```
{chres | editres |newres} CONTAINER (resourceName) mem+(memberName1, ¥
memberName2,....) of_class(memberClassName)
```

クラスが同じであれば一度に複数のメンバを(カンマで区切って)追加できますが、異なるクラスのメンバを追加する場合は、of_class 記述子があるため、クラスごとにコマンドを指定する必要があることに注意してください。

CONTAINER オブジェクトからメンバを削除するには、以下の構文を使用します。

```
{chres | editres} CONTAINER (resourceName) mem-(memberName1, ¥
 memberName2,....) of_class(memberClassName)
```

authorize コマンドを使用する場合の構文は以下のとおりです。

```
{authorize | auth} CONTAINER resourceName ¥
[uid({userName | *})] ¥
[gid(groupName)] ¥
[access(authority)]
```

authority は、コンテナ内のすべてのクラスに対して有効なアクセス権限です。

例

1. 同じクラスのメンバからなる *cont1* というコンテナを作成します。

   newres CONTAINER cont1 mem+(polaris, betelgeuse, sirius) of_class(TERMINAL)

2. 異なるクラスのメンバを追加します。

   chres CONTAINER cont1 mem+(D:¥file.txt) of_class(FILE)

3. ある特定のクラスに属するメンバを削除します。

   chres CONTAINER cont1 mem-(polaris, sirius) of_class(TERMINAL)

DICTIONARY クラス

DICTIONARY クラスの各レコードは、eTrust AC データベースに格納されている共通辞書内の、パスワードと比較する単語を定義します。ユーザがパスワードを変更すると、変更されたパスワードは、この DICTIONARY クラスの各レコードと照合してチェックされます。

DICTIONARY クラスへのレコード(単語)の追加に加えて、ユーティリティまたはプログラムを実行して、外部ファイルから辞書へ単語をインポートすることができます。

DICTIONARY クラスのレコードの変更できるプロパティについて以下に説明します。

変更可能なプロパティ

AUDIT

eTrust AC の監査ログに記録されるアクセス イベントのタイプです。有効な値は以下のとおりです。

- all - すべてのアクセス要求が監査されます。
- none - アクセス要求の監査は行われません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで audit パラメータを使用します。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで owner パラメータを使用します。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。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。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで comment[-] パラメータを使用します。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

DOMAIN クラス

DOMAIN クラスの各レコードは、Windows ネットワークのドメインを定義します（Windows 専用のクラスです）。

DOMAIN レコードのキーは、ドメイン名です。DOMAIN クラスのレコードの変更できるプロパティについて以下に説明します。

変更可能なプロパティ

ACL

リソースへのアクセスを許可されているアクセサ（ユーザおよびグループ）およびアクセス タイプのリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ（ユーザまたはグループ）への参照。eTrust AC に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク（*）を入力します。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。

ACL プロパティを変更するには、authorize コマンドで access(*authority*) パラメータ、または authorize- コマンドを使用します。

AUDIT

eTrust AC の監査ログに記録されるアクセス イベントのタイプです。有効な値は以下のとおりです。

- all - すべてのアクセス要求が監査されます。
- success - 許可されたすべてのアクセス要求が監査されます。
- failure - 拒否されたアクセス要求のみが監査されます。この値がデフォルト値です。
- none - アクセス要求の監査は行われません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで audit パラメータを使用します。

CALACL

カレンダ アクセス制御リストです。これは、Unicenter TNG カレンダ ステータスに基づいてリソースへのアクセスが許可されているアクセサ（ユーザおよびグループ）のリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ（ユーザまたはグループ）への参照。eTrust AC に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク（*）を入力します。
- **カレンダ参照** - Unicenter TNG のカレンダへの参照。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。

カレンダが有効な場合にのみアクセスが許可されます。その他の場合はすべてのアクセスが拒否されます。

ACL アクセスに基づいて、ユーザまたはグループにリソースへのアクセスを許可するには、authorize コマンドで calendar パラメータを使用します。

CALENDAR

eTrust AC のユーザ、グループ、およびリソース制限の Unicenter TNG カレンダオブジェクトを表します。eTrust AC は、一定の間隔で Unicenter TNG のアクティブなカレンダを取得します。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで calendar パラメータと calendar- パラメータを使用します。

CATEGORY

リソースに割り当てる 1 つまたは複数のセキュリティ カテゴリです。CATEGORY クラスに定義されている任意のセキュリティ カテゴリを指定できます。リソースに 1 つまたは複数のセキュリティ 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**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。

リソースのこのプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで category[-] パラメータを使用します。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。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。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

DAYTIME

ユーザがリソースにアクセスできる日時を管理する、日付と時刻の制限です。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで restrictions(days and time) パラメータを使用します。

GROUPS

レコードが属する CONTAINER クラスのレコードのリストです。

DOMAIN クラスのレコードのこのプロパティを変更するには、該当する CONTAINER クラスのレコードの MEMBERS プロパティを変更する必要があります。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで mem+ か mem- パラメータを使用します。

NACL

リソースへのアクセスが許可されないアクセサ(ユーザおよびグループ)と、許可されないアクセス タイプのリストです。NACL の各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを NACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されないアクセス** - アクセサが明示的にアクセスを許可されないリソースへのアクセスのタイプです。

NACL プロパティを変更するには、authorize コマンドで deniedaccess(*accesstype*) パラメータ、または authorize- コマンドで deniedaccess- パラメータを使用します。

NOTIFY

リソースの監査イベントが生成された場合に通知を受け取るユーザです。selogrd を使用して指定の電子メール アドレスに送信できる特別な監査レコードを作成することもできます。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで notify[-] パラメータを使用します。

制限: 30 文字。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

PACL

プログラム アクセス制御リストです。特定のプログラムから、またはプログラム名のパターンに一致するプログラムからアクセス要求が行われた場合に、アクセサに適用される ACL です。

パターンを指定すると、PACL によって保護されているリソースは、指定したパターンに一致するプログラムを使用しないとアクセスできません。プログラムが複数のパターンと一致する場合は、文字数が最も多いパターンが優先されます。

プログラム アクセス制御リストの各要素には、以下の情報が含まれています。

- **プログラム参照** - 指定または名前パターン一致による PROGRAM クラスのレコードへの参照。
- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。
- **許可されたアクセス** - 指定されたプログラムを使用している場合にアクセサに許可されるアクセス権。有効な値については、ACL プロパティを参照してください。

ACL プロパティにプログラム、アクセサ、およびアクセス タイプを追加するには、authorize コマンドで via(pgm) パラメータを使用します。ACL プロパティからこれらを削除するには、authorize- コマンドで via(pgm) パラメータを使用します。

SECLABEL

リソースのセキュリティ ラベルです。セキュリティ ラベルは、セキュリティ レベルをセキュリティ カテゴリに関連付けます。

適用する場合、セキュリティ ラベルは、レコードに設定された特定のセキュリティ レベルおよびセキュリティ カテゴリよりも優先されます。セキュリティ ラベルを割り当てることは、ラベルのレベルとカテゴリをユーザに明示的に割り当てることと同じです。指定されたセキュリティ ラベルは、SECLABEL クラスのレコードとして定義する必要があります。USER クラスのレコードにセキュリティ ラベルが設定されている場合は、以下の条件が両方とも満たされている場合にのみ、リソースへのアクセス権がユーザに与えられます。

- セキュリティ ラベルに指定されたユーザのセキュリティ レベルが、リソースのセキュリティ レベル以上であること。
- リソース レコードに指定されたすべてのセキュリティ カテゴリが、ユーザのセキュリティ ラベルのセキュリティ カテゴリ リストに含まれていること。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで label[-] パラメータを使用します。

SECLEVEL

ユーザまたはリソースのセキュリティ レベルです。セキュリティ レベルは 0 から 255 までの正の整数です。値 0 は、セキュリティ レベルを割り当てないことを意味します。リソースにセキュリティ レベルを割り当てた場合は、ユーザのセキュリティ レベルがリソースのセキュリティ レベル以上である場合にのみ、リソースへのアクセス権がユーザに与えられます。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで level[-] パラメータを使用します。

UACC

リソースに対するデフォルトのアクセス権です。eTrust Access Control に定義されていないアクセサ、またはリソースの ACL に登録されていないアクセサに与えるアクセス権を示します。有効な値については、リソースの ACL プロパティを参照してください。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで defaccess パラメータを使用します。

WARNING

警告モードを有効にするかどうかを示します。警告モードを有効にすると、すべてのアクセス要求が許可されます。アクセス要求がアクセス ルールに違反する場合は、レコードが監査ログに書き込まれます。

注: 警告モードの場合、eTrust Access Control では、リソース グループに対する警告メッセージは作成されません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで warning[-] パラメータを使用します。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

FILE クラス

FILE クラスの各レコードは、特定のファイル、特定のディレクトリ、またはファイル名パターンが一致しているファイルに対するアクセス権限を定義します。まだ作成していないファイルについてもルールを定義できます。

デバイス ファイルおよびシンボリック リンクも他のファイルと同様に保護できます。ただし、リンクを保護しても、リンク先のファイルは自動的に保護されません。

スクリプトをファイルとして定義する場合は、ファイルに対する read アクセス権と execute アクセス権の両方を許可します。バイナリを定義する場合は、execute アクセス権のみで十分です。

特別な _restricted グループに属していないユーザの場合、FILE クラスの _default レコード(_default レコードがない場合は UACC クラスの FILE のレコード)では、seos.ini ファイル、seosd.trace ファイル、seos.audit ファイル、および seos.error ファイルなど、*eTrust AC* の一部であるファイルのみが保護されます。これらのファイルは eTrust AC に明示的に定義されていませんが、eTrust AC で自動的に保護されます。

FILE クラスのレコードのキーは、レコードが保護するファイルまたはディレクトリの名前です。完全パスを指定する必要があります。FILE クラスのレコードの変更できるプロパティについて以下に説明します。

変更可能なプロパティ

ACL

リソースへのアクセスを許可されているアクセサ(ユーザおよびグループ)およびアクセス タイプのリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。FILE クラスの有効なアクセス権限は、以下のとおりです。
  - all - そのクラスに対して許可されるすべての操作の実行をアクセサに許可します。
  - chdir - read および execute に相当するディレクトリへのアクセス権をアクセサに許可します。
  - chown - ファイルの所有者の変更をアクセサに許可します。
  - control - delete および rename 以外のすべてのアクセス権をアクセサに許可します。
  - create - ファイルの作成をアクセサに許可します。

- delete - ファイルの削除をアクセサに許可します。
- execute - プログラムの実行をアクセサに許可します。このアクセス タイプを使用するには、読み取りアクセス権限も必要です。
- none - どの操作の実行もアクセサに許可しません。
- read - ファイルまたはディレクトリを変更せずに使用することをアクセサに許可します。
- rename - ファイル名の変更をアクセサに許可します。
- sec - ファイルの ACL の変更をアクセサに許可します。
- update - read、write、および execute を組み合わせたアクセス権をアクセサに許可します。
- utime - ファイル変更日時の変更をアクセサに許可します。
- write - ファイルまたはディレクトリの変更をアクセサに許可します。

ACL プロパティを変更するには、authorize コマンドで access(*authority*) パラメータ、または authorize- コマンドを使用します。

AUDIT

eTrust AC の監査ログに記録されるアクセス イベントのタイプです。有効な値は以下のとおりです。

- all - すべてのアクセス要求が監査されます。
- success - 許可されたすべてのアクセス要求が監査されます。
- failure - 拒否されたアクセス要求のみが監査されます。この値がデフォルト値です。
- none - アクセス要求の監査は行われません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで audit パラメータを使用します。

CALACL

カレンダ アクセス制御リストです。これは、Unicenter TNG カレンダ ステータスに基づいてリソースへのアクセスが許可されているアクセサ(ユーザおよびグループ)のリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

アクセサ参照 - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。

- **カレンダ参照** - Unicenter TNG のカレンダへの参照。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。FILE クラスの有効なアクセス権限は、以下のとおりです。
  - all - そのクラスに対して許可されるすべての操作の実行をアクセサに許可します。

- chdir - read および execute に相当するディレクトリへのアクセス権をアクセサに許可します。
- chown - ファイルの所有者の変更をアクセサに許可します。
- control - delete および rename 以外のすべてのアクセス権をアクセサに許可します。
- create - ファイルの作成をアクセサに許可します。
- delete - ファイルの削除をアクセサに許可します。
- execute - プログラムの実行をアクセサに許可します。このアクセス タイプを使用するには、読み取りアクセス権限も必要です。
- none - どの操作の実行もアクセサに許可しません。
- read - ファイルまたはディレクトリを変更せずに使用することをアクセサに許可します。
- rename - ファイル名の変更をアクセサに許可します。
- sec - ファイルの ACL の変更をアクセサに許可します。
- update - read、write、および execute を組み合わせたアクセス権をアクセサに許可します。
- utime - ファイル変更日時の変更をアクセサに許可します。
- write - ファイルまたはディレクトリの変更をアクセサに許可します。

カレンダが有効な場合にのみアクセスが許可されます。その他の場合はすべてのアクセスが拒否されます。

ACL アクセスに基づいて、ユーザまたはグループにリソースへのアクセスを許可するには、authorize コマンドで calendar パラメータを使用します。

CALENDAR

eTrust AC のユーザ、グループ、およびリソース制限の Unicenter TNG カレンダ オブジェクトを表します。eTrust AC は、一定の間隔で Unicenter TNG のアクティブなカレンダを取得します。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで calendar パラメータと calendar- パラメータを使用します。

CATEGORY

リソースに割り当てる 1 つまたは複数のセキュリティ カテゴリです。CATEGORY クラスに定義されている任意のセキュリティ カテゴリを指定できます。リソースに 1 つまたは複数のセキュリティ 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**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。

リソースのこのプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで category[-] パラメータを使用します。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。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。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

DAYTIME

ユーザがリソースにアクセスできる日時を管理する、曜日と時刻の制限です。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで restrictions(days and time) パラメータを使用します。

GROUPS

リソース レコードが属する GFILE クラスまたは CONTAINER クラスのレコードのリストです。

FILE クラスのレコードのこのプロパティを変更するには、該当する CONTAINER クラスまたは GFILE クラスのレコードの MEMBERS プロパティを変更する必要があります。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで mem+ か mem- パラメータを使用します。

NACL

リソースへのアクセスが許可されないアクセサ(ユーザおよびグループ)と、許可されないアクセス タイプのリストです。NACL の各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを NACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されないアクセス** - アクセサが明示的にアクセスを許可されないリソースへのアクセスのタイプです。FILE クラスの有効なアクセス権限は、以下のとおりです。
  - all - アクセサがそのクラスに対してすべての操作を実行できないようにします。
  - chdir - read および execute に相当する権限を持つアクセサがディレクトリにアクセスできないようにします。
  - chown - ファイルの所有者の変更をアクセサに許可します。
  - control - アクセサが delete および rename 以外のすべてのアクセスを行うことができないようにします。
  - create - アクセサがファイルを作成できないようにします。
  - execute - アクセサがプログラムを実行できないようにします。このアクセスタイプを使用するには、読み取りアクセス権限も必要です。

- none - すべての操作の実行をアクセサに許可します。
- read - アクセサがファイルを表示できないようにします。
- rename - アクセサがファイルの名前を変更できないようにします。
- sec - アクセサがファイルの ACL を変更できないようにします。
- update - アクセサがファイルを更新できないようにします。
- utime - アクセサがファイルの変更時刻を変更できないようにします。
- write - アクセサがファイルまたはディレクトリを変更できないようにします。

NACL プロパティを変更するには、authorize コマンドで deniedaccess(*accesstype*) パラメータ、または authorize- コマンドで deniedaccess- パラメータを使用します。

NOTIFY

リソースの監査イベントが生成された場合に通知を受け取るユーザです。selogrd を使用して指定の電子メール アドレスに送信できる特別な監査レコードを作成することもできます。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで notify[-] パラメータを使用します。

制限: 30 文字。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

PACL

プログラム アクセス制御リストです。特定のプログラムから、またはプログラム名のパターンに一致するプログラムからアクセス要求が行われた場合に、アクセサに適用される ACL です。

パターンを指定すると、PACL によって保護されているリソースは、指定したパターンに一致するプログラムを使用しないとアクセスできません。プログラムが複数のパターンと一致する場合は、文字数が最も多いパターンが優先されます。

プログラム アクセス制御リストの各要素には、以下の情報が含まれています。

- **プログラム参照** - 指定または名前パターン一致による PROGRAM クラスのレコードへの参照。
- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。
- **許可されたアクセス** - 指定されたプログラムを使用している場合にアクセサに許可されるアクセス権。有効な値については、ACL プロパティを参照してください。

ACL プロパティにプログラム、アクセサ、およびアクセス タイプを追加するには、authorize コマンドで via(pgm) パラメータを使用します。ACL プロパティからこれらを削除するには、authorize- コマンドで via(pgm) パラメータを使用します。

SECLABEL

リソースのセキュリティ ラベルです。セキュリティ ラベルは、セキュリティ レベルをセキュリティ カテゴリに関連付けます。

適用する場合、セキュリティ ラベルは、レコードに設定された特定のセキュリティ レベルおよびセキュリティ カテゴリよりも優先されます。セキュリティ ラベルを割り当てることは、ラベルのレベルとカテゴリをユーザに明示的に割り当てることと同じです。指定されたセキュリティ ラベルは、SECLABEL クラスのレコードとして定義する必要があります。USER クラスのレコードにセキュリティ ラベルが設定されている場合は、以下の条件が両方とも満たされている場合にのみ、リソースへのアクセス権がユーザに与えられます。

- セキュリティ ラベルに指定されたユーザのセキュリティ レベルが、リソースのセキュリティ レベル以上であること。
- リソース レコードに指定されたすべてのセキュリティ カテゴリが、ユーザのセキュリティ ラベルのセキュリティ カテゴリ リストに含まれていること。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで label[-] パラメータを使用します。

SECLEVEL

ユーザまたはリソースのセキュリティ レベルです。セキュリティ レベルは 0 から 255 までの正の整数です。値 0 は、セキュリティ レベルを割り当てないことを意味します。リソースにセキュリティ レベルを割り当てた場合は、ユーザのセキュリティ レベルがリソースのセキュリティ レベル以上である場合にのみ、リソースへのアクセス権がユーザに与えられます。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで level[-] パラメータを使用します。

UACC

リソースに対するデフォルトのアクセス権です。eTrust Access Control に定義されていないアクセサ、またはリソースの ACL に登録されていないアクセサに与えるアクセス権を示します。有効な値については、リソースの ACL プロパティを参照してください。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで defaccess パラメータを使用します。

WARNING

警告モードを有効にするかどうかを示します。警告モードを有効にすると、すべてのアクセス要求が許可されます。アクセス要求がアクセス ルールに違反する場合は、レコードが監査ログに書き込まれます。

注: 警告モードの場合、eTrust Access Control では、リソース グループに対する警告メッセージは作成されません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで warning[-] パラメータを使用します。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

ファイル名パターン

個別のファイルまたは指定されたファイル名パターン(**マスク**)に一致するすべてのファイルに対して、FILE クラスのレコードを作成できます。マスクには、ワイルドカードとして ?(パスを区切る文字以外の任意の 1 文字を表す)および *(0 個以上の文字を表す)を使用できます。eTrust AC では、以下のファイル名マスクは指定できません。

- /*
- /tmp/*
- /etc/*

一部の特定のファイルについては、FILE クラスのレコードがない場合でもアクセスルールが適用されます。

- (UNIX/Linux のみ)すべてのユーザは、少なくとも、/etc/group ファイルおよび *eTrustACDir*/seos.ini ファイルに対する読み取りアクセス権を必ず持っています。書き込みアクセス権限を与えるには、これらのファイルに対して FILE クラスのレコードを作成します。
- (UNIX/Linux のみ)デフォルトでは、*eTrustACDir*/etc/loginpgms.init ファイル、*eTrustACDir*/etc/nfsdevs.init ファイル、*eTrustACDir*/etc/privpgms.init ファイル、および *eTrustACDir*/etc/xdmpgms.init ファイルは、FILE クラスの _default レコードにより保護されます。ただし、独自の FILE クラスのレコードをこれらのファイルに作成すると、その保護がこのデフォルトの保護より優先されます。
- (UNIX/Linux のみ)*eTrustACDir*/bin/* ファイルには、eTrust AC のバイナリ実行可能ファイルが含まれています。このファイルは、FILE クラスのレコードによって保護できます。特定の FILE クラスのレコードがこのようなファイルを保護せず、(UNIX/Linux の seos.ini ファイルで)protect_bin トークンが yes に設定されている場合は、これらのファイルには FILE クラスの _default アクセス ルールが適用されます。このトークンのデフォルトは no です。これは、ファイルに適用される特定の FILE クラスのレコードが存在する場合、そのレコードによってのみファイルが保護されることを意味します。

重要: protect_bin トークンが yes に設定されている間は、FILE クラスのレコードで _default アクセスを none に設定しないでください。すべての eTrustACDir/bin ファイルに FILE クラスのレコードがないと、このような設定の組み合わせにより、eTrust AC を使用できなくなることがあります。

(Windows のみ)すべてのユーザは、少なくとも、*system_directory*¥system32¥pwdchange.dll ファイルおよび *system_directory*¥system32¥susrauth.dll ファイルに対する読み取りアクセス権限を必ず持っています。

注: 監査ログとそのバックアップ ファイル、エラー ログとそのバックアップ ファイル、トレース ログと seos データベース、seos ヘルプ ファイル、および seos メッセージ ファイルはユーザが読み取ることができますが、書き込みができるのは eTrust AC のみです。これらのファイルに対して指定した FILE クラスのレコードは無視されます。

GAPPL クラス

GAPPL クラスの各レコードは、eTrust Web Access Control または eTrust Single Sign-On で使用するアプリケーションのグループを定義します。各アプリケーションの APPL クラスのレコードを作成した後に、そのレコードを GAPPL クラスのレコードに追加する必要があります。次に、APPL クラスのレコードを GAPPL クラスのレコードに明示的に連結してグループ化します。

GAPPL クラスのレコードのキーは、GAPPL クラスのレコードの名前です。GAPPL クラスのレコードで変更できるプロパティについて以下に説明します。

変更可能なプロパティ

ACL

リソースへのアクセスを許可されているアクセサ(ユーザおよびグループ)およびアクセス タイプのリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。GAPPL クラスの有効なアクセス権限は、以下のとおりです。
  - execute - プログラムの実行をアクセサに許可します。このアクセス タイプを使用するには、読み取りアクセス権限も必要です。
  - none - どの操作の実行もアクセサに許可しません。
  - read - ファイルまたはディレクトリを変更せずに使用することをアクセサに許可します。

ACL プロパティを変更するには、authorize コマンドで access(*authority*) パラメータ、または authorize- コマンドを使用します。

AUDIT

eTrust AC の監査ログに記録されるアクセス イベントのタイプです。有効な値は以下のとおりです。

- all - すべてのアクセス要求が監査されます。
- success - 許可されたすべてのアクセス要求が監査されます。
- failure - 拒否されたアクセス要求のみが監査されます。この値がデフォルト値です。
- none - アクセス要求の監査は行われません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで audit パラメータを使用します。

AZNACL

権限 ACL です。リソースの説明に基づいてリソースへのアクセスを許可できます。説明は、オブジェクトではなく認証エンジンに送信されます。オブジェクトは、ほとんどの場合データベースに存在しません。

CALACL

カレンダ アクセス制御リストです。これは、Unicenter TNG カレンダ ステータスに基づいてリソースへのアクセスが許可されているアクセサ(ユーザおよびグループ)のリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **カレンダ参照** - Unicenter TNG のカレンダへの参照。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。GAPPL クラスの有効なアクセス権限は、以下のとおりです。
  - execute - プログラムの実行をアクセサに許可します。このアクセス タイプを使用するには、読み取りアクセス権限も必要です。
  - none - どの操作の実行もアクセサに許可しません。
  - read - ファイルまたはディレクトリを変更せずに使用することをアクセサに許可します。

カレンダが有効な場合にのみアクセスが許可されます。その他の場合はすべてのアクセスが拒否されます。

ACL アクセスに基づいて、ユーザまたはグループにリソースへのアクセスを許可するには、authorize コマンドで calendar パラメータを使用します。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。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。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

GROUPS

リソース レコードが属する CONTAINER クラスのレコードのリストです。

GAPPL クラスのレコードのこのプロパティを変更するには、該当する CONTAINER クラスのレコードの MEMBERS プロパティを変更する必要があります。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで mem+ か mem- パラメータを使用します。

MEMBERS

APPL クラスにある、グループのメンバとなるオブジェクトのリストです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで mem+ か mem- パラメータを使用します。

NACL

リソースへのアクセスが許可されないアクセサ(ユーザおよびグループ)と、許可されないアクセス タイプのリストです。NACL の各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを NACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されないアクセス** -アクセサが明示的にアクセスを許可されないリソースへのアクセスのタイプです。GAPPL クラスの有効なアクセス権限は、以下のとおりです。
  - execute-アクセサがプログラムを実行できないようにします。このアクセスタイプを使用するには、読み取りアクセス権限も必要です。
  - none - すべての操作の実行をアクセサに許可します。
  - read - アクセサがファイルまたはディレクトリを表示できないようにします。

NACL プロパティを変更するには、authorize コマンドで deniedaccess(*accesstype*) パラメータ、または authorize- コマンドで deniedaccess- パラメータを使用します。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

GAUTHHOST クラス

GAUTHHOST クラスの各レコードは、eTrust Web Access Control または eTrust Single Sign-On で使用する認証ホストのグループを定義します。各アプリケーションの AUTHHOST クラスのレコードを作成した後に、作成したレコードを GAUTHHOST クラスのレコードに追加する必要があります。次に、AUTHHOST クラスのレコードを GAUTHHOST クラスのレコードに明示的に連結してグループ化します。

GAUTHHOST クラスのレコードのキーは、GAUTHHOST クラスのレコードの名前です。GAUTHHOST クラスのレコードで変更できるプロパティについて以下に説明します。

変更可能なプロパティ

ACL

リソースへのアクセスを許可されているアクセサ(ユーザおよびグループ)およびアクセス タイプのリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。GAUTHHOST クラスの有効なアクセス権限は、以下のとおりです。
  - none - どの操作の実行もアクセサに許可しません。
  - read- 認証されたホストからのログインをアクセサに許可します。

ACL プロパティを変更するには、authorize コマンドで access(*authority*) パラメータ、または authorize- コマンドを使用します。

AUDIT

eTrust AC の監査ログに記録されるアクセス イベントのタイプです。有効な値は以下のとおりです。

- all - すべてのアクセス要求が監査されます。
- success - 許可されたすべてのアクセス要求が監査されます。
- failure - 拒否されたアクセス要求のみが監査されます。この値がデフォルト値です。
- none - アクセス要求の監査は行われません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで audit パラメータを使用します。

AZNACL

権限 ACL です。リソースの説明に基づいてリソースへのアクセスを許可できます。説明は、オブジェクトではなく認証エンジンに送信されます。オブジェクトは、ほとんどの場合データベースに存在しません。

CALACL

カレンダ アクセス制御リストです。これは、Unicenter TNG カレンダ ステータスに基づいてリソースへのアクセスが許可されているアクセサ(ユーザおよびグループ)のリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **カレンダ参照** - Unicenter TNG のカレンダへの参照。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。GAUTHHOST クラスの有効なアクセス権限は、以下のとおりです。
  - none - どの操作の実行もアクセサに許可しません。
  - read- 認証されたホストからのログインをアクセサに許可します。

カレンダが有効な場合にのみアクセスが許可されます。その他の場合はすべてのアクセスが拒否されます。

ACL アクセスに基づいて、ユーザまたはグループにリソースへのアクセスを許可するには、authorize コマンドで calendar パラメータを使用します。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。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。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

GROUPS

リソース レコードが属する CONTAINER クラスのレコードのリストです。

GAUTHHOST クラスのレコードのこのプロパティを変更するには、該当する CONTAINER クラスのレコードの MEMBERS プロパティを変更する必要があります。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで mem+ か mem- パラメータを使用します。

MEMBERS

AUTHHOST クラスにある、グループのメンバとなるオブジェクトのリストです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで mem+ か mem- パラメータを使用します。

NACL

リソースへのアクセスが許可されないアクセサ(ユーザおよびグループ)と、許可されないアクセス タイプのリストです。NACL の各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを NACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されないアクセス** - アクセサが明示的にアクセスを許可されないリソースへのアクセスのタイプです。GAUTHHOST クラスの有効なアクセス権限は、以下のとおりです。
  - none - すべての操作の実行をアクセサに許可します。
  - read- 認証されたホストからアクセサがログインできないようにします。

NACL プロパティを変更するには、authorize コマンドで deniedaccess(*accesstype*) パラメータ、または authorize- コマンドで deniedaccess- パラメータを使用します。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

GFILE クラス

GFILE クラスの各レコードは、特定のファイルまたはディレクトリのグループ、または名前パターンと一致するファイルに対して許可するアクセス権限を定義します。各アプリケーションの FILE クラス レコードを作成した後に、作成したレコードを GFILE レコードに追加する必要があります。次に、FILE クラスのレコードを GFILE クラスのレコードに明示的に連結してグループ化します。まだ作成していないファイルについても、FILE クラスのレコードを定義できます。

GFILE クラスのレコードのキーは、GFILE レコードの名前です。GFILE クラスのレコードで変更できるプロパティについて以下に説明します。

変更可能なプロパティ

ACL

リソースへのアクセスを許可されているアクセサ(ユーザおよびグループ)およびアクセス タイプのリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。GFILE クラスの有効なアクセス権限は、以下のとおりです。
  - none - どの操作の実行もアクセサに許可しません。
  - all - そのクラスに対して許可されるすべての操作の実行をアクセサに許可します。
  - chdir - read および execute に相当する、ディレクトリへのアクセス権をアクセサに許可します。
  - chown - グループ内のファイルの所有者の変更をアクセサに許可します。
  - chmod-- グループ内のファイルまたはディレクトリを削除する以外のすべての操作を許可または拒否します。
  - control - delete および rename 以外のすべてのアクセス権をアクセサに許可します。
  - create - ファイルの作成をアクセサに許可します。
  - delete - ファイルの削除をアクセサに許可します。
  - execute - プログラムの実行をアクセサに許可します。このアクセス タイプを使用するには、読み取りアクセス権限も必要です。
  - read - グループ内のファイルまたはディレクトリを変更せずに使用することをアクセサに許可します。

- rename - グループ内のファイルまたはディレクトリの名前の変更をアクセサに許可します。
- sec - グループ内のファイルまたはディレクトリの ACL の変更をアクセサに許可します。
- update - read、write、および execute を組み合わせたアクセス権をアクセサに許可します。
- utime - グループ内のファイルまたはディレクトリの変更日時の変更をアクセサに許可します。
- write - グループ内のファイルまたはディレクトリの変更をアクセサに許可します。

ACL プロパティを変更するには、authorize コマンドで access(*authority*) パラメータ、または authorize- コマンドを使用します。

AUDIT

eTrust AC の監査ログに記録されるアクセス イベントのタイプです。

有効な値は以下のとおりです。

- all - すべてのアクセス要求が監査されます。
- success - 許可されたすべてのアクセス要求が監査されます。
- failure - 拒否されたアクセス要求のみが監査されます。この値がデフォルト値です。
- none - アクセス要求の監査は行われません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで audit パラメータを使用します。

CALACL

カレンダ アクセス制御リストです。これは、Unicenter TNG カレンダ ステータスに基づいてリソースへのアクセスが許可されているアクセサ(ユーザおよびグループ)のリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **カレンダ参照** - Unicenter TNG のカレンダへの参照。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。有効な値については、ACL プロパティを参照してください。

カレンダが有効な場合にのみアクセスが許可されます。その他の場合はすべてのアクセスが拒否されます。

ACL アクセスに基づいて、ユーザまたはグループにリソースへのアクセスを許可するには、authorize コマンドで calendar パラメータを使用します。

CALENDAR

eTrust AC のユーザ、グループ、およびリソース制限の Unicenter TNG カレンダ オブジェクトを表します。eTrust AC は、一定の間隔で Unicenter TNG のアクティブなカレンダを取得します。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで calendar パラメータと calendar- パラメータを使用します。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。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。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

DAYTIME

ユーザがリソースにアクセスできる日時を管理する、曜日と時刻の制限です。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで restrictions(days and time) パラメータを使用します。

GROUPS

リソース レコードが属する CONTAINER クラスのレコードのリストです。

GFILE クラスのレコードのこのプロパティを変更するには、該当する CONTAINER クラスのレコードの MEMBERS プロパティを変更する必要があります。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで mem+ か mem- パラメータを使用します。

MEMBERS

FILE クラスにある、グループのメンバとなるオブジェクトのリストです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで mem+ か mem- パラメータを使用します。

NACL

リソースへのアクセスが許可されないアクセサ(ユーザおよびグループ)と、許可されないアクセス タイプのリストです。NACL の各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを NACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されないアクセス** - アクセサが明示的にアクセスを許可されないリソースへのアクセスのタイプです。有効な値については、ACL プロパティを参照してください。

NACL プロパティを変更するには、authorize コマンドで deniedaccess(*accesstype*) パラメータ、または authorize- コマンドで deniedaccess- パラメータを使用します。

NOTIFY

リソースの監査イベントが生成された場合に通知を受け取るユーザです。selogrd を使用して指定の電子メール アドレスに送信できる特別な監査レコードを作成することもできます。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで notify[-] パラメータを使用します。

制限: 30 文字。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

PACL

プログラム アクセス制御リストです。特定のプログラムから、またはプログラム名のパターンに一致するプログラムからアクセス要求が行われた場合に、アクセサに適用される ACL です。

パターンを指定すると、PACL によって保護されているリソースは、指定したパターンに一致するプログラムを使用しないとアクセスできません。プログラムが複数のパターンと一致する場合は、文字数が最も多いパターンが優先されます。

プログラム アクセス制御リストの各要素には、以下の情報が含まれています。

- **プログラム参照** - 指定または名前パターン一致による PROGRAM クラスのレコードへの参照。
- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。
- **許可されたアクセス** - 指定されたプログラムを使用している場合にアクセサに許可されるアクセス権。有効な値については、ACL プロパティを参照してください。

ACL プロパティにプログラム、アクセサ、およびアクセス タイプを追加するには、authorize コマンドで via(pgm) パラメータを使用します。ACL プロパティからこれらを削除するには、authorize- コマンドで via(pgm) パラメータを使用します。

WARNING

警告モードを有効にするかどうかを示します。警告モードを有効にすると、すべてのアクセス要求が許可されます。アクセス要求がアクセス ルールに違反する場合は、レコードが監査ログに書き込まれます。

注: 警告モードの場合、eTrust Access Control では、リソース グループに対する警告メッセージは作成されません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで warning[-] パラメータを使用します。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

GHOST クラス

GHOST クラスの各レコードは、ホストのグループを定義します。各ホストの HOST クラス レコードを作成した後に、作成したレコードを GHOST レコードに追加する必要があります。サービスは、/etc/services ファイル（UNIX/Linux の場合）、¥system32¥drivers¥etc¥services ファイル（Windows の場合）、または他のサービス名解決方法を使用して、システムに定義する必要があります。サービスに許可を与える場合は、サービスの名前ではなく TCP/IP プロトコルのポート番号で指定できます。サービスを追加する場合は、サービスの名前ではなく TCP/IP プロトコルのポート番号で指定できます。次に、HOST クラスのレコードを GHOST クラスのレコードに明示的に連結してグループ化します。

GHOST クラスのレコードはアクセス ルールを定義します。このアクセス ルールは、インターネットで通信する際に、ホストのグループに属する他の端末（ホスト）がローカル ホストに対して持つアクセス権限を管理します。各クライアント グループ（GHOST レコード）について、INETACL プロパティにクライアント グループに属しているホストに、ローカル ホストが提供するサービスを制御するサービス ルールのリストが表示されます。

GHOST クラスのレコードのキーは、GHOST レコードの名前です。GHOST クラスのレコードで変更できるプロパティについて以下に説明します。

変更可能なプロパティ

AUDIT

eTrust AC の監査ログに記録されるアクセス イベントのタイプです。有効な値は以下のとおりです。

- all - すべてのアクセス要求が監査されます。
- success - 許可されたすべてのアクセス要求が監査されます。
- failure - 拒否されたアクセス要求のみが監査されます。この値がデフォルト値です。
- none - アクセス要求の監査は行われません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで audit パラメータを使用します。

CALENDAR

eTrust AC のユーザ、グループ、およびリソース制限の Unicenter TNG カレンダ オブジェクトを表します。eTrust AC は、一定の間隔で Unicenter TNG のアクティブなカレンダを取得します。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで calendar パラメータと calendar- パラメータを使用します。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。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。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

DAYTIME

ユーザがリソースにアクセスできる日時を管理する、曜日と時刻の制限です。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで restrictions(days and time) パラメータを使用します。

GROUPS

リソース レコードが属する CONTAINER クラスのレコードのリストです。

GHOST クラスのレコードのこのプロパティを変更するには、該当する CONTAINER クラスのレコードの MEMBERS プロパティを変更する必要があります。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで mem+ か mem- パラメータを使用します。

INETACL

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ています。

- **サービス参照** - サービス(ポート番号またはサービス名)への参照。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。
- **許可されるアクセス** - サービスに対してクライアント ホストが持つ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、以下のとおりです。
  - read - ローカル ホストにホスト グループへのサービスの提供を許可します。
  - none - ローカル ホストにホスト グループへのサービスの提供を許可しません。

INETACL プロパティでアクセサおよびアクセス タイプを変更するには、authorize[-] コマンド の *access(type-of-access*) パラメータ、service パラメータ、および stationName パラメータを使用します。

INSERVRANGE

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、サービスの範囲を示します。

INSERVRANGE プロパティでアクセサおよびアクセス タイプを変更するには、authorize[-] コマンド の service(*serviceRange*) パラメータを使用します。

MEMBERS

HOST クラスにある、グループのメンバとなるオブジェクトのリストです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで mem+ か mem- パラメータを使用します。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

WARNING

警告モードを有効にするかどうかを示します。警告モードを有効にすると、すべてのアクセス要求が許可されます。アクセス要求がアクセス ルールに違反する場合は、レコードが監査ログに書き込まれます。

注: 警告モードの場合、eTrust Access Control では、リソース グループに対する警告メッセージは作成されません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで warning[-] パラメータを使用します。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

GSUDO クラス

GSUDO クラスの各レコードは、タスク委任、つまり DO（sesudo）によって、ユーザに実行が許可または禁止されるアクションのグループを定義します。各アクションの SUDO クラスのレコードを作成した後に、作成したレコードを GSUDO クラスのレコードに追加する必要があります。

各リソースに対して同じアクセス ルールを指定する代わりに、GSUDO を使用して、SUDO リソースのグループに対してアクセス ルールを定義します。次に、SUDO クラスのレコードを GSUDO クラスのレコードに明示的に連結してグループ化します。

GSUDO クラスのレコードのキーは、グループの名前です。GSUDO クラスのレコードで変更できるプロパティについて以下に説明します。

変更可能なプロパティ

ACL

リソースへのアクセスを許可されているアクセサ（ユーザおよびグループ）およびアクセス タイプのリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ（ユーザまたはグループ）への参照。eTrust AC に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク（*）を入力します。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。GSUDO クラスの有効なアクセス権限は、以下のとおりです。
  - execute - プログラムの実行をアクセサに許可します。
  - none - どの操作の実行もアクセサに許可しません。
  - ACL プロパティを変更するには、authorize コマンドで access(*authority*) パラメータ、または authorize- コマンドを使用します。

AUDIT

eTrust AC の監査ログに記録されるアクセス イベントのタイプです。有効な値は以下のとおりです。

- all - すべてのアクセス要求が監査されます。
- success - 許可されたすべてのアクセス要求が監査されます。
- failure - 拒否されたアクセス要求のみが監査されます。この値がデフォルト値です。
- none - アクセス要求の監査は行われません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで audit パラメータを使用します。

CALACL

カレンダ アクセス制御リストです。これは、Unicenter TNG カレンダ ステータスに基づいてリソースへのアクセスが許可されているアクセサ(ユーザおよびグループ)のリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **カレンダ参照** - Unicenter TNG のカレンダへの参照。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。GSUDO クラスの有効なアクセス権限は、以下のとおりです。
  - execute - プログラムの実行をアクセサに許可します。
  - none - どの操作の実行もアクセサに許可しません。

カレンダが有効な場合にのみアクセスが許可されます。その他の場合はすべてのアクセスが拒否されます。

ACL アクセスに基づいて、ユーザまたはグループにリソースへのアクセスを許可するには、authorize コマンドで calendar パラメータを使用します。

CALENDAR

eTrust AC のユーザ、グループ、およびリソース制限の Unicenter TNG カレンダ オブジェクトを表します。eTrust AC は、一定の間隔で Unicenter TNG のアクティブなカレンダを取得します。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで calendar パラメータと calendar- パラメータを使用します。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。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。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

GROUPS

リソース レコードが属する CONTAINER クラスのレコードのリストです。

GSUDO クラスのレコードのこのプロパティを変更するには、該当する CONTAINER クラスのレコードの MEMBERS プロパティを変更する必要があります。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで mem+ か mem- パラメータを使用します。

MEMBERS

SUDO クラスにある、グループのメンバとなるオブジェクトのリストです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで mem+ か mem- パラメータを使用します。

NACL

リソースへのアクセスが許可されないアクセサ(ユーザおよびグループ)と、許可されないアクセス タイプのリストです。NACL の各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを NACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されないアクセス** - アクセサが明示的にアクセスを許可されないリソースへのアクセスのタイプです。GSUDO クラスの有効なアクセス権限は、以下のとおりです。
  - execute- アクセサがプログラムを実行できないようにします。
  - none - すべての操作の実行をアクセサに許可します。

NACL プロパティを変更するには、authorize コマンドで deniedaccess(*accesstype*) パラメータ、または authorize- コマンドで deniedaccess- パラメータを使用します。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

WARNING

警告モードを有効にするかどうかを示します。警告モードを有効にすると、すべてのアクセス要求が許可されます。アクセス要求がアクセス ルールに違反する場合は、レコードが監査ログに書き込まれます。

注: 警告モードの場合、eTrust Access Control では、リソース グループに対する警告メッセージは作成されません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで warning[-] パラメータを使用します。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

GTERMINAL クラス

GTERMINAL クラスの各レコードは、端末のグループを定義します。各端末の TERMINAL クラスのレコードを作成した後に、作成したレコードを GTERMINAL クラスのレコードに追加する必要があります。次に、TERMINAL クラスのレコードを GTERMINAL クラスのレコードに明示的に連結してグループ化します。

端末グループは、アクセス ルールを定義する場合に役に立ちます。端末ごとに同じアクセス ルールを指定する代わりに、1 つのみのコマンドを使用して、端末グループに対してアクセス ルールを指定することができます。同様に、1 つのみのコマンドをユーザ グループに対して使用して、端末グループに対して 1 つのルールを適用することもできます。

GTERMINAL クラスのレコードのキーは、端末グループの名前です。GTERMINAL クラスのレコードで変更できるプロパティについて以下に説明します。

変更可能なプロパティ

ACL

リソースへのアクセスを許可されているアクセサ(ユーザおよびグループ)およびアクセス タイプのリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。GTERMINAL クラスの有効なアクセス権限は、以下のとおりです。
  - none - どの操作の実行もアクセサに許可しません。
  - read - グループ内の任意の端末からのログインをアクセサに許可します。
  - write - グループ内の任意の端末からの eTrust AC の管理をアクセサに許可します。

ACL プロパティを変更するには、authorize コマンドで access(*authority*) パラメータ、または authorize- コマンドを使用します。

AUDIT

eTrust AC の監査ログに記録されるアクセス イベントのタイプです。有効な値は以下のとおりです。

- all - すべてのアクセス要求が監査されます。
- success - 許可されたすべてのアクセス要求が監査されます。
- failure - 拒否されたアクセス要求のみが監査されます。この値がデフォルト値です。

- none - アクセス要求の監査は行われません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで audit パラメータを使用します。

CALACL

カレンダ アクセス制御リストです。これは、Unicenter TNG カレンダ ステータスに基づいてリソースへのアクセスが許可されているアクセサ(ユーザおよびグループ)のリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **カレンダ参照** - Unicenter TNG のカレンダへの参照。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。GTERMINAL クラスの有効なアクセス権限は、以下のとおりです。
  - none - どの操作の実行もアクセサに許可しません。
  - read - グループ内の任意の端末からのログインをアクセサに許可します。
  - write - グループ内の任意の端末からの eTrust AC の管理をアクセサに許可します。

カレンダが有効な場合にのみアクセスが許可されます。その他の場合はすべてのアクセスが拒否されます。

ACL アクセスに基づいて、ユーザまたはグループにリソースへのアクセスを許可するには、authorize コマンドで calendar パラメータを使用します。

CALENDAR

eTrust AC のユーザ、グループ、およびリソース制限の Unicenter TNG カレンダ オブジェクトを表します。eTrust AC は、一定の間隔で Unicenter TNG のアクティブなカレンダを取得します。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで calendar パラメータと calendar- パラメータを使用します。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。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。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

GROUPS

リソース レコードが属する CONTAINER クラスのレコードのリストです。

GTERMINAL クラスのレコードのこのプロパティを変更するには、該当する CONTAINER クラスのレコードの MEMBERS プロパティを変更する必要があります。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで mem+ か mem- パラメータを使用します。

MEMBERS

TERMINAL クラスにある、グループのメンバとなるオブジェクトのリストです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで mem+ か mem- パラメータを使用します。

NACL

リソースへのアクセスが許可されないアクセサ(ユーザおよびグループ)と、許可されないアクセス タイプのリストです。NACL の各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを NACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されないアクセス** - アクセサが明示的にアクセスを許可されないリソースへのアクセスのタイプです。GTERMINAL クラスの有効なアクセス権限は、以下のとおりです。
  - none - すべての操作の実行をアクセサに許可します。
  - read - アクセサがグループ内の任意の端末からログインできないようにします。
  - write - アクセサがグループ内の任意の端末から eTrust AC を管理できないようにします。

NACL プロパティを変更するには、authorize コマンドで deniedaccess(*accesstype*) パラメータ、または authorize- コマンドで deniedaccess- パラメータを使用します。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

WARNING

警告モードを有効にするかどうかを示します。警告モードを有効にすると、すべてのアクセス要求が許可されます。アクセス要求がアクセス ルールに違反する場合は、レコードが監査ログに書き込まれます。

注: 警告モードの場合、eTrust Access Control では、リソース グループに対する警告メッセージは作成されません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで warning[-] パラメータを使用します。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

HNODE クラス

HNODE クラスには、組織の Policy Model 階層に関する情報が含まれています。つまり、伝達ツリー構造（サブスクライバ、親 PMDB など）が含まれます。このクラスの各レコードは、このツリー内のノード（階層ノード）を表します。このクラス内のオブジェクトの名前は、エンドポイントの実際のホスト名（例： myHost.ca.com）または Policy Model ノードの PMDB 名（例： myPMD@myHost.ca.com）です。

このクラスは、さまざまな PMDB やエンドポイントからアップロードされ、DMS に格納される情報を管理するために使用されます。

変更可能なプロパティ

このレコードに含まれている以下のプロパティは、selang によって変更できます。

SUBSCRIBERS

伝達ツリー内のノードのサブスクライバのリストです。このプロパティを更新すると、PARENTS プロパティも自動的に HNODE オブジェクト名で更新されます。

SUBSCRIBER_STATUS

親ごとのノードのステータスです。プロパティの値は、以下のフィールドを持つ構造体です。

oidSubs

HNODE オブジェクトのオブジェクト ID です。SUBSCRIBERS プロパティの値と同じです。

status

以下のいずれかのステータスを表す値です。

- available
- unavailable
- sync
- unknown

stime

最後のステータスの更新時間。

POLICIES

このノードに展開されるポリシーのリストです。

POLICY_STATUS

POLICIES プロパティに表示される各ポリシーのステータスです。プロパティの値は、以下のフィールドを持つ構造体です。

oidPolicy

POLICY オブジェクトのオブジェクト ID です。POLICIES プロパティの値と同じです。

policy_status

以下のいずれかを表す整数です。

- Transferred
- Deployed
- Undeployed
- Deployed with Failures
- Signature Faillures
- Queued
- Undeployed with Failures
- Transfer Failures
- Unknown

deviation

このノードにポリシー偏差があるかどうかを表す値です。有効な値は以下のとおりです。

- Yes
- No
- Unset

dev_time

最後の偏差ステータスの更新時間。

ptime

最後のポリシー ステータスの更新時間。

updator

ポリシーを展開または削除したユーザの名前を示します。

変更できないプロパティ

このレコードに含まれている以下のプロパティは、eTrust AC によって自動的に変更されます。selang を使用して変更することはできません。

PARENTS

伝達ツリー内のノードの親である PMDB のリストです（parent_pmd レジストリ エントリでも定義されます）。

NODE_TYPE

以下のいずれかを表す値です。

- eAC
- TNG
- TSS
- RACF
- ACF

HOLIDAY クラス

HOLIDAY クラスの各レコードは、ログイン時に特別な許可が必要となる 1 つまたは複数の期間を定義します。

各ユーザには、レコード内のすべての期間について同じアクセス権限が設定されます。これは、複数の休日期間を 1 つの HOLIDAY クラスのレコードに格納した場合、ある期間中にユーザにログインを許可し、別の期間中にはログインを禁止するという処理はできないことを意味します。たとえば、特定のユーザが元日にはログインでき、クリスマスにはログインできないようにする場合、これら 2 つの休日は別々のレコードに定義する必要があります。

特定の年を指定しない場合、休日は 毎年適用されるとみなされます。

newusr コマンド、chusr コマンド、または editusr コマンドで IGN_HOL 属性を指定することによって、個々のユーザに対する HOLIDAY クラス制限を無効にできます。

HOLIDAY クラスのレコードのキーは、HOLIDAY クラスのレコードの名前です。HOLIDAY クラスのレコードで変更できるプロパティについて以下に説明します。

変更可能なプロパティ

ACL

リソースへのアクセスを許可されているアクセサ(ユーザおよびグループ)およびアクセス タイプのリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。HOLIDAY クラスの有効なアクセス権限は、以下のとおりです。
  - none - どの操作の実行もアクセサに許可しません。
  - read - レコードに指定されている休日期間中のログインをアクセサに許可します。

ACL プロパティを変更するには、authorize コマンドで access(*authority*) パラメータ、または authorize- コマンドを使用します。

AUDIT

eTrust AC の監査ログに記録されるアクセス イベントのタイプです。有効な値は以下のとおりです。

- all - すべてのアクセス要求が監査されます。
- success - 許可されたすべてのアクセス要求が監査されます。

- failure - 拒否されたアクセス要求のみが監査されます。この値がデフォルト値です。
- none - アクセス要求の監査は行われません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで audit パラメータを使用します。

CALACL

カレンダ アクセス制御リストです。これは、Unicenter TNG カレンダ ステータスに基づいてリソースへのアクセスが許可されているアクセサ(ユーザおよびグループ)のリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **カレンダ参照** - Unicenter TNG のカレンダへの参照。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。HOLIDAY クラスの有効なアクセス権限は、以下のとおりです。
  - none - どの操作の実行もアクセサに許可しません。
  - read - レコードに指定されている休日期間中のログインをアクセサに許可します。

カレンダが有効な場合にのみアクセスが許可されます。その他の場合はすべてのアクセスが拒否されます。

ACL アクセスに基づいて、ユーザまたはグループにリソースへのアクセスを許可するには、authorize コマンドで calendar パラメータを使用します。

CATEGORY

リソースに割り当てる 1 つまたは複数のセキュリティ カテゴリです。CATEGORY クラスに定義されている任意のセキュリティ カテゴリを指定できます。リソースに 1 つまたは複数のセキュリティ 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**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。

リソースのこのプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで category[-] パラメータを使用します。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。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。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

GROUPS

リソース レコードが属する CONTAINER クラスのレコードのリストです。

HOLIDAY クラスのレコードのこのプロパティを変更するには、該当する CONTAINER クラスのレコードの MEMBERS プロパティを変更する必要があります。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで mem+ か mem- パラメータを使用します。

HOL_DATE

ユーザがログインできない期間を示します。

HOL_DATE プロパティには、以下のルールが適用されます。

- 特定の年を指定しない場合、その期間または休日は毎年適用されるとみなされます。年は、99 または 1999 のように、2 桁または 4 桁で指定できます。
- 開始時間を指定しない場合、その日の開始時間(午前 0 時)が使用され、終了時間を指定しない場合、その日の終了時間(午前 0 時)が使用されます。
- 時間帯を指定せずに日付のみを指定した場合、その日 1 日が休日とみなされます。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで dates パラメータを使用します。

NACL

リソースへのアクセスが許可されないアクセサ(ユーザおよびグループ)と、許可されないアクセス タイプのリストです。NACL の各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを NACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されないアクセス** - アクセサが明示的にアクセスを許可されないリソースへのアクセスのタイプです。HOLIDAY クラスの有効なアクセス権限は、以下のとおりです。
  - none - すべての操作の実行をアクセサに許可します。
  - read - レコードに指定されている休日期間中にアクセサがログインできないようにします。

NACL プロパティを変更するには、authorize コマンドで deniedaccess(*accesstype*) パラメータ、または authorize- コマンドで deniedaccess- パラメータを使用します。

NOTIFY

リソースの監査イベントが生成された場合に通知を受け取るユーザです。selogrd を使用して指定の電子メール アドレスに送信できる特別な監査レコードを作成することもできます。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで notify[-] パラメータを使用します。

制限: 30 文字。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

SECLABEL

リソースのセキュリティ ラベルです。セキュリティ ラベルは、セキュリティ レベルをセキュリティ カテゴリに関連付けます。

適用する場合、セキュリティ ラベルは、レコードに設定された特定のセキュリティ レベルおよびセキュリティ カテゴリよりも優先されます。セキュリティ ラベルを割り当てることは、ラベルのレベルとカテゴリをユーザに明示的に割り当てることと同じです。指定されたセキュリティ ラベルは、SECLABEL クラスのレコードとして定義する必要があります。USER クラスのレコードにセキュリティ ラベルが設定されている場合は、以下の条件が両方とも満たされている場合にのみ、リソースへのアクセス権がユーザに与えられます。

- セキュリティ ラベルに指定されたユーザのセキュリティ レベルが、リソースのセキュリティ レベル以上であること。
- リソース レコードに指定されたすべてのセキュリティ カテゴリが、ユーザのセキュリティ ラベルのセキュリティ カテゴリ リストに含まれていること。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで label[-] パラメータを使用します。

SECLEVEL

ユーザまたはリソースのセキュリティ レベルです。セキュリティ レベルは 0 から 255 までの正の整数です。値 0 は、セキュリティ レベルを割り当てないことを意味します。リソースにセキュリティ レベルを割り当てた場合は、ユーザのセキュリティ レベルがリソースのセキュリティ レベル以上である場合にのみ、リソースへのアクセス権がユーザに与えられます。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで level[-] パラメータを使用します。

UACC

リソースに対するデフォルトのアクセス権です。eTrust Access Control に定義されていないアクセサ、またはリソースの ACL に登録されていないアクセサに与えるアクセス権を示します。有効な値については、リソースの ACL プロパティを参照してください。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで defaccess パラメータを使用します。

WARNING

警告モードを有効にするかどうかを示します。警告モードを有効にすると、すべてのアクセス要求が許可されます。アクセス要求がアクセス ルールに違反する場合は、レコードが監査ログに書き込まれます。

注: 警告モードの場合、eTrust Access Control では、リソース グループに対する警告メッセージは作成されません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで warning[-] パラメータを使用します。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

HOST クラス

HOST クラスの各レコードは、アクセス ルールを定義します。このアクセス ルールは、インターネットで通信する際に、他の端末(ホスト)のローカル ホストに対するアクセス権限を管理します。HOST クラスのレコードは、ローカル ホストのクライアントを表します。各クライアント(HOST レコード)について、INETACL プロパティに、ローカル ホストがクライアントに提供するサービスを制御するサービス ルールのリストが表示されます。

HOST クラスに追加する名前は、システムにホストとして定義されている必要があります。つまり、/etc/hosts ファイル(UNIX/Linux の場合)または ¥system32¥drivers¥etc¥hosts ファイル(Windows の場合)に指定されているか、NIS システムまたは DNS システムに定義されている必要があります。

サービスは、/etc/services ファイル(UNIX/Linux の場合)、¥system32¥drivers¥etc¥services ファイル(Windows の場合)、または他のサービス名解決方法を使用して、システムに定義する必要があります。サービスに許可を与える場合は、サービスの名前ではなく TCP/IP プロトコルのポート番号で指定できます。

また、eTrust AC では、/etc/rpc ファイル(UNIX/Linux の場合)または ¥etc¥rpc ファイル(Windows の場合)に指定された portmapper によって割り当てられる動的なポート名もサポートしています。

eTrust AC では、ホスト名に別名を使用できます。ただし、別名を表すレコードが権限チェックに使用されることはありません。別名の呼び出しでは、常に実際の名前(正規の名前)が使用されます。eTrust AC がインストールされたコンピュータとの接続を保護するには、IP アドレスの正確な名前がわかっている必要があります。

HOST クラスのレコードのキーは、ホストの名前です。HOST クラスのレコードで変更できるプロパティについて以下に説明します。

変更可能なプロパティ

AUDIT

eTrust AC の監査ログに記録されるアクセス イベントのタイプです。有効な値は以下のとおりです。

- all - すべてのアクセス要求が監査されます。
- success - 許可されたすべてのアクセス要求が監査されます。
- failure - 拒否されたアクセス要求のみが監査されます。この値がデフォルト値です。
- none - アクセス要求の監査は行われません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで audit パラメータを使用します。

CALENDAR

eTrust AC のユーザ、グループ、およびリソース制限の Unicenter TNG カレンダ オブジェクトを表します。eTrust AC は、一定の間隔で Unicenter TNG のアクティブなカレンダを取得します。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで calendar パラメータと calendar- パラメータを使用します。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。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。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

DAYTIME

ユーザがリソースにアクセスできる日時を管理する、曜日と時刻の制限です。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで restrictions(days and time) パラメータを使用します。

GROUPS

リソース レコードが属する GHOST クラスまたは CONTAINER クラスのレコードのリストです。

HOST クラスのレコードのこのプロパティを変更するには、該当する CONTAINER クラスまたは GHOST クラスのレコードの MEMBERS プロパティを変更する必要があります。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで mem+ か mem- パラメータを使用します。

INETACL

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ています。

- **サービス参照** - サービス(ポート番号またはサービス名)への参照。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。
- **許可されるアクセス** - サービスに対してクライアント ホストが持つ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、以下のとおりです。
  - read - ローカル ホストにホスト グループへのサービスの提供を許可します。
  - none - ローカル ホストにホスト グループへのサービスの提供を許可しません。

INETACL プロパティでアクセサおよびアクセス タイプを変更するには、authorize[-] コマンド の *access (type-of-access)* パラメータ、service パラメータ、および stationName パラメータを使用します。

INSERVRANGE

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、サービスの範囲を示します。

INSERVRANGE プロパティでアクセサおよびアクセス タイプを変更するには、authorize[-] コマンド の service(serviceRange) パラメータを使用します。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

WARNING

警告モードを有効にするかどうかを示します。警告モードを有効にすると、すべてのアクセス要求が許可されます。アクセス要求がアクセス ルールに違反する場合は、レコードが監査ログに書き込まれます。

注: 警告モードの場合、eTrust Access Control では、リソース グループに対する警告メッセージは作成されません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで warning[-] パラメータを使用します。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

HOSTNET クラス

HOSTNET クラスの各レコードは、特定のネットワーク上のすべてのホストで構成されたグループを定義します。HOSTNET クラスのレコードはアクセス ルールを定義します。このアクセス ルールは、インターネットで通信する場合に、特定のネットワーク上にある他の端末(ホスト)がローカル ホストに対して持つアクセス権を管理します。各 HOSTNET レコードの名前は、IP アドレスの mask 値と match 値で構成されます。各ホスト グループ(HOSTNET レコード)について、INETACL プロパティにはローカル ホストがグループ内のホストに提供するサービスを制御するサービス ルールのリストが表示されます。

HOSTNET クラスのレコードのキーは、HOSTNET レコードの名前です。HOSTNET クラスのレコードで変更できるプロパティの一覧とその説明を以下に示します。

変更可能なプロパティ

AUDIT

eTrust AC の監査ログに記録されるアクセス イベントのタイプです。有効な値は以下のとおりです。

- all - すべてのアクセス要求が監査されます。
- success - 許可されたすべてのアクセス要求が監査されます。
- failure - 拒否されたアクセス要求のみが監査されます。この値がデフォルト値です。
- none - アクセス要求の監査は行われません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで audit パラメータを使用します。

CALENDAR

eTrust AC のユーザ、グループ、およびリソース制限の Unicenter TNG カレンダ オブジェクトを表します。eTrust AC は、一定の間隔で Unicenter TNG のアクティブなカレンダを取得します。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで calendar パラメータと calendar- パラメータを使用します。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。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。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

DAYTIME

ユーザがリソースにアクセスできる日時を管理する、曜日と時刻の制限です。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで restrictions(days and time) パラメータを使用します。

GROUPS

リソース レコードが属する CONTAINER クラスのレコードのリストです。

HOSTNET クラスのレコードのこのプロパティを変更するには、該当する CONTAINER クラスのレコードの MEMBERS プロパティを変更する必要があります。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで mem+ か mem- パラメータを使用します。

INETACL

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ています。

- **サービス参照** - サービス(ポート番号またはサービス名)への参照。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。
- **許可されるアクセス** - サービスに対してクライアント ホストが持つ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、以下のとおりです。
  - read - ローカル ホストにホスト グループへのサービスの提供を許可します。
  - none - ローカル ホストにホスト グループへのサービスの提供を許可しません。

INETACL プロパティでアクセサおよびアクセス タイプを変更するには、authorize[-] コマンド の *access(type-of-access*) パラメータ、service パラメータ、および stationName パラメータを使用します。

INSERVRANGE

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、サービスの範囲を示します。

INSERVRANGE プロパティでアクセサおよびアクセス タイプを変更するには、authorize[-] コマンド の service(serviceRange) パラメータを使用します。

INMASKMATCH

ネットワークを識別する mask および match の値です。mask と match の値は要求元ホストの IP アドレスに適用され、そのホストがネットワークに属しているかどうかが判断されます。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで mask パラメータおよび match パラメータを使用します。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

WARNING

警告モードを有効にするかどうかを示します。警告モードを有効にすると、すべてのアクセス要求が許可されます。アクセス要求がアクセス ルールに違反する場合は、レコードが監査ログに書き込まれます。

注: 警告モードの場合、eTrust Access Control では、リソース グループに対する警告メッセージは作成されません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで warning[-] パラメータを使用します。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

HOSTNP クラス

HOSTNP クラスの各レコードは、類似した名前を持つホストのグループを定義します。HOSTNP レコードはアクセス ルールを定義します。このアクセス ルールは、インターネットで通信する際に、レコードの名前パターンに一致する他の端末(ホスト)のローカル ホストに対するアクセス権を管理します。INETACL プロパティは、各マスク(HOSTNP レコード)のサービス ルールを一覧表示します。このサービス ルールは、ローカル ホストからホストグループに提供されるサービスを管理します。

HOSTNP クラスのレコードのキーは、HOSTNP レコードによって保護されるホストのホスト名をフィルタ処理するために使用される名前パターンです。HOSTNP クラスのレコードで変更できるプロパティについて以下に説明します。

変更可能なプロパティ

AUDIT

eTrust AC の監査ログに記録されるアクセス イベントのタイプです。有効な値は以下のとおりです。

- all - すべてのアクセス要求が監査されます。
- success - 許可されたすべてのアクセス要求が監査されます。
- failure - 拒否されたアクセス要求のみが監査されます。この値がデフォルト値です。
- none - アクセス要求の監査は行われません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで audit パラメータを使用します。

CALENDAR

eTrust AC のユーザ、グループ、およびリソース制限の Unicenter TNG カレンダ オブジェクトを表します。eTrust AC は、一定の間隔で Unicenter TNG のアクティブなカレンダを取得します。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで calendar パラメータと calendar- パラメータを使用します。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。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。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

DAYTIME

ユーザがリソースにアクセスできる日時を管理する、曜日と時刻の制限です。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで restrictions(days and time) パラメータを使用します。

GROUPS

リソース レコードが属する CONTAINER クラスのレコードのリストです。

HOSTNP クラスのレコードのこのプロパティを変更するには、該当する CONTAINER クラスのレコードの MEMBERS プロパティを変更する必要があります。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで mem+ か mem- パラメータを使用します。

INETACL

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ています。

- **サービス参照** - サービス(ポート番号またはサービス名)への参照。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。
- **許可されるアクセス** - サービスに対してクライアント ホストが持つ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、以下のとおりです。
  - read - ローカル ホストにホスト グループへのサービスの提供を許可します。
  - none - ローカル ホストにホスト グループへのサービスの提供を許可しません。

INETACL プロパティでアクセサおよびアクセス タイプを変更するには、authorize[-] コマンド の *access (type-of-access)* パラメータ、service パラメータ、および stationName パラメータを使用します。

INSERVRANGE

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、サービスの範囲を示します。

INSERVRANGE プロパティでアクセサおよびアクセス タイプを変更するには、authorize[-] コマンド の service(serviceRange) パラメータを使用します。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

WARNING

警告モードを有効にするかどうかを示します。警告モードを有効にすると、すべてのアクセス要求が許可されます。アクセス要求がアクセス ルールに違反する場合は、レコードが監査ログに書き込まれます。

注: 警告モードの場合、eTrust Access Control では、リソース グループに対する警告メッセージは作成されません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで warning[-] パラメータを使用します。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

MFTERMINAL クラス

MFTERMINAL クラスの各レコードは、eTrust AC の管理に使用されるメインフレーム コンピュータを定義します。MFTERMINAL クラスは、TERMINAL クラスと特性は同じですが、eTrust AC によってインターセプトされません。

MFTERMINAL クラスのレコードのキーは、メインフレーム コンピュータの名前です。MFTERMINAL クラスのレコードで変更できるプロパティについて以下に説明します。

変更可能なプロパティ

ACL

リソースへのアクセスを許可されているアクセサ(ユーザおよびグループ)およびアクセス タイプのリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。MFTERMINAL クラスの有効なアクセス権限は、以下のとおりです。
  - none - どの操作の実行もアクセサに許可しません。
  - read - メインフレーム端末からのログインをアクセサに許可します。
  - write - メインフレーム端末からの eTrust AC の管理をアクセサに許可します。

ACL プロパティを変更するには、authorize コマンドで access(*authority*) パラメータ、または authorize- コマンドを使用します。

AUDIT

eTrust AC の監査ログに記録されるアクセス イベントのタイプです。有効な値は以下のとおりです。

- all - すべてのアクセス要求が監査されます。
- success - 許可されたすべてのアクセス要求が監査されます。
- failure - 拒否されたアクセス要求のみが監査されます。この値がデフォルト値です。
- none - アクセス要求の監査は行われません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで audit パラメータを使用します。

CALACL

カレンダ アクセス制御リストです。これは、Unicenter TNG カレンダ ステータスに基づいてリソースへのアクセスが許可されているアクセサ(ユーザおよびグループ)のリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **カレンダ参照** - Unicenter TNG のカレンダへの参照。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。MFTERMINAL クラスの有効なアクセス権限は、以下のとおりです。
  - none - どの操作の実行もアクセサに許可しません。
  - read - メインフレーム端末からのログインをアクセサに許可します。
  - write - メインフレーム端末からの eTrust AC の管理をアクセサに許可します。

カレンダが有効な場合にのみアクセスが許可されます。その他の場合はすべてのアクセスが拒否されます。

ACL アクセスに基づいて、ユーザまたはグループにリソースへのアクセスを許可するには、authorize コマンドで calendar パラメータを使用します。

CALENDAR

eTrust AC のユーザ、グループ、およびリソース制限の Unicenter TNG カレンダ オブジェクトを表します。eTrust AC は、一定の間隔で Unicenter TNG のアクティブなカレンダを取得します。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで calendar パラメータと calendar- パラメータを使用します。

CATEGORY

リソースに割り当てる 1 つまたは複数のセキュリティ カテゴリです。CATEGORY クラスに定義されている任意のセキュリティ カテゴリを指定できます。リソースに 1 つまたは複数のセキュリティ 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**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。

リソースのこのプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで category[-] パラメータを使用します。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。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。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

DAYTIME

ユーザがリソースにアクセスできる日時を管理する、曜日と時刻の制限です。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで restrictions(days and time) パラメータを使用します。

GROUPS

リソース レコードが属する CONTAINER クラスのレコードのリストです。

MFTERMINAL クラスのレコードのこのプロパティを変更するには、該当する CONTAINER クラスのレコードの MEMBERS プロパティを変更する必要があります。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで mem+ か mem- パラメータを使用します。

NACL

リソースへのアクセスが許可されないアクセサ(ユーザおよびグループ)と、許可されないアクセス タイプのリストです。NACL の各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust AC に定義されているすべてのユーザを NACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されないアクセス** - アクセサが明示的にアクセスを許可されないリソースへのアクセスのタイプです。MFTERMINAL クラスの有効なアクセス権限は、以下のとおりです。
  - none - すべての操作の実行をアクセサに許可します。
  - read - アクセサがメインフレーム端末からログインできないようにします。
  - write - アクセサがメインフレーム端末から eTrust AC を管理できないようにします。

NACL プロパティを変更するには、authorize コマンドで deniedaccess(*accesstype*) パラメータ、または authorize- コマンドで deniedaccess- パラメータを使用します。

NOTIFY

リソースの監査イベントが生成された場合に通知を受け取るユーザです。selogrd を使用して指定の電子メール アドレスに送信できる特別な監査レコードを作成することもできます。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで notify[-] パラメータを使用します。

制限: 30 文字。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

PACL

プログラム アクセス制御リストです。特定のプログラムから、またはプログラム名のパターンに一致するプログラムからアクセス要求が行われた場合に、アクセサに適用される ACL です。

パターンを指定すると、PACL によって保護されているリソースは、指定したパターンに一致するプログラムを使用しないとアクセスできません。プログラムが複数のパターンと一致する場合は、文字数が最も多いパターンが優先されます。

プログラム アクセス制御リストの各要素には、以下の情報が含まれています。

- **プログラム参照** - 指定または名前パターン一致による PROGRAM クラスのレコードへの参照。
- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。
- **許可されたアクセス** - 指定されたプログラムを使用している場合にアクセサに許可されるアクセス権。有効な値については、ACL プロパティを参照してください。

ACL プロパティにプログラム、アクセサ、およびアクセス タイプを追加するには、authorize コマンドで via(pgm) パラメータを使用します。ACL プロパティからこれらを削除するには、authorize- コマンドで via(pgm) パラメータを使用します。

SECLABEL

リソースのセキュリティ ラベルです。セキュリティ ラベルは、セキュリティ レベルをセキュリティ カテゴリに関連付けます。

適用する場合、セキュリティ ラベルは、レコードに設定された特定のセキュリティ レベルおよびセキュリティ カテゴリよりも優先されます。セキュリティ ラベルを割り当てることは、ラベルのレベルとカテゴリをユーザに明示的に割り当てることと同じです。指定されたセキュリティ ラベルは、SECLABEL クラスのレコードとして定義する必要があります。USER クラスのレコードにセキュリティ ラベルが設定されている場合は、以下の条件が両方とも満たされている場合にのみ、リソースへのアクセス権がユーザに与えられます。

- セキュリティ ラベルに指定されたユーザのセキュリティ レベルが、リソースのセキュリティ レベル以上であること。
- リソース レコードに指定されたすべてのセキュリティ カテゴリが、ユーザのセキュリティ ラベルのセキュリティ カテゴリ リストに含まれていること。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで label[-] パラメータを使用します。

SECLEVEL

ユーザまたはリソースのセキュリティ レベルです。セキュリティ レベルは 0 から 255 までの正の整数です。値 0 は、セキュリティ レベルを割り当てないことを意味します。リソースにセキュリティ レベルを割り当てた場合は、ユーザのセキュリティ レベルがリソースのセキュリティ レベル以上である場合にのみ、リソースへのアクセス権がユーザに与えられます。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで level[-] パラメータを使用します。

UACC

リソースに対するデフォルトのアクセス権です。eTrust Access Control に定義されていないアクセサ、またはリソースの ACL に登録されていないアクセサに与えるアクセス権を示します。有効な値については、リソースの ACL プロパティを参照してください。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで defaccess パラメータを使用します。

WARNING

警告モードを有効にするかどうかを示します。警告モードを有効にすると、すべてのアクセス要求が許可されます。アクセス要求がアクセス ルールに違反する場合は、レコードが監査ログに書き込まれます。

注: 警告モードの場合、eTrust Access Control では、リソース グループに対する警告メッセージは作成されません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで warning[-] パラメータを使用します。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

POLICY クラス

POLICY クラスの各レコードは、ポリシーの展開および展開解除に必要な情報を定義します。これらのレコードには、ポリシーを展開および展開解除するための selang コマンドのリストを含む RULESET オブジェクトへのリンクが含まれます。ポリシーの展開では、selang コマンドの deploy を実行します。このコマンドではリンクされている RULESET オブジェクトにあるコマンドを全て実行します。ポリシーの展開解除では、selang コマンドの deploy- を実行します。このコマンドは、リンクされている RULESET コマンドに格納されている再定義のコマンドを全て実行します。

変更可能なプロパティ

レコードに含まれている以下のプロパティは、selang によって変更できます。

RULESETS

ポリシーを定義する RULESET オブジェクトのリストです。

SIGNATURE

ポリシーに関連付けられた RULESET オブジェクトのシグネチャに基づくハッシュ値です。

変更できないプロパティ

レコードに含まれている以下のプロパティは、eTrust Access Control によって自動的に変更されます。selang を使用して変更することはできません。

HNODE

このポリシーが展開される eTrust AC ノードのリストです。

PROCESS クラス

PROCESS クラスの各レコードは、プログラム（実行可能ファイル）を定義します。それぞれ独自のアドレス空間で実行されるプログラムは、（kill コマンドによって）強制終了されないように保護する必要があります。特に、主要なユーティリティやデータベース サーバは、そのプロセスがサービス妨害（DoS）攻撃の主な標的になりやすいため、保護することをお勧めします。

注: PROCESS クラスにプログラムを定義する場合、FILE クラスにもプログラムを定義する必要があります。こうすると、許可なしに実行可能ファイルを変更（置換または破損）できなくなるため、実行可能ファイルを保護できます。

eTrust AC は、通常の終了シグナル（SIGTERM）と、アプリケーションがマスクできない 2 つのシグナル（SIGKILL および SIGSTOP）の 3 つの終了シグナル（kill）からプロセスを保護します。

環境	シグナル	数値
Windows	KILL	Win32 API
UNIX/Linux	Terminate Process	9
UNIX/Linux および Windows	STOP	コンピュータによって異なる。
UNIX/Linux および Windows	TERM	15

SIGHUP や SIGUSR1 などのその他のシグナルは、ターゲットとなるプロセスに渡されます。そのプロセスでは、終了シグナルを無視するかどうか、あるいは何らかの方法でそのシグナルに対処するかどうかを決定します。

PROCESS クラスのレコードのキーは、レコードが保護するプログラムの名前です。完全パスを指定します。PROCESS クラスのレコードで変更できるプロパティについて以下に説明します。

変更可能なプロパティ

ACL

リソースへのアクセスを許可されているアクセサ(ユーザおよびグループ)およびアクセス タイプのリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust Access Control に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。PROCESS クラスの有効なアクセス権限は、以下のとおりです。
  - none - どの操作の実行もアクセサに許可しません。
  - read - プロセスの強制終了(kill)をアクセサに許可します。

ACL プロパティを変更するには、authorize コマンドまたは authorize- コマンドで access(*authority*) パラメータを使用します。

AUDIT

eTrust Access Control の監査ログに記録されるアクセス イベントのタイプです。有効な値は以下のとおりです。

- all - すべてのアクセス要求が監査されます。
- success - 許可されたすべてのアクセス要求が監査されます。
- failure - 拒否されたアクセス要求のみが監査されます。この値がデフォルト値です。
- none - アクセス要求の監査は行われません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで audit パラメータを使用します。

CALACL

カレンダ アクセス制御リストです。これは、Unicenter TNG カレンダ ステータスに基づいてリソースへのアクセスが許可されているアクセサ(ユーザおよびグループ)のリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust Access Control に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **カレンダ参照** - Unicenter TNG のカレンダへの参照。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。PROCESS クラスの有効なアクセス権限は、以下のとおりです。
  - none - どの操作の実行もアクセサに許可しません。
  - read - プロセスの強制終了(kill)をアクセサに許可します。

カレンダが有効な場合にのみアクセスが許可されます。その他の場合はすべてのアクセスが拒否されます。

ACL アクセスに基づいて、ユーザまたはグループにリソースへのアクセスを許可するには、authorize コマンドで calendar パラメータを使用します。

CALENDAR

eTrust Access Control のユーザ、グループ、およびリソース制限の Unicenter TNG カレンダ オブジェクトを表します。eTrust Access Control は、一定の間隔で Unicenter TNG のアクティブなカレンダを取得します。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで calendar パラメータと calendar- パラメータを使用します。

CATEGORY

リソースに割り当てる 1 つまたは複数のセキュリティ カテゴリです。CATEGORY クラスに定義されている任意のセキュリティ カテゴリを指定できます。リソースに 1 つまたは複数のセキュリティ 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**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。

リソースのこのプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで category[-] パラメータを使用します。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。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。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

DAYTIME

ユーザがリソースにアクセスできる日時を管理する、日付と時刻の制限です。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで restrictions(days and time) パラメータを使用します。

GROUPS

リソース レコードが属する CONTAINER クラスのレコードのリストです。

PROCESS クラスのレコードのこのプロパティを変更するには、該当する CONTAINER クラスのレコードの MEMBERS プロパティを変更する必要があります。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで mem+ パラメータか mem- パラメータを使用します。

NACL

リソースへのアクセスが許可されないアクセサ(ユーザおよびグループ)と、許可されないアクセス タイプのリストです。NACL の各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust Access Control に定義されているすべてのユーザを NACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されないアクセス** - アクセサが明示的にアクセスを許可されないリソースへのアクセスのタイプです。PROCESS クラスの有効なアクセス権限は、以下のとおりです。
  - none - すべての操作の実行をアクセサに許可します。
  - read - アクセサがプロセスを強制終了(kill)できないようにします。

NACL プロパティを変更するには、authorize コマンドで deniedaccess(*accesstype*) パラメータ、または authorize- コマンドで deniedaccess- パラメータを使用します。

NOTIFY

リソースの監査イベントが生成された場合に通知を受け取るユーザです。selogrd を使用して指定の電子メール アドレスに送信できる特別な監査レコードを作成することもできます。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで notify[-] パラメータを使用します。

制限: 30 文字。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

PACL

プログラム アクセス制御リストです。特定のプログラムから、またはプログラム名のパターンに一致するプログラムからアクセス要求が行われた場合に、アクセサに適用される ACL です。

パターンを指定すると、PACL によって保護されているリソースは、指定したパターンに一致するプログラムを使用しないとアクセスできません。プログラムが複数のパターンと一致する場合は、文字数が最も多いパターンが優先されます。

プログラム アクセス制御リストの各要素には、以下の情報が含まれています。

- **プログラム参照** - 指定または名前パターン一致による PROGRAM クラスのレコードへの参照。
- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。
- **許可されたアクセス** - 指定されたプログラムを使用している場合にアクセサに許可されるアクセス権。有効な値については、ACL プロパティを参照してください。

ACL プロパティにプログラム、アクセサ、およびアクセス タイプを追加するには、authorize コマンドで via(pgm) パラメータを使用します。ACL プロパティからこれらを削除するには、authorize- コマンドで via(pgm) パラメータを使用します。

SECLABEL

リソースのセキュリティ ラベルです。セキュリティ ラベルは、セキュリティ レベルをセキュリティ カテゴリに関連付けます。

適用する場合、セキュリティ ラベルは、レコードに設定された特定のセキュリティ レベルおよびセキュリティ カテゴリよりも優先されます。セキュリティ ラベルを割り当てることは、ラベルのレベルとカテゴリをユーザに明示的に割り当てることと同じです。指定されたセキュリティ ラベルは、SECLABEL クラスのレコードとして定義する必要があります。USER クラスのレコードにセキュリティ ラベルが設定されている場合は、以下の条件が両方とも満たされている場合にのみ、リソースへのアクセス権がユーザに与えられます。

- セキュリティ ラベルに指定されたユーザのセキュリティ レベルが、リソースのセキュリティ レベル以上であること。
- リソース レコードに指定されたすべてのセキュリティ カテゴリが、ユーザのセキュリティ ラベルのセキュリティ カテゴリ リストに含まれていること。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで label[-] パラメータを使用します。

SECLEVEL

ユーザまたはリソースのセキュリティ レベルです。セキュリティ レベルは 0 から 255 までの正の整数です。値 0 は、セキュリティ レベルを割り当てないことを意味します。リソースにセキュリティ レベルを割り当てた場合は、ユーザのセキュリティ レベルがリソースのセキュリティ レベル以上である場合にのみ、リソースへのアクセス権がユーザに与えられます。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで level[-] パラメータを使用します。

UACC

リソースに対するデフォルトのアクセス権です。eTrust Access Control に定義されていないアクセサ、またはリソースの ACL に登録されていないアクセサに与えるアクセス権を示します。有効な値については、リソースの ACL プロパティを参照してください。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで defaccess パラメータを使用します。

WARNING

警告モードを有効にするかどうかを示します。警告モードを有効にすると、すべてのアクセス要求が許可されます。アクセス要求がアクセス ルールに違反する場合は、レコードが監査ログに書き込まれます。

注: 警告モードの場合、eTrust Access Control では、リソース グループに対する警告メッセージは作成されません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで warning[-] パラメータを使用します。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

PROGRAM クラス

PROGRAM クラスの各レコードは、trusted computing base の一部とみなされるプログラムを定義します。このクラスに属するプログラムは、変更されたかどうかが Watchdog 機能によって監視されるため、セキュリティ違反がないものとして信頼できます。trusted プログラムが変更されると、変更されたプログラムは eTrust AC によって自動的に untrusted のマークが付けられ、実行できなくなります。オプションで、BLOCKRUN プロパティを使用して、untrusted プログラムの実行を許可または阻止することができます。

各 PROGRAM レコードには、trusted プログラム ファイルに関する情報を定義するいくつかのプロパティが含まれています。

注:

- また、最新のアクセサ情報(ACCSTIME プロパティや ACCSWHO プロパティ)をトレースするためには、trusted である実行可能ファイルのレコードを FILE クラスに作成する必要があります。eTrust AC の権限チェックは、最初に FILE クラスについて行われます。PROGRAM クラスの権限チェックは、常にその後に行われます。
- プログラムは、PROGRAM クラスに定義されていない限り、プログラム アクセス制御リスト(PACL)で使用できません(ただし、プログラムを PACL に追加すると、プログラムは自動的に PROGRAM クラスに追加されます)。
- ディレクトリは PROGRAM クラスに定義できません。

PROGRAM クラスのレコードのキーは、レコードが保護するプログラムのファイル名です。オブジェクト 名として、ファイルの完全パスを指定する必要があります。PROGRAM クラスのレコードで変更できるプロパティについて以下に説明します。

変更可能なプロパティ

ACL

リソースへのアクセスを許可されているアクセサ(ユーザおよびグループ)およびアクセス タイプのリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust Access Control に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。PROGRAM クラスの有効なアクセス権限は、以下のとおりです。
  - execute - プログラムの実行をアクセサに許可します。
  - none - どの操作の実行もアクセサに許可しません。

ACL プロパティを変更するには、authorize コマンドまたは authorize- コマンドで access(*authority*) パラメータを使用します。

注: PROGRAM クラスでは、ACL は「ファイル」リソースでのみ使用できます。ACL では最初にファイル リソース レコードがチェックされ、アクセスが許可される場合は、プログラム リソース レコードがチェックされます。

AUDIT

eTrust Access Control の監査ログに記録されるアクセス イベントのタイプです。有効な値は以下のとおりです。

- all - すべてのアクセス要求が監査されます。
- success - 許可されたすべてのアクセス要求が監査されます。
- failure - 拒否されたアクセス要求のみが監査されます。この値がデフォルト値です。
- none - アクセス要求の監査は行われません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで audit パラメータを使用します。

BLOCKRUN

Trusted プログラムであるかどうかのチェックを行うかどうかと、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係なく、実行がブロックされます。

以下に使用例を示します。

```
newres program c:¥windows¥system32¥notepad.exe defaccess(x) owner(nobody) blockrun
```

リソースのこのプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで blockrun[-] パラメータを使用します。

CALACL

カレンダ アクセス制御リストです。これは、Unicenter TNG カレンダ ステータスに基づいてリソースへのアクセスが許可されているアクセサ(ユーザおよびグループ)のリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust Access Control に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **カレンダ参照** - Unicenter TNG のカレンダへの参照。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。PROGRAM クラスの有効なアクセス権限は、以下のとおりです。
  - execute - プログラムの実行をアクセサに許可します。
  - none - どの操作の実行もアクセサに許可しません。

カレンダが有効な場合にのみアクセスが許可されます。その他の場合はすべてのアクセスが拒否されます。

ACL アクセスに基づいて、ユーザまたはグループにリソースへのアクセスを許可するには、authorize コマンドで calendar パラメータを使用します。

CALENDAR

eTrust Access Control のユーザ、グループ、およびリソース制限の Unicenter TNG カレンダ オブジェクトを表します。eTrust Access Control は、一定の間隔で Unicenter TNG のアクティブなカレンダを取得します。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで calendar パラメータと calendar- パラメータを使用します。

CATEGORY

リソースに割り当てる 1 つまたは複数のセキュリティ カテゴリです。CATEGORY クラスに定義されている任意のセキュリティ カテゴリを指定できます。リソースに 1 つまたは複数のセキュリティ 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**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。

リソースのこのプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで category[-] パラメータを使用します。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。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。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

DAYTIME

ユーザがリソースにアクセスできる日時を管理する、曜日と時刻の制限です。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで restrictions(days and time) パラメータを使用します。

GROUPS

リソース レコードが属する CONTAINER クラスのレコードのリストです。

PROGRAM クラスのレコードのこのプロパティを変更するには、該当する CONTAINER クラスのレコードの MEMBERS プロパティを変更する必要があります。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで mem+ パラメータか mem- パラメータを使用します。

NACL

リソースへのアクセスが許可されないアクセサ(ユーザおよびグループ)と、許可されないアクセス タイプのリストです。NACL の各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust Access Control に定義されているすべてのユーザを NACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されないアクセス** - アクセサが明示的にアクセスを許可されないリソースへのアクセスのタイプです。PROGRAM クラスの有効なアクセス権限は、以下のとおりです。
  - execute - アクセサがプログラムを実行できないようにします。
  - none - すべての操作の実行をアクセサに許可します。

NACL プロパティを変更するには、authorize コマンドで deniedaccess(*accesstype*) パラメータ、または authorize- コマンドで deniedaccess- パラメータを使用します。

NOTIFY

リソースの監査イベントが生成された場合に通知を受け取るユーザです。selogrd を使用して指定の電子メール アドレスに送信できる特別な監査レコードを作成することもできます。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで notify[-] パラメータを使用します。

制限: 30 文字。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

PACL

プログラム アクセス制御リストです。特定のプログラムから、またはプログラム名のパターンに一致するプログラムからアクセス要求が行われた場合に、アクセサに適用される ACL です。

パターンを指定すると、PACL によって保護されているリソースは、指定したパターンに一致するプログラムを使用しないとアクセスできません。プログラムが複数のパターンと一致する場合は、文字数が最も多いパターンが優先されます。

プログラム アクセス制御リストの各要素には、以下の情報が含まれています。

- **プログラム参照** - 指定または名前パターン一致による PROGRAM クラスのレコードへの参照。
- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。

- **許可されたアクセス** - 指定されたプログラムを使用している場合にアクセサに許可されるアクセス権。有効な値については、ACL プロパティを参照してください。

ACL プロパティにプログラム、アクセサ、およびアクセス タイプを追加するには、authorize コマンドで via(pgm) パラメータを使用します。ACL プロパティからこれらを削除するには、authorize- コマンドで via(pgm) パラメータを使用します。

注: PROGRAM クラスでは、PACL は「ファイル」リソースでのみ使用できます。ACL では最初にファイル リソース レコードがチェックされ、アクセスが許可される場合は、プログラム リソース レコードがチェックされます。

PGMINFO

eTrust Access Control で自動的に生成されるプログラムの情報です。

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 eTrust Access Control により Untrusted として定義されます。

以下のフラグを選択すると、この検証プロセスから関連情報を**除外**できます。

- crc - CRC（巡回冗長検査）および MD5 シグネチャ
- device - （UNIX/Linux のみ）ファイルが置かれている論理ディスク
- group - （UNIX/Linux のみ）プログラム ファイルを所有する UNIX/Linux グループ
- inode - （UNIX/Linux のみ）プログラム ファイルのファイル システム アドレス
- mode - （UNIX/Linux のみ）プログラム ファイルの UNIX/Linux セキュリティ モード（許可）
- mtime - プログラム ファイルが最後に変更された時刻
- owner - （UNIX/Linux のみ）プログラム ファイルを所有する UNIX/Linux ユーザ
- sha1 - SHA1 シグネチャ。SHA（Secure Hash Algorithm）と呼ばれるデジタル シグネチャ方法で、プログラムまたは機密ファイルに適用することができます。
- size - プログラム ファイルのサイズ

このプロパティのフラグを変更するには、chres コマンド、editres コマンド、または newres コマンドで flags パラメータ、flags+ パラメータ、または flags- パラメータを使用します。

SECLABEL

リソースのセキュリティ ラベルです。セキュリティ ラベルは、セキュリティ レベルをセキュリティ カテゴリに関連付けます。

適用する場合、セキュリティ ラベルは、レコードに設定された特定のセキュリティ レベルおよびセキュリティ カテゴリよりも優先されます。セキュリティ ラベルを割り当てることは、ラベルのレベルとカテゴリをユーザに明示的に割り当てることと同じです。指定されたセキュリティ ラベルは、SECLABEL クラスのレコードとして定義する必要があります。USER クラスのレコードにセキュリティ ラベルが設定されている場合は、以下の条件が両方とも満たされている場合にのみ、リソースへのアクセス権がユーザに与えられます。

- セキュリティ ラベルに指定されたユーザのセキュリティ レベルが、リソースのセキュリティ レベル以上であること。
- リソース レコードに指定されたすべてのセキュリティ カテゴリが、ユーザのセキュリティ ラベルのセキュリティ カテゴリ リストに含まれていること。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで label[-] パラメータを使用します。

SECLEVEL

ユーザまたはリソースのセキュリティ レベルです。セキュリティ レベルは 0 から 255 までの正の整数です。値 0 は、セキュリティ レベルを割り当てないことを意味します。リソースにセキュリティ レベルを割り当てた場合は、ユーザのセキュリティ レベルがリソースのセキュリティ レベル以上である場合にのみ、リソースへのアクセス権がユーザに与えられます。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで level[-] パラメータを使用します。

UACC

リソースに対するデフォルトのアクセス権です。eTrust Access Control に定義されていないアクセサ、またはリソースの ACL に登録されていないアクセサに与えるアクセス権を示します。有効な値については、リソースの ACL プロパティを参照してください。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで defaccess パラメータを使用します。

UNTRUST

プログラムが trusted かどうかを示します。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他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、eTrust AC によって UNTRUST プロパティが自動的に設定されます。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで trust[-] パラメータを使用します。

WARNING

警告モードを有効にするかどうかを示します。警告モードを有効にすると、すべてのアクセス要求が許可されます。アクセス要求がアクセス ルールに違反する場合は、レコードが監査ログに書き込まれます。

注: 警告モードの場合、eTrust Access Control では、リソース グループに対する警告メッセージは作成されません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで warning[-] パラメータを使用します。

変更できないプロパティ

ACCSTIME

レコードが最後にアクセスされた日時です。

ACCSWHO

レコードに最後にアクセスした管理者です。

CREATE_TIME

レコードが作成された日時です。

MD5

ファイルの RSA-MD5 シグネチャです。

UNTRUSTREASON

プログラムが untrusted になった理由です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

PWPOLICY クラス

PWPOLICY クラスの各レコードは、パスワード ポリシーを定義します。パスワード ポリシーは、新しいパスワードの妥当性とパスワードの有効期間の両方に関する一連のルールです。

PWPOLICY クラスのキーは、パスワード ポリシーの名前です。PWPOLICY クラスのレコードで変更できるプロパティについて以下に説明します。

変更可能なプロパティ

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。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。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

GROUPS

リソース レコードが属する CONTAINER クラスのレコードのリストです。

PWPOLICY クラスのレコードのこのプロパティを変更するには、該当する CONTAINER クラスのレコードの MEMBERS プロパティを変更する必要があります。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで mem+ パラメータか mem- パラメータを使用します。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

PASSWDRULES

パスワード ルールを示します。このプロパティには、eTrust 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。

このプロパティを変更するには、setoptions コマンドで password パラメータおよび rules オプションまたは rules- オプションを使用します。

変更できないプロパティ

APPLS

パスワード ポリシーにリンクされている eTrust Web Access Control アプリケーションのリストです。

CREATE_TIME

レコードが作成された日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

REGKEY クラス

REGKEY クラスの各レコードは、Windows の環境設定情報が保存されているレジストリのキーのツリー構造を定義します(Windows 専用のクラスです)。

デフォルトでは、eTrust AC により、eTrust AC のレジストリ エントリが保護されます。このレジストリのルートは以下の場所にあります。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥eTrustAccessControl

また、eTrust AC により、以下のリンクとその内容も保護されます。

HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services

REGKEY レコードのキーは、レジストリ キーの完全パスです。REGKEY クラスのレコードで変更できるプロパティについて以下に説明します。

注: ファイル名パターンの一部としてワイルドカードを使用できます。ワイルドカードは、*(0 個以上の文字を表す)および ?(任意の 1 文字を表す)です。

変更可能なプロパティ

ACL

リソースへのアクセスを許可されているアクセサ(ユーザおよびグループ)およびアクセス タイプのリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust Access Control に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。REGKEY クラスの有効なアクセス権限は、以下のとおりです。
  - all - そのクラスに対して許可されるすべての操作の実行をアクセサに許可します。
  - delete - Windows レジストリ キーの削除をアクセサに許可します。
  - none - どの操作の実行もアクセサに許可しません。
  - read - Windows レジストリ キーの内容の一覧表示をアクセサに許可します。
  - write - Windows レジストリ キーの変更をアクセサに許可します。

ACL プロパティを変更するには、authorize コマンドまたは authorize- コマンドで access(*authority*) パラメータを使用します。

AUDIT

eTrust Access Control の監査ログに記録されるアクセス イベントのタイプです。有効な値は以下のとおりです。

- all - すべてのアクセス要求が監査されます。
- success - 許可されたすべてのアクセス要求が監査されます。
- failure - 拒否されたアクセス要求のみが監査されます。この値がデフォルト値です。
- none - アクセス要求の監査は行われません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで audit パラメータを使用します。

CALACL

カレンダ アクセス制御リストです。これは、Unicenter TNG カレンダ ステータスに基づいてリソースへのアクセスが許可されているアクセサ(ユーザおよびグループ)のリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust Access Control に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **カレンダ参照** - Unicenter TNG のカレンダへの参照。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。REGKEY クラスの有効なアクセス権限は、以下のとおりです。
  - all - そのクラスに対して許可されるすべての操作の実行をアクセサに許可します。
  - delete - Windows レジストリ キーの削除をアクセサに許可します。
  - none - どの操作の実行もアクセサに許可しません。
  - read - Windows レジストリ キーの内容の一覧表示をアクセサに許可します。
  - write - Windows レジストリ キーの変更をアクセサに許可します。

カレンダが有効な場合にのみアクセスが許可されます。その他の場合はすべてのアクセスが拒否されます。

ACL アクセスに基づいて、ユーザまたはグループにリソースへのアクセスを許可するには、authorize コマンドで calendar パラメータを使用します。

CALENDAR

eTrust Access Control のユーザ、グループ、およびリソース制限の Unicenter TNG カレンダ オブジェクトを表します。eTrust Access Control は、一定の間隔で Unicenter TNG のアクティブなカレンダを取得します。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで calendar パラメータと calendar- パラメータを使用します。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。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。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

DAYTIME

ユーザがリソースにアクセスできる日時を管理する、曜日と時刻の制限です。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで restrictions(days and time) パラメータを使用します。

GROUPS

リソース レコードが属する CONTAINER クラスのレコードのリストです。

REGKEY クラスのレコードのこのプロパティを変更するには、該当する CONTAINER クラスのレコードの MEMBERS プロパティを変更する必要があります。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで mem+ パラメータか mem- パラメータを使用します。

NACL

リソースへのアクセスが許可されないアクセサ(ユーザおよびグループ)と、許可されないアクセス タイプのリストです。NACL の各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust Access Control に定義されているすべてのユーザを NACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されないアクセス** - アクセサが明示的にアクセスを許可されないリソースへのアクセスのタイプです。REGKEY クラスの有効なアクセス権限は、以下のとおりです。
  - all - アクセサがそのクラスに対してすべての操作を実行できないようにします。
  - delete - アクセサが Windows レジストリ キーを削除できないようにします。
  - none - すべての操作の実行をアクセサに許可します。
  - read - アクセサが Windows レジストリ キーを変更できないようにします。
  - write - アクセサが Windows レジストリ キーを変更できないようにします。

NACL プロパティを変更するには、authorize コマンドで deniedaccess(*accesstype*) パラメータ、または authorize- コマンドで deniedaccess- パラメータを使用します。

NOTIFY

リソースの監査イベントが生成された場合に通知を受け取るユーザです。selogrd を使用して指定の電子メール アドレスに送信できる特別な監査レコードを作成することもできます。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで notify[-] パラメータを使用します。

制限: 30 文字。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

PACL

プログラム アクセス制御リストです。特定のプログラムから、またはプログラム名のパターンに一致するプログラムからアクセス要求が行われた場合に、アクセサに適用される ACL です。

パターンを指定すると、PACL によって保護されているリソースは、指定したパターンに一致するプログラムを使用しないとアクセスできません。プログラムが複数のパターンと一致する場合は、文字数が最も多いパターンが優先されます。

プログラム アクセス制御リストの各要素には、以下の情報が含まれています。

- **プログラム参照** - 指定または名前パターン一致による PROGRAM クラスのレコードへの参照。
- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。
- **許可されたアクセス** - 指定されたプログラムを使用している場合にアクセサに許可されるアクセス権。有効な値については、ACL プロパティを参照してください。

ACL プロパティにプログラム、アクセサ、およびアクセス タイプを追加するには、authorize コマンドで via(pgm) パラメータを使用します。ACL プロパティからこれらを削除するには、authorize- コマンドで via(pgm) パラメータを使用します。

UACC

リソースに対するデフォルトのアクセス権です。eTrust Access Control に定義されていないアクセサ、またはリソースの ACL に登録されていないアクセサに与えるアクセス権を示します。有効な値については、リソースの ACL プロパティを参照してください。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで defaccess パラメータを使用します。

WARNING

警告モードを有効にするかどうかを示します。警告モードを有効にすると、すべてのアクセス要求が許可されます。アクセス要求がアクセス ルールに違反する場合は、レコードが監査ログに書き込まれます。

注: 警告モードの場合、eTrust Access Control では、リソース グループに対する警告メッセージは作成されません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで warning[-] パラメータを使用します。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

RESOURCE_DESC クラス

RESOURCE_DESC クラスの各レコードは、eTrust Web Access Control でアクセスを許可するユーザ定義の新しいクラス オブジェクトの名前をすべて定義します。RESOURCE_DESC クラスに新しいオブジェクトを作成することはできません。既存のオブジェクトの変更のみが可能です。

RESOURCE_DESC クラスのレコードで変更できるプロパティについて以下に説明します。

変更可能なプロパティ

CLASS_RIGHT**

32 種類のアクセス権のオプションは、すべて変更可能です。最初の 4 種類のアクセス権のデフォルト値は、以下のとおりです。

- CLASS_RIGHT1 - 読み取り
- CLASS_RIGHT2 - 書き込み
- CLASS_RIGHT3 - 実行
- CLASS_RIGHT4 - 名前変更

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。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。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

RESPONSE_LIST

このオブジェクトの名前が含まれる RESPONSE_TAB クラスのオブジェクトの名前です。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

RESPONSE_TAB クラス

RESPONSE_TAB クラスの各レコードは、さまざまな権限付与の決定に応じた eTrust Web Access Control の応答テーブルを定義します。

応答は、権限要求が許可または拒否された後にアプリケーションに返されるパーソナライズされた答えです。応答はキーと値のペアで構成され、特定のアプリケーションによって認識されます。応答を定義すると、ユーザの特定のニーズおよび権限付与の許可に従って、ポータル サイトをパーソナライズすることができます。

RESPONSE_TAB クラスのレコードで変更できるプロパティについて以下に説明します。

変更可能なプロパティ

CLASS_RIGHT**

キーと値のペア（たとえば、button1=yes、picture2=no など）が含まれている文字列を一覧表示する 32 種類のオプションの応答プロパティです。各アクセス値に対して 1 つのプロパティを指定します。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。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。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

OF_RESOURCE

同一のユーザ定義クラスを参照する RESOURCE_DESC クラスのオブジェクトの名前です。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

RULESET クラス

RULESET クラスの各レコードは、ポリシーを定義するルールのセットを表します。オブジェクト名は、ポリシー名に基づいて指定します。

変更可能なプロパティ

レコードに含まれている以下のプロパティは、selang によって変更できます。

SIGNATURE

RULESET_DOCMDS プロパティと RULESET_UNDOCMDS プロパティに基づくハッシュ値です。

RULESET_DOCMDS

ポリシーを同時に定義するための selang のコマンドのリストです。これらは、ポリシーの展開のために実行されるコマンドです。

重要: ポリシーの展開では、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展開スクリプト ファイルに含めないでください。UNIX/Linux(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。

RULESET_UNDOCMDS

一緒にポリシー展開解除スクリプトを定義する selang のコマンドのリストです。これらは、ポリシーの展開解除のために実行されるコマンドです。

変更できないプロパティ

レコードに含まれている以下のプロパティは、eTrust Access Control によって自動的に変更されます。selang を使用して変更することはできません。

RULESET_DOCMD_IDX

コマンド インデックスです。これは RULESET_DOCMDS リストのコマンド数のカウンタになります。

RULESET_UNDOCMD_IDX

コマンド インデックスです。これは RULESET_UNDOCMDS リストのコマンド数のカウンタになります。

RULESET_POLICIES

このルール セットを使用するポリシー(POLICY オブジェクト)のリストです。

SECFILE クラス

SECFILE クラスの各レコードは、監視対象ファイルを定義します。SECFILE クラスのレコードによって、システムの重要なファイルを検証できます。ただし、このレコードは条件付きアクセス制御リストには表示できません。

頻繁に更新されない機密システム ファイルをこのクラスに追加し、権限のないユーザがこれらのファイルを変更していないことを確認します。監視対象として SECFILE クラスに指定するファイルの例を以下に示します。

UNIX/Linux の場合	Windows の場合
/.rhosts	¥system32¥drivers¥etc¥hosts
/etc/services	¥system32¥drivers¥etc¥services
/etc/protocols	¥system32¥drivers¥etc¥protocols
/etc/hosts	
/etc/hosts.equiv	

Watchdog はこれらのファイルをスキャンし、これらのファイルに関する既知の情報が変更されていないことを確認します。

注: ディレクトリは SECFILE クラスに定義できません。

SECFILE クラスのレコードのキーは、SECFILE レコードが保護するファイルの名前です。完全パスを指定します。SECFILE クラスのレコードで変更できるプロパティについて以下に説明します。

変更可能なプロパティ

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。この情報が eTrust Access Control による権限付与に使用されることはありません。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

GROUPS

リソース レコードが属する CONTAINER クラスのレコードのリストです。

SECFILE クラスのレコードのこのプロパティを変更するには、該当する CONTAINER クラスのレコードの MEMBERS プロパティを変更する必要があります。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで mem+ パラメータか mem- パラメータを使用します。

HPUXACL

HP-UX システム ACL です。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

PGMINFO

eTrust Access Control で自動的に生成されるプログラムの情報です。

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 eTrust Access Control により Untrusted として定義されます。

以下のフラグを選択すると、この検証プロセスから関連情報を**除外**できます。

- crc - CRC（巡回冗長検査）および MD5 シグネチャ
- device - （UNIX/Linux のみ）ファイルが置かれている論理ディスク

- group - （UNIX/Linux のみ）プログラム ファイルを所有する UNIX/Linux グループ
- inode - （UNIX/Linux のみ）プログラム ファイルのファイル システム アドレス
- mode - （UNIX/Linux のみ）プログラム ファイルの UNIX/Linux セキュリティ モード（許可）
- mtime - プログラム ファイルが最後に変更された時刻
- owner - （UNIX/Linux のみ）プログラム ファイルを所有する UNIX/Linux ユーザ
- sha1 - SHA1 シグネチャ。SHA（Secure Hash Algorithm）と呼ばれるデジタル シグネチャ方法で、プログラムまたは機密ファイルに適用することができます。
- size - プログラム ファイルのサイズ

このプロパティのフラグを変更するには、chres コマンド、editres コマンド、または newres コマンドで flags パラメータ、flags+ パラメータ、または flags- パラメータを使用します。

UNTRUST

プログラムが Trusted かどうかを示します。ファイルに設定したフラグのいずれかに何らかの変更が加えられた場合、eTrust Access Control によって UNTRUST プロパティが自動的に設定されます。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで trust[-] パラメータを使用します。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

MD5

ファイルの RSA-MD5 シグネチャです。

UNTRUSTREASON

プログラムが Untrusted になった理由

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

SECLABEL クラス

SECLABEL クラスの各レコードは、セキュリティ レベルをセキュリティ カテゴリに関連付けます。SECLABEL クラスがアクティブな場合、セキュリティ ラベルは USER クラスのレコードの特定のセキュリティ レベルおよびセキュリティ カテゴリの割り当てよりも優先されます。セキュリティ ラベルの割り当ては、セキュリティ ラベルのセキュリティ レベルおよびセキュリティ カテゴリをユーザに明示的に割り当てることと同じです。

USER クラスのレコードにセキュリティ ラベルが設定されている場合は、以下の条件が満たされている場合にのみ、リソースに対するアクセス権限がユーザに与えられます。

- セキュリティ ラベルに指定されたユーザのセキュリティ レベルが、リソースのセキュリティ レベル以上であること。
- リソース レコードに指定されたすべてのセキュリティ カテゴリが、ユーザのセキュリティ ラベルのセキュリティ カテゴリ リストに含まれていること。

注(Windows): eTrust Access Control に定義されている各セキュリティ ラベルは、SECLABEL クラスのレコードを持つ必要があります。

SECLABEL クラスのレコードのキーは、セキュリティ ラベルの名前です。この名前は、ユーザまたはリソースに割り当てる場合、セキュリティ ラベルの識別に使用されます。SECLABEL クラスのレコードで変更できるプロパティについて以下に説明します。

変更可能なプロパティ

CATEGORY

リソースに割り当てる 1 つまたは複数のセキュリティ カテゴリです。CATEGORY クラスに定義されている任意のセキュリティ カテゴリを指定できます。リソースに 1 つまたは複数のセキュリティ 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**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。

リソースのこのプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで category[-] パラメータを使用します。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。この情報が eTrust Access Control による権限付与に使用されることはありません。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

SECLEVEL

ユーザまたはリソースのセキュリティ レベルです。セキュリティ レベルは 0 から 255 までの正の整数です。値 0 は、セキュリティ レベルを割り当てないことを意味します。リソースにセキュリティ レベルを割り当てた場合は、ユーザのセキュリティ レベルがリソースのセキュリティ レベル以上である場合にのみ、リソースへのアクセス権がユーザに与えられます。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで level[-] パラメータを使用します。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

SEOS クラス

SEOS クラスは、eTrust Access Control の権限付与システムの動作を制御します。

クラスには、一般的なセキュリティと権限のオプションを指定する、SEOS という 1 つのレコードのみが含まれています。SEOS クラスのレコードで変更できるプロパティについて以下に説明します。

変更可能なプロパティ

ACCPACL

認証プロセスで UACC（defaccess）および PACL のリストをスキャンする順序を示します。

ACCPACL がアクティブであり、ユーザのアクセス権が ACL で明示的に指定されている場合は、そのアクセサが許可されたアクセス権となります。アクセス権が ACL ではなく PACL で明示的に指定されている場合は、PACL アクセス権が許可されたアクセス権となります。ACL と PACL のいずれにも明示的なアクセス権が指定されていない場合は、defaccess のアクセス定義がチェックされます。

ACCPACL がアクティブでない場合は、最初に ACL の明示的なアクセス権がチェックされます。ACL にチェック対象リソースに関する明示的なアクセス権が定義されていない場合は、次に defaccess 定義がチェックされます。defaccess に明示的なアクセス権が定義されていない場合は、次に PACL アクセス権の定義がチェックされます。

eTrust Access Control のインストール時に、このプロパティの値は yes に設定されます。

このプロパティを変更するには、setoptions コマンドで accpacl パラメータまたは accpacl- パラメータを使用します。

ADMIN

ADMIN クラスをアクティブにするかどうかを示します。通常、ADMIN クラスはアクティブで、セキュリティ管理タスクの実行許可を制御します。ADMIN クラスがアクティブでない場合は、すべてのユーザが eTrust Access Control の管理者と同様の作業を行うことができます。

APPL

APPL クラスをアクティブにするかどうかを示します。

AUTHHOST

AUTHHOST クラスをアクティブにするかどうかを示します。

CALENDAR

CALENDAR クラスをアクティブにするかどうかを示します。

CATEGORY

CATEGORY クラスをアクティブにするかどうかを示します。

CNG_ADMIN_PWD

PWMANAGER 属性を持つユーザが selang を使用して ADMIN ユーザのパスワードを変更できるかどうかを示します。デフォルトは yes です。

このプロパティをアクティブまたは非アクティブにするには、setoptions コマンドで class+ パラメータまたは class- パラメータと CNG_ADMIN_PWD オプションを使用します。

CNG_OWN_PWD

ユーザが selang を使用して自分のパスワードを変更できるかどうかを示します。

このプロパティをアクティブまたは非アクティブにするには、setoptions コマンドで class+ パラメータまたは class- パラメータと CNG_OWN_PWD オプションを使用します。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。この情報が eTrust Access Control による権限付与に使用されることはありません。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

CONNECT

CONNECT クラスをアクティブにするかどうかを示します。CONNECT クラスがアクティブな場合、このクラスのレコードは外部への接続を保護します。

HOST クラスがアクティブな場合、CONNECT クラスは、アクティブであってもアクティブなクラスとして使用されません。

TCP クラスがアクティブな場合、CONNECT クラスはアクティブなクラスとして使用されません。

DAYTIMERES

(UNIX/Linux のみ)eTrust Access Control でリソースの日時制限をチェックするかどうかを示します。

DOMAIN

(Windows のみ)DOMAIN クラスをアクティブにするかどうかを示します。

FILE

FILE クラスをアクティブにするかどうかを示します。FILE クラスがアクティブな場合、このクラスのレコードはファイルおよびディレクトリを保護します。

GRACCR

累積されたユーザのグループ権限を eTrust Access Control でチェックするかどうかを示します。

このプロパティをアクティブまたは非アクティブにするには、setoptions コマンドで class+ パラメータまたは class- パラメータと GRACCR オプションを使用します。

HOLIDAY

HOLIDAY クラスをアクティブにするかどうかを示します。HOLIDAY クラスがアクティブな場合、定義された休日期間中にユーザがログインするには特別な許可が必要となります。

HOST

HOST クラスをアクティブにするかどうかを示します。HOST クラスがアクティブな場合、eTrust Access Control は、リモート ホストから受信する TCP/IP サービス要求を保護します。

HOST クラスがアクティブな場合、TCP クラスおよび CONNECT クラスは、アクティブであってもアクティブなクラスとして使用されません。

HOST クラスは、デフォルトではアクティブです。

INACT

ユーザ ログインを一時停止するまでの非アクティブ状態の日数を示します。非アクティブ状態の日とは、ユーザがログインしていない日を指します。

このプロパティを更新するには、setoptions コマンドで inactive パラメータ、または inactive- パラメータを使用します。

LOGINAPPL

(UNIX/Linux のみ)LOGINAPPL クラスをアクティブにするかどうかを示します。

MAXLOGINS

ユーザに許可される同時ログインの最大数(端末セッション数)です。この値を超えると、ユーザのアクセスは拒否されます。値が 0 の場合は、最大数を設定しないことを意味します。ユーザは任意の数の端末セッションに同時にログインできます。eTrust Access Control では、ログイン、selang、GUI などの個々のタスクが 1 つの端末セッションとみなされます。そのため、ユーザがログインして selang を実行するか、またはデータベースを管理する場合は、0 を指定するか、1 より大きい値を指定する必要があります。

USER クラスのレコードの MAXLOGINS プロパティの値は、GROUP クラスのレコードの値よりも優先されます。これらの両方のプロパティ値は、SEOS クラスのレコードの MAXLOGINS プロパティよりも優先されます。SEOS クラスのレコードの値は、アクセサ レコードに明示的な値の指定がない場合に使用されるデフォルト値です。

SEOS クラスのこのプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで maxlogins パラメータを使用します。

MFTERMINAL

MFTERMINAL クラスをアクティブにするかどうかを示します。

PASSWDRULES

パスワード ルールを示します。このプロパティには、eTrust 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。

このプロパティを変更するには、setoptions コマンドで password パラメータおよび rules オプションまたは rules- オプションを使用します。

PASSWORD

パスワード チェックをアクティブにするかどうかを示します。

このプロパティをアクティブまたは非アクティブにするには、setoptions コマンドで class+ パラメータまたは class− パラメータおよび PASSWORD オプションを使用します。

PROCESS

PROCESS クラスをアクティブにするかどうかを示します。PROCESS クラスがアクティブな場合、このクラスのレコードは、定義されているプロセスが（kill コマンドによって）強制終了されないように保護します。

ファイルは、FILE クラスにも定義されている必要があります。

PROGRAM

PROGRAM クラスをアクティブにするかどうかを示します。PROGRAM クラスがアクティブな場合、このクラスのレコードは、Trusted のマークが付いて定義されたプログラムを保護します。

PWPOLICY

PWPOLICY クラスをアクティブにするかどうかを示します。

REGKEY

（Windows のみ）REGKEY クラスをアクティブにするかどうかを示します。

RESOURCE_DESC

RESOURCE_DESC クラスをアクティブにするかどうかを示します。

RESPONSE_TAB

RESPONSE_TAB クラスをアクティブにするかどうかを示します。

SECLABEL

SECLABEL クラスをアクティブにするかどうかを示します。

SECLEVEL

SECLEVEL クラスをアクティブにするかどうかを示します。

SUDO

sesudo で使用する SUDO クラスをアクティブにするかどうかを示します。

SURROGATE

SURROGATE クラスをアクティブにするかどうかを示します。SURROGATE クラスがアクティブな場合、eTrust Access Control は代理要求を保護します。

TCP

TCP クラスをアクティブにするかどうかを示します。TCP クラスがアクティブな場合、eTrust Access Control は、メール、ftp、http などの TCP サービスの送受信を保護します。

HOST クラスがアクティブな場合、TCP クラスは、アクティブであってもアクティブなクラスとして使用されません。

TCP クラスがアクティブな場合、CONNECT クラスはアクティブなクラスとして使用されません。

TERMINAL

TERMINAL クラスをアクティブにするかどうかを示します。TERMINAL クラスがアクティブな場合、eTrust Access Control は、サインオン時に端末アクセス チェックを行い、X-window セッションを保護します。

USER_ATTR

USER_ATTR クラスをアクティブにするかどうかを示します。

USER_DIR

USER_DIR クラスをアクティブにするかどうかを示します。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

ENDTIME

データベース ファイルが通常の方法で最後に閉じられた日時です。

STARTTIME

データベース ファイルが最後に開かれた日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

selang の構文

SEOS クラス プロパティの現在のステータスを表示するには、selang の以下のコマンドを入力します。

```
setoptions list
```

クラスのアクティブ化ステータスを変更するには、selang の以下のコマンドを入力します。

```
setoptions class+(className)
```

または

```
setoptions class-(className)
```

CNG_ADMIN_PWD、CNG_OWN_PWD、GRACCR、および PASSWORD のプロパティは、アクティブ化ステータスを変更する目的のためにクラスとして扱われます。

SPECIALPGM クラス

SPECIALPGM クラスは、特定のプログラムに特別なセキュリティ権限を指定します。

SPECIALPGM クラスの各レコードには、以下のいずれかの機能があります。

- Windows の場合は、backup、DCM、PBF、PBN、STOP、SURROGATE、および REGISTRY の各機能を登録します。UNIX/Linux の場合は、xdm、backup、mail、DCM、PBF、PBN、stop、および surrogate の各プログラムを登録します。
- eTrust Access Control の特別な権限付与によって保護する必要があるアプリケーションを論理ユーザ ID に関連付けます。これにより、***誰が***実行しているかではなく***何が***実行されているかによって、アクセス許可を効率的に設定できます。

注: SPECIALPGM クラスにプログラムを定義する場合、FILE クラスにもプログラムを定義する必要があります。こうすると、許可なしに実行可能ファイルを変更(置換または破損)できなくなるため、実行可能ファイルを保護でき、eTrust Access Control が実行されていないときに修正された場合には、PROGRAM リソースによってプログラムの起動が防止されます。

SPECIALPGMTYPE プロパティを使用して、システム サービス、デーモン、またはその他の特別なプログラムを登録します。

SEOSUID プロパティおよび NATIVEUID プロパティを使用して、論理ユーザをプログラムに割り当てます。

SPECIALPGM クラスのレコードのキーは、特別なプログラムへのパス、または特別なプログラムの範囲またはパターンへのパスです。SPECIALPGM クラスのレコードで変更できるプロパティについて以下に説明します。

変更可能なプロパティ

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。この情報が eTrust Access Control による権限付与に使用されることはありません。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

UNIXUID

プログラムまたはプロセスを起動するユーザを示します。eTrust Access Control のすべてのユーザを指定するには、「*」を使用します。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで nativeuid パラメータを使用します。

注: eTrust Access Control の旧バージョンとの互換性を維持するために、NATIVUID プロパティの代わりに UNIXUID プロパティを使用できます。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

SPECIALPGMTYPE

アクセスを許可する際に、eTrust Access Control が無視するアクセス チェックのタイプを決定します。

Windows の場合、このタイプは backup、dcm、pbf、pbn、stop、registry、および surrogate、またはこれらの組み合わせです。UNIX/Linux の場合は、backup、mail、xdm、dcm、pbf、pbn、surrogate、および stop、またはこれらの組み合わせです。

backup

READ アクセス、CHDIR アクセス、および UTIME アクセスを省略します。

注: バックアップを成功させるには 2 つの方法があります。バックアップ プログラムを root 以外のユーザが実行する場合、このユーザを OPERATOR として定義する必要があります。バックアップ プログラムが root によって実行される場合、SPECIALPGM クラスにバックアップ プログラムを pgmtype(backup) として登録するだけで十分です。

次に例を示します。

```
nr specialpgm /usr/sbin/tar pgmtype(backup) owner(nobody)
```

dcm

STOP イベントを除くすべてのイベントに対するセキュリティ チェックを省略します。

mail

(UNIX/Linux のみ)setuid イベントおよび setgid イベントに対するデータベース チェックを省略します。この mail によるデータベース チェックの省略により、アクセスを試みるメールをトレースできます。

pbf

ファイル処理イベントに対するデータベース チェックを省略します。

pbn

ネットワーク関連のイベントに対するデータベース チェックを省略します。

registry

(Windows のみ)Windows レジストリを操作するプログラムに対するデータベース チェックを省略します。

stop

STOP 機能に対するデータベース チェックを省略します。

surrogate

カーネル内の ID 変更イベントに対するデータベース チェックを省略します。このように surrogate によってデータベース チェックを省略した場合は、トレースを行うことができません。

xdm

(UNIX/Linux のみ)制限されたネットワーク範囲(6000 ～ 6010)に対してネットワーク イベント(TCP クラス、HOST クラス、および CONNECT クラスなど)を省略します。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで pgmtype パラメータを使用します。

たとえば、UNIX/Linux では以下のコマンドを実行できます。

```
chres SPECIALPGM /bin/login pgmtype(surrogate)
```

Windows では以下のコマンドを実行できます。

```
newres SPECIALPGM ("c:¥winnt¥system32¥wbem¥winmgmt.exe") pgmtype(REGISTRY)
```

SEOSUID

(UNIX/Linux のみ)この特別なプログラムを実行する権限がある論理ユーザを示します。この論理ユーザは、データベースの USER クラスのレコードに定義されている必要があります。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで seosuid パラメータを使用します。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

UNIX/Linux での selang の例

/DATABASE/data/* にあるファイルを保護するために、データベースの管理者は、ファイル サーバ デーモン firmdb_filemgr を使用します。このファイル サーバは、/opt/dbfirm/bin/firmdb_filemgr にあります。このデーモンは通常 root 権限で実行され、データは root シェルによるアクセスが可能な状態になっています。

以下の例では、これらのファイルの唯一のアクセサとして論理ユーザが定義されます。つまり、他のユーザはアクセスを制限されます。

1. 以下のコマンドを使用して、「機密」ファイルを eTrust Access Control に定義します。

   ```
   newres file /DATABASE/data/* defaccess(NONE) owner(nobody)
   ```

2. ファイルにアクセスする論理ユーザを定義します。

   ```
   newusr firmDB_mgr
   ```

3. 論理ユーザ firmDB_mgr のみにファイルへのアクセスを許可します。

   ```
   Authorize file /DATABASE/data/* uid(firmDB_mgr) access(ALL).
   ```

4. 最後に、論理ユーザ firmDB_mgr が firmdb_filemgr を実行できるようにします。

   ```
   newres SPECIALPGM /opt/dbfirm/bin/firmdb_filemgr unixuid(root) ¥
   seosuid(firmDB_mgr).
   ```

この結果、デーモンがファイルにアクセスすると、eTrust Access Control は、root ユーザではなく論理ユーザをファイルのアクセサとして認識します。ハッカーが root ユーザとしてファイルにアクセスしようとしても、アクセスできません。

Windows での selang の例

C:¥DATABASE¥data にあるファイルを保護するために、データベースの管理者は、firmdb_filemgr.exe というファイル サーバ サービスを使用します。このファイル サーバは、C:¥Program Files¥dbfirm¥bin¥firmdb_filemgr.exe にあります。このサービスは通常システム アカウントで実行され、データはあらゆるシステム ハックが可能な状態になっています。

以下の例では、これらのファイルの唯一のアクセサとして論理ユーザが定義されます。つまり、他のユーザはアクセスを制限されます。

1. 以下のコマンドを使用して、「機密」ファイルを eTrust AC に定義します。

   ```
   newres file C:¥DATABASE¥data¥* defaccess(NONE) owner(nobody)
   ```

2. ファイルにアクセスする論理ユーザを定義します。

   ```
   newusr firmDB_mgr
   ```

3. 論理ユーザ firmDB_mgr のみにファイルへのアクセスを許可します。

```
Authorize file C:¥DATABASE¥data¥* uid(firmDB_mgr) access(ALL)
```

4. 最後に、論理ユーザ firmDB_mgr が firmdb_filemgr を実行できるようにします。

```
newres SPECIALPGM ("C:¥Program Files¥dbfirm¥bin¥firmdb_filemgr.exe") ¥
nativeuid(system) seosuid(firmDB_mgr)
```

この結果、サービスがファイルにアクセスすると、eTrust Access Control は、システム アカウントではなく論理ユーザをファイルのアクセサとして認識します。ハッカーがシステム アカウントでファイルにアクセスしようとしても、アクセスできません。

SUDO クラス

SUDO クラスの各レコードは、あるユーザが sesudo コマンド(258 ページ)を使用して別のユーザの権限を借用できるようにするためのコマンドを識別します。

SUDO クラスのレコードのキーは、SUDO レコードの名前です。この名前は、ユーザが SUDO レコードでコマンドを実行する際に、コマンド名の代わりに使用されます。SUDO クラスのレコードで変更できるプロパティについて以下に説明します。

注: 端末サービスがインストールされているコンピュータで、SYSTEM アカウント以外のユーザ アカウントが SeOS タスク委任機能サービスを実行しているときは、sesudo コマンドで対話処理を実行することができません。

変更可能なプロパティ

ACL

リソースへのアクセスを許可されているアクセサ(ユーザおよびグループ)およびアクセス タイプのリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust Access Control に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。SUDO クラスの有効なアクセス権限は、以下のとおりです。
  - execute - プログラムの実行をアクセサに許可します。
  - none - どの操作の実行もアクセサに許可しません。
  - ACL プロパティを変更するには、authorize コマンドまたは authorize- コマンドで *access(authority)* パラメータを使用します。

AUDIT

eTrust Access Control の監査ログに記録されるアクセス イベントのタイプです。有効な値は以下のとおりです。

- all - すべてのアクセス要求が監査されます。
- success - 許可されたすべてのアクセス要求が監査されます。
- failure - 拒否されたアクセス要求のみが監査されます。この値がデフォルト値です。
- none - アクセス要求の監査は行われません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで audit パラメータを使用します。

CALACL

カレンダ アクセス制御リストです。これは、Unicenter TNG カレンダ ステータスに基づいてリソースへのアクセスが許可されているアクセサ(ユーザおよびグループ)のリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust Access Control に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **カレンダ参照** - Unicenter TNG のカレンダへの参照。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。SUDO クラスの有効なアクセス権限は、以下のとおりです。
  - execute - プログラムの実行をアクセサに許可します。
  - none - どの操作の実行もアクセサに許可しません。

カレンダが有効な場合にのみアクセスが許可されます。その他の場合はすべてのアクセスが拒否されます。

ACL アクセスに基づいて、ユーザまたはグループにリソースへのアクセスを許可するには、authorize コマンドで calendar パラメータを使用します。

CALENDAR

eTrust Access Control のユーザ、グループ、およびリソース制限の Unicenter TNG カレンダ オブジェクトを表します。eTrust Access Control は、一定の間隔で Unicenter TNG のアクティブなカレンダを取得します。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで calendar パラメータと calendar- パラメータを使用します。

CATEGORY

リソースに割り当てる 1 つまたは複数のセキュリティ カテゴリです。CATEGORY クラスに定義されている任意のセキュリティ カテゴリを指定できます。リソースに 1 つまたは複数のセキュリティ 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**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。

リソースのこのプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで category[-] パラメータを使用します。

COMMENT

sesudo が実行するコマンドです。このパラメータは、旧バージョンの eTrust Access Control で使用されていた DATA パラメータに代わるものです。

最大 255 文字の英数字からなる文字列です。この文字列には、コマンドが含まれています。さらに、許可されているパラメータおよび禁止されているパラメータも含まれています。

たとえば、以下のプロファイル定義では、COMMENT プロパティが正しく使用されています。

```
newres SUDO profile_name comment('command::NAME')
```

このプロパティの指定と SUDO レコードの定義の詳細については、「管理者ガイド」を参照してください。

注: このクラスでの COMMENT プロパティの使用方法は、その他のクラスでの使用方法とは異なります。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

DAYTIME

ユーザがリソースにアクセスできる日時を管理する、日付と時刻の制限です。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで restrictions(days and time) パラメータを使用します。

GROUPS

リソース レコードが属する CONTAINER クラスのレコードのリストです。

SUDO クラスのレコードのこのプロパティを変更するには、該当する CONTAINER クラスのレコードの MEMBERS プロパティを変更する必要があります。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで mem+ パラメータか mem- パラメータを使用します。

INTERACTIVE

sesudo で実行する予定のアプリケーションが対話形式の Windows アプリケーション(notepad.exe、cmd.exe など)で、サービス アプリケーションではない場合に、このスイッチを指定する必要があります。sesudo クライアント コマンドで対話形式のアプリケーションを実行しようとしても、「interactive」と指定していない場合には、バックグランドで実行され、対話機能が失われます。

注: 一部の Windows アプリケーションは、Windows の制限のために、フォアグラウンド モードで実行できません。

NACL

リソースへのアクセスが許可されないアクセサ(ユーザおよびグループ)と、許可されないアクセス タイプのリストです。NACL の各要素には、以下の情報が含まれています。

アクセサ参照 - アクセサ(ユーザまたはグループ)への参照。eTrust Access Control に定義されているすべてのユーザを NACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。

- **許可されないアクセス** - アクセサが明示的にアクセスを許可されないリソースへのアクセスのタイプです。SUDO クラスの有効なアクセス権限は、以下のとおりです。

- execute - アクセサがプログラムを実行できないようにします。
- none - すべての操作の実行をアクセサに許可します。

NACL プロパティを変更するには、authorize コマンドで deniedaccess(*accesstype*) パラメータ、または authorize- コマンドで deniedaccess- パラメータを使用します。

NOTIFY

リソースの監査イベントが生成された場合に通知を受け取るユーザです。selogrd を使用して指定の電子メール アドレスに送信できる特別な監査レコードを作成することもできます。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで notify[-] パラメータを使用します。

制限: 30 文字。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

PACL

プログラム アクセス制御リストです。特定のプログラムから、またはプログラム名のパターンに一致するプログラムからアクセス要求が行われた場合に、アクセサに適用される ACL です。

パターンを指定すると、PACL によって保護されているリソースは、指定したパターンに一致するプログラムを使用しないとアクセスできません。プログラムが複数のパターンと一致する場合は、文字数が最も多いパターンが優先されます。

プログラム アクセス制御リストの各要素には、以下の情報が含まれています。

- **プログラム参照** - 指定または名前パターン一致による PROGRAM クラスのレコードへの参照。
- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。
- **許可されたアクセス** - 指定されたプログラムを使用している場合にアクセサに許可されるアクセス権。有効な値については、ACL プロパティを参照してください。

ACL プロパティにプログラム、アクセサ、およびアクセス タイプを追加するには、authorize コマンドで via(pgm) パラメータを使用します。ACL プロパティからこれらを削除するには、authorize- コマンドで via(pgm) パラメータを使用します。

PASSWORDREQ

(UNIX/Linux のみ)sesudo コマンドが実行前にターゲット ユーザ パスワードを要求するかどうかを示します。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで password パラメータを使用します。

SECLABEL

リソースのセキュリティ ラベルです。セキュリティ ラベルは、セキュリティ レベルをセキュリティ カテゴリに関連付けます。

適用する場合、セキュリティ ラベルは、レコードに設定された特定のセキュリティ レベルおよびセキュリティ カテゴリよりも優先されます。セキュリティ ラベルを割り当てることは、ラベルのレベルとカテゴリをユーザに明示的に割り当てることと同じです。指定されたセキュリティ ラベルは、SECLABEL クラスのレコードとして定義する必要があります。USER クラスのレコードにセキュリティ ラベルが設定されている場合は、以下の条件が両方とも満たされている場合にのみ、リソースへのアクセス権がユーザに与えられます。

- セキュリティ ラベルに指定されたユーザのセキュリティ レベルが、リソースのセキュリティ レベル以上であること。
- リソース レコードに指定されたすべてのセキュリティ カテゴリが、ユーザのセキュリティ ラベルのセキュリティ カテゴリ リストに含まれていること。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで label[-] パラメータを使用します。

SECLEVEL

ユーザまたはリソースのセキュリティ レベルです。セキュリティ レベルは 0 から 255 までの正の整数です。値 0 は、セキュリティ レベルを割り当てないことを意味します。リソースにセキュリティ レベルを割り当てた場合は、ユーザのセキュリティ レベルがリソースのセキュリティ レベル以上である場合にのみ、リソースへのアクセス権がユーザに与えられます。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで level[-] パラメータを使用します。

TARGUSR

(UNIX/Linux のみ)ターゲット UID を示します。この UID は、コマンドを実行するためのアクセス許可の借用先ユーザを設定します。デフォルトは root です。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで targuid パラメータを使用します。

UACC

リソースに対するデフォルトのアクセス権です。eTrust Access Control に定義されていないアクセサ、またはリソースの ACL に登録されていないアクセサに与えるアクセス権を示します。有効な値については、リソースの ACL プロパティを参照してください。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで defaccess パラメータを使用します。

WARNING

警告モードを有効にするかどうかを示します。警告モードを有効にすると、すべてのアクセス要求が許可されます。アクセス要求がアクセス ルールに違反する場合は、レコードが監査ログに書き込まれます。

注: 警告モードの場合、eTrust Access Control では、リソース グループに対する警告メッセージは作成されません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで warning[-] パラメータを使用します。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

SURROGATE クラス

SURROGATE クラスの各レコードは、他のユーザがユーザの ID を使用しようとしたときに、ユーザを他のユーザから保護するための制限を定義します。eTrust Access Control では、権限を持つユーザのみがアクセスできる抽象オブジェクトとして ID 変更要求を処理します。

SURROGATE クラスのレコードは、ID 変更要求から保護する対象のユーザまたはグループを表します。特別な 2 つのレコード(USER._default および GROUP._default)は、個々の SURROGATE クラスのレコードを持たないユーザおよびグループを表します。ユーザのデフォルトとグループのデフォルトを区別する必要がない場合、代わりに SURROGATE クラスに _default レコードを使用できます。

SURROGATE クラスのレコードのキーは、SURROGATE レコードの名前です。SURROGATE クラスのレコードで変更できるプロパティについて以下に説明します。

変更可能なプロパティ

ACL

リソースへのアクセスを許可されているアクセサ(ユーザおよびグループ)およびアクセス タイプのリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust Access Control に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。SURROGATE クラスの有効なアクセス権限は、以下のとおりです。
  - none - どの操作の実行もアクセサに許可しません。
  - read - ユーザに対する su 要求の実行をアクセサに許可します。

ACL プロパティを変更するには、authorize コマンドまたは authorize- コマンドで access(*authority*) パラメータを使用します。

AUDIT

eTrust Access Control の監査ログに記録されるアクセス イベントのタイプです。有効な値は以下のとおりです。

- all - すべてのアクセス要求が監査されます。
- success - 許可されたすべてのアクセス要求が監査されます。
- failure - 拒否されたアクセス要求のみが監査されます。この値がデフォルト値です。
- none - アクセス要求の監査は行われません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで audit パラメータを使用します。

CALACL

カレンダ アクセス制御リストです。これは、Unicenter TNG カレンダ ステータスに基づいてリソースへのアクセスが許可されているアクセサ(ユーザおよびグループ)のリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust Access Control に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **カレンダ参照** - Unicenter TNG のカレンダへの参照。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。SURROGATE クラスの有効なアクセス権限は、以下のとおりです。
  - none - どの操作の実行もアクセサに許可しません。
  - read - ユーザに対する su 要求の実行をアクセサに許可します。

カレンダが有効な場合にのみアクセスが許可されます。その他の場合はすべてのアクセスが拒否されます。

ACL アクセスに基づいて、ユーザまたはグループにリソースへのアクセスを許可するには、authorize コマンドで calendar パラメータを使用します。

CALENDAR

eTrust Access Control のユーザ、グループ、およびリソース制限の Unicenter TNG カレンダ オブジェクトを表します。eTrust Access Control は、一定の間隔で Unicenter TNG のアクティブなカレンダを取得します。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで calendar パラメータと calendar- パラメータを使用します。

CATEGORY

リソースに割り当てる 1 つまたは複数のセキュリティ カテゴリです。CATEGORY クラスに定義されている任意のセキュリティ カテゴリを指定できます。リソースに 1 つまたは複数のセキュリティ 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**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。

リソースのこのプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで category[-] パラメータを使用します。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。この情報が eTrust Access Control による権限付与に使用されることはありません。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

DAYTIME

ユーザがリソースにアクセスできる日時を管理する、曜日と時刻の制限です。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで restrictions(days and time) パラメータを使用します。

GROUPS

リソース レコードが属する CONTAINER クラスのレコードのリストです。

SURROGATE クラスのレコードのこのプロパティを変更するには、該当する CONTAINER クラスのレコードの MEMBERS プロパティを変更する必要があります。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで mem+ パラメータか mem- パラメータを使用します。

NACL

リソースへのアクセスが許可されないアクセサ(ユーザおよびグループ)と、許可されないアクセス タイプのリストです。NACL の各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust Access Control に定義されているすべてのユーザを NACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されないアクセス** - アクセサが明示的にアクセスを許可されないリソースへのアクセスのタイプです。SURROGATE クラスの有効なアクセス権限は、以下のとおりです。
  - none - すべての操作の実行をアクセサに許可します。
  - read - アクセサがユーザに対して su 要求を行うことができないようにします。

NACL プロパティを変更するには、authorize コマンドで deniedaccess(*accesstype*) パラメータ、または authorize- コマンドで deniedaccess- パラメータを使用します。

NOTIFY

リソースの監査イベントが生成された場合に通知を受け取るユーザです。selogrd を使用して指定の電子メール アドレスに送信できる特別な監査レコードを作成することもできます。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで notify[-] パラメータを使用します。

制限: 30 文字。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

PACL

プログラム アクセス制御リストです。特定のプログラムから、またはプログラム名のパターンに一致するプログラムからアクセス要求が行われた場合に、アクセサに適用される ACL です。

パターンを指定すると、PACL によって保護されているリソースは、指定したパターンに一致するプログラムを使用しないとアクセスできません。プログラムが複数のパターンと一致する場合は、文字数が最も多いパターンが優先されます。

プログラム アクセス制御リストの各要素には、以下の情報が含まれています。

- **プログラム参照** - 指定または名前パターン一致による PROGRAM クラスのレコードへの参照。
- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。
- **許可されたアクセス** - 指定されたプログラムを使用している場合にアクセサに許可されるアクセス権。有効な値については、ACL プロパティを参照してください。

ACL プロパティにプログラム、アクセサ、およびアクセス タイプを追加するには、authorize コマンドで via(pgm) パラメータを使用します。ACL プロパティからこれらを削除するには、authorize- コマンドで via(pgm) パラメータを使用します。

SECLABEL

リソースのセキュリティ ラベルです。セキュリティ ラベルは、セキュリティ レベルをセキュリティ カテゴリに関連付けます。

適用する場合、セキュリティ ラベルは、レコードに設定された特定のセキュリティ レベルおよびセキュリティ カテゴリよりも優先されます。セキュリティ ラベルを割り当てることは、ラベルのレベルとカテゴリをユーザに明示的に割り当てることと同じです。指定されたセキュリティ ラベルは、SECLABEL クラスのレコードとして定義する必要があります。USER クラスのレコードにセキュリティ ラベルが設定されている場合は、以下の条件が両方とも満たされている場合にのみ、リソースへのアクセス権がユーザに与えられます。

- セキュリティ ラベルに指定されたユーザのセキュリティ レベルが、リソースのセキュリティ レベル以上であること。
- リソース レコードに指定されたすべてのセキュリティ カテゴリが、ユーザのセキュリティ ラベルのセキュリティ カテゴリ リストに含まれていること。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで label[-] パラメータを使用します。

SECLEVEL

ユーザまたはリソースのセキュリティ レベルです。セキュリティ レベルは 0 から 255 までの正の整数です。値 0 は、セキュリティ レベルを割り当てないことを意味します。リソースにセキュリティ レベルを割り当てた場合は、ユーザのセキュリティ レベルがリソースのセキュリティ レベル以上である場合にのみ、リソースへのアクセス権がユーザに与えられます。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで level[-] パラメータを使用します。

UACC

リソースに対するデフォルトのアクセス権です。eTrust Access Control に定義されていないアクセサ、またはリソースの ACL に登録されていないアクセサに与えるアクセス権を示します。有効な値については、リソースの ACL プロパティを参照してください。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで defaccess パラメータを使用します。

WARNING

警告モードを有効にするかどうかを示します。警告モードを有効にすると、すべてのアクセス要求が許可されます。アクセス要求がアクセス ルールに違反する場合は、レコードが監査ログに書き込まれます。

注: 警告モードの場合、eTrust Access Control では、リソース グループに対する警告メッセージは作成されません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで warning[-] パラメータを使用します。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

SURROGATE 要求の制限

selang を使用して新しい SURROGATE クラスのレコードを eTrust Access Control に定義するには、以下のコマンドを入力します。

```
newres SURROGATE USER. userName
```

注: eTrust Access Control では、ユーザとグループに同じ名前を指定できるため、代理レコードで参照しているオブジェクトがユーザかグループかを eTrust Access Control に通知する必要があります。これを行うには、例で示したように、オブジェクト名の前に「USER」または「GROUP」とピリオドを付けます。

TCP クラス

TCP クラスの各レコードは、メール、ftp、http などの TCP/IP サービスのレコードを定義します。TCP クラスがアクティブで、権限付与に使用されている場合、TCP リソースが明示的または暗示的にアクセスを許可する場合のみ、ホストはローカル ホストからサービスを取得することができます。同様に、ユーザまたはグループは、TCP リソースによって明示的または暗黙的にアクセス権限を与えられた場合にのみ、ローカル ホストのサービスを使用してリモート ホストにアクセスできます。

注: TCP クラスを使用してレコードを定義する場合は、同じレコードに対して CONNECT クラスを使用しないでください。

このクラスを使用すると、ホスト名だけでなく、IP アドレスに基づいてルールを設定できるので便利です。ドメイン名が変更されても、IP アドレスで設定されたホストを引き続き保護できます。

各レコードの ACL では、サービスを要求する個々のホストのみではなく、ホスト グループ(GHOST)、ネットワーク(HOSTNET)、および名前パターンで定義された一連のホスト(HOSTNP)に対しても、アクセス タイプを指定できます。

また、レコードの CACL では、サービスを使用して特定のホストまたはホストのグループ(GHOST リソース、HOSTNET リソース、または HOSTNP リソース)にアクセスできる特定のユーザおよびグループを指定できます。

HOST クラスまたは CONNECT クラスがアクティブになっている(つまり、アクセスの基準として使用されている)場合、TCP クラスを実質的にアクティブにすることはできません。

TCP レコードのキーは、TCP/IP サービスの名前です。TCP クラスは、送信サービス**および**受信サービスを制御します。

eTrust Access Control では、この名前によりサービスが識別されます。TCP クラスのレコードで変更できるプロパティについて以下に説明します。

変更可能なプロパティ

ACL

ローカル ホストがサービスを提供するホスト(HOST、GHOST、HOSTNET、および HOSTNP タイプ のリソース)とアクセス タイプのリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **ホスト参照** - HOST クラス、GHOST クラス、HOSTNET クラス、または HOSTNP クラスのレコードへの参照。
- **許可されるアクセス** - ホスト参照に与えられる、リソースに対するアクセス権限。TCP クラスの有効なアクセス権限は、以下のとおりです。
  - none - どの操作の実行もホスト参照に許可しません。

- read - ローカル ホストからの TCP サービスの取得をホスト参照に許可します。

ACL プロパティを変更するには、authorize コマンドまたは authorize- コマンドで access(*authority*)パラメータを使用します。

AUDIT

eTrust Access Control の監査ログに記録されるアクセス イベントのタイプです。有効な値は以下のとおりです。

- all - すべてのアクセス要求が監査されます。
- success - 許可されたすべてのアクセス要求が監査されます。
- failure - 拒否されたアクセス要求のみが監査されます。この値がデフォルト値です。
- none - アクセス要求の監査は行われません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで audit パラメータを使用します。

CACL

サービスに対してアクセスが許可されているユーザおよびグループ、およびそれらのユーザおよびグループがアクセスできるホストのリストです。条件付きアクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - ユーザまたはグループの名前。
- **ホスト参照** - HOST クラス、GHOST クラス、HOSTNET クラス、または HOSTNP クラスのレコードへの参照。
- **許可されるアクセス** - サービスに対してアクセサが持つ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、以下のとおりです。
- write - このサービスを使用したホストまたはホストのグループへのアクセスをアクセサに許可します。
- none - このサービスを使用したホストまたはホストのグループへのアクセスをアクセサに許可しません。

このプロパティを変更するには、authorize コマンドまたは authorize- コマンドを使用します。

CALACL

カレンダ アクセス制御リストです。これは、Unicenter TNG カレンダ ステータスに基づいてリソースへのアクセスが許可されているアクセサ(ユーザおよびグループ)のリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust Access Control に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。

- **カレンダ参照** - Unicenter TNG のカレンダへの参照。
- **許可されるアクセス** - ホスト参照に与えられる、リソースに対するアクセス権限。TCP クラスの有効なアクセス権限は、以下のとおりです。
  - none - どの操作の実行もホスト参照に許可しません。
  - read - ローカル ホストからの TCP サービスの取得をホスト参照に許可します。

カレンダが有効な場合にのみアクセスが許可されます。その他の場合はすべてのアクセスが拒否されます。

ACL アクセスに基づいて、ユーザまたはグループにリソースへのアクセスを許可するには、authorize コマンドで calendar パラメータを使用します。

CALENDAR

eTrust Access Control のユーザ、グループ、およびリソース制限の Unicenter TNG カレンダ オブジェクトを表します。eTrust Access Control は、一定の間隔で Unicenter TNG のアクティブなカレンダを取得します。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで calendar パラメータと calendar- パラメータを使用します。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。この情報が eTrust Access Control による権限付与に使用されることはありません。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

DAYTIME

ユーザがリソースにアクセスできる日時を管理する、曜日と時刻の制限です。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで restrictions(days and time) パラメータを使用します。

GROUPS

リソース レコードが属する CONTAINER クラスのレコードのリストです。

TCP クラスのレコードのこのプロパティを変更するには、該当する CONTAINER クラスのレコードの MEMBERS プロパティを変更する必要があります。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで mem+ パラメータか mem- パラメータを使用します。

NACL

リソースへのアクセスが許可されないアクセサ(ユーザおよびグループ)と、許可されないアクセス タイプのリストです。NACL の各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust Access Control に定義されているすべてのユーザを NACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されないアクセス** - アクセサが明示的にアクセスを許可されないリソースへのアクセスのタイプです。TCP クラスの有効なアクセス権限は、以下のとおりです。
  - none - すべての操作の実行をホスト参照に許可します。
  - read - ホスト参照がローカル ホストから TCP サービスを取得できないようにします。

NACL プロパティを変更するには、authorize コマンドで deniedaccess(*accesstype*) パラメータ、または authorize- コマンドで deniedaccess- パラメータを使用します。

NOTIFY

リソースの監査イベントが生成された場合に通知を受け取るユーザです。selogrd を使用して指定の電子メール アドレスに送信できる特別な監査レコードを作成することもできます。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで notify[-] パラメータを使用します。

制限: 30 文字。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

PACL

プログラム アクセス制御リストです。特定のプログラムから、またはプログラム名のパターンに一致するプログラムからアクセス要求が行われた場合に、アクセサに適用される ACL です。

パターンを指定すると、PACL によって保護されているリソースは、指定したパターンに一致するプログラムを使用しないとアクセスできません。プログラムが複数のパターンと一致する場合は、文字数が最も多いパターンが優先されます。

プログラム アクセス制御リストの各要素には、以下の情報が含まれています。

- **プログラム参照** - 指定または名前パターン一致による PROGRAM クラスのレコードへの参照。
- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。
- **許可されたアクセス** - 指定されたプログラムを使用している場合にアクセサに許可されるアクセス権。有効な値については、ACL プロパティを参照してください。

ACL プロパティにプログラム、アクセサ、およびアクセス タイプを追加するには、authorize コマンドで via(pgm) パラメータを使用します。ACL プロパティからこれらを削除するには、authorize- コマンドで via(pgm) パラメータを使用します。

UACC

リソースに対するデフォルトのアクセス権です。eTrust Access Control に定義されていないアクセサ、またはリソースの ACL に登録されていないアクセサに与えるアクセス権を示します。有効な値については、リソースの ACL プロパティを参照してください。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで defaccess パラメータを使用します。

WARNING

警告モードを有効にするかどうかを示します。警告モードを有効にすると、すべてのアクセス要求が許可されます。アクセス要求がアクセス ルールに違反する場合は、レコードが監査ログに書き込まれます。

注: 警告モードの場合、eTrust Access Control では、リソース グループに対する警告メッセージは作成されません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで warning[-] パラメータを使用します。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

TERMINAL クラス

TERMINAL クラスの各レコードは、ローカル ホストの端末、ネットワーク上にある別のホストの端末、またはログイン セッションを実行できる X 端末を定義します。端末のアクセス許可はユーザ ログイン手続きの過程でチェックされ、使用権限のない端末からユーザがログインすることはできません。

TERMINAL クラスは、また管理アクセスも制御します。ADMIN ユーザは、適切なアクセス権限がある端末からのみ、eTrust Access Control を管理できます。

新しい TERMINAL クラスのレコードを定義すると、eTrust Access Control は、ユーザが指定した名前を完全修飾名に変換しようとします。変換に成功すると、完全修飾名がデータベースに格納されます。変換に失敗すると、ユーザが指定した名前が格納されます。これ以降、このレコードを参照するコマンド(chres、showres、rmres、authorize など)を発行する際には、データベースに保存されている名前を使用する必要があります。

TERMINAL クラスのレコードのキーは、端末の名前です。eTrust Access Control では、この名前により端末が識別されます。TERMINAL クラスのレコードで変更できるプロパティについて以下に説明します。

変更可能なプロパティ

ACL

リソースへのアクセスを許可されているアクセサ(ユーザおよびグループ)およびアクセス タイプのリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust Access Control に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。TERMINAL クラスの有効なアクセス権限は、以下のとおりです。
  - none - どの操作の実行もアクセサに許可しません。
  - read - 端末からのログインをアクセサに許可します。
  - write - 端末からの eTrust Access Control の管理をアクセサに許可します。

ACL プロパティを変更するには、authorize コマンドまたは authorize- コマンドで access(*authority*)パラメータを使用します。

AUDIT

eTrust Access Control の監査ログに記録されるアクセス イベントのタイプです。有効な値は以下のとおりです。

- all - すべてのアクセス要求が監査されます。

- success - 許可されたすべてのアクセス要求が監査されます。
- failure - 拒否されたアクセス要求のみが監査されます。この値がデフォルト値です。
- none - アクセス要求の監査は行われません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで audit パラメータを使用します。

CALACL

カレンダ アクセス制御リストです。これは、Unicenter TNG カレンダ ステータスに基づいてリソースへのアクセスが許可されているアクセサ(ユーザおよびグループ)のリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust Access Control に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **カレンダ参照** - Unicenter TNG のカレンダへの参照。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。TERMINAL クラスの有効なアクセス権限は、以下のとおりです。
  - none - どの操作の実行もアクセサに許可しません。
  - read - 端末からのログインをアクセサに許可します。
  - write - 端末からの eTrust Access Control の管理をアクセサに許可します。

カレンダが有効な場合にのみアクセスが許可されます。その他の場合はすべてのアクセスが拒否されます。

ACL アクセスに基づいて、ユーザまたはグループにリソースへのアクセスを許可するには、authorize コマンドで calendar パラメータを使用します。

CALENDAR

eTrust Access Control のユーザ、グループ、およびリソース制限の Unicenter TNG カレンダ オブジェクトを表します。eTrust Access Control は、一定の間隔で Unicenter TNG のアクティブなカレンダを取得します。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで calendar パラメータと calendar- パラメータを使用します。

CATEGORY

リソースに割り当てる 1 つまたは複数のセキュリティ カテゴリです。CATEGORY クラスに定義されている任意のセキュリティ カテゴリを指定できます。リソースに 1 つまたは複数のセキュリティ 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**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。

リソースのこのプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで category[-] パラメータを使用します。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。この情報が eTrust Access Control による権限付与に使用されることはありません。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

DAYTIME

ユーザがリソースにアクセスできる日時を管理する、日付と時刻の制限です。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで restrictions(days and time) パラメータを使用します。

GROUPS

リソース レコードが属する GTERMINAL クラスまたは CONTAINER クラスのレコードのリストです。

TERMINAL クラスのレコードのこのプロパティを変更するには、該当する CONTAINER クラスまたは GTERMINAL クラスのレコードの MEMBERS プロパティを変更する必要があります。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで mem+ パラメータか mem- パラメータを使用します。

NACL

リソースへのアクセスが許可されないアクセサ(ユーザおよびグループ)と、許可されないアクセス タイプのリストです。NACL の各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust Access Control に定義されているすべてのユーザを NACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されないアクセス** - アクセサが明示的にアクセスを許可されないリソースへのアクセスのタイプです。TERMINAL クラスの有効なアクセス権限は、以下のとおりです。
  - none - すべての操作の実行をアクセサに許可します。
  - read - アクセサが端末からログインできないようにします。
  - write - アクセサが端末から eTrust Access Control を管理できないようにします。

NACL プロパティを変更するには、authorize コマンドで deniedaccess(*accesstype*) パラメータ、または authorize- コマンドで deniedaccess- パラメータを使用します。

NOTIFY

リソースの監査イベントが生成された場合に通知を受け取るユーザです。selogrd を使用して指定の電子メール アドレスに送信できる特別な監査レコードを作成することもできます。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで notify[-] パラメータを使用します。

制限: 30 文字。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

PACL

プログラム アクセス制御リストです。特定のプログラムから、またはプログラム名のパターンに一致するプログラムからアクセス要求が行われた場合に、アクセサに適用される ACL です。

パターンを指定すると、PACL によって保護されているリソースは、指定したパターンに一致するプログラムを使用しないとアクセスできません。プログラムが複数のパターンと一致する場合は、文字数が最も多いパターンが優先されます。

プログラム アクセス制御リストの各要素には、以下の情報が含まれています。

- **プログラム参照** - 指定または名前パターン一致による PROGRAM クラスのレコードへの参照。
- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。
- **許可されたアクセス** - 指定されたプログラムを使用している場合にアクセサに許可されるアクセス権。有効な値については、ACL プロパティを参照してください。

ACL プロパティにプログラム、アクセサ、およびアクセス タイプを追加するには、authorize コマンドで via(pgm) パラメータを使用します。ACL プロパティからこれらを削除するには、authorize- コマンドで via(pgm) パラメータを使用します。

SECLABEL

リソースのセキュリティ ラベルです。セキュリティ ラベルは、セキュリティ レベルをセキュリティ カテゴリに関連付けます。

適用する場合、セキュリティ ラベルは、レコードに設定された特定のセキュリティ レベルおよびセキュリティ カテゴリよりも優先されます。セキュリティ ラベルを割り当てることは、ラベルのレベルとカテゴリをユーザに明示的に割り当てることと同じです。指定されたセキュリティ ラベルは、SECLABEL クラスのレコードとして定義する必要があります。

USER クラスのレコードにセキュリティ ラベルが設定されている場合は、以下の条件が両方とも満たされている場合にのみ、リソースへのアクセス権がユーザに与えられます。

- セキュリティ ラベルに指定されたユーザのセキュリティ レベルが、リソースのセキュリティ レベル以上であること。
- リソース レコードに指定されたすべてのセキュリティ カテゴリが、ユーザのセキュリティ ラベルのセキュリティ カテゴリ リストに含まれていること。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで label[-] パラメータを使用します。

SECLEVEL

ユーザまたはリソースのセキュリティ レベルです。セキュリティ レベルは 0 から 255 までの正の整数です。値 0 は、セキュリティ レベルを割り当てないことを意味します。リソースにセキュリティ レベルを割り当てた場合は、ユーザのセキュリティ レベルがリソースのセキュリティ レベル以上である場合にのみ、リソースへのアクセス権がユーザに与えられます。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで level[-] パラメータを使用します。

UACC

リソースに対するデフォルトのアクセス権です。eTrust Access Control に定義されていないアクセサ、またはリソースの ACL に登録されていないアクセサに与えるアクセス権を示します。有効な値については、リソースの ACL プロパティを参照してください。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで defaccess パラメータを使用します。

WARNING

警告モードを有効にするかどうかを示します。警告モードを有効にすると、すべてのアクセス要求が許可されます。アクセス要求がアクセス ルールに違反する場合は、レコードが監査ログに書き込まれます。

注: 警告モードの場合、eTrust Access Control では、リソース グループに対する警告メッセージは作成されません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで warning[-] パラメータを使用します。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

UACC クラス

UACC クラスの各レコードは、リソース クラスに許可するデフォルト アクセスを定義します。UACC クラスのレコードは、eTrust Access Control で保護されないクラスのリソースに許可するアクセス レベルも決定します。

UACC は、一部のクラスを除いたほとんどのクラスに適用できます。FILE クラスの場合、UACC は標準とは異なる方法で適用されます(以下の表を参照してください)。各クラスでの UACC クラスの使用方法を以下の表に示します。

UACC の使用方法	クラス
標準	ADMIN、APPL、AUTHHOST、CALENDAR、CONNECT、CONTAINER、DOMAIN、GAPPL、GAUTHHOST、GHOST、GSUDO、GTERMINAL、HOLIDAY、HOST、HOSTNET、HOSTNP、MFTERMINAL、PROCESS、PROGRAM、REGKEY、SUDO、SURROGATE、TCP、TERMINAL、USER_DIR、ユーザ定義クラス
非標準	FILE、GFILE
なし	AGENT、AGENT_TYPE、CATEGORY、GROUP、PWPOLICY、RESOURCE_DESC、RESPONSE_TAB、SECFILE、SECLABEL、SEOS、SPECIALPGM、USER、USER_ATTR

特別な _restricted グループに属していないユーザの場合、UACC クラスの FILE のレコードでは、seos.ini ファイル、seosd.trace ファイル、seos.audit ファイル、および seos.error ファイルなど、eTrust Access Control の一部のファイルのみが保護されます。これらのファイルは eTrust Access Control に明示的に定義されていませんが、eTrust Access Control で自動的に保護されます。

UACC クラスのレコードのキーは、UACC プロパティを定義するクラスの名前です。UACC クラスのレコードで変更できるプロパティについて以下に説明します。

変更可能なプロパティ

ACL

リソースへのアクセスを許可されているアクセサ(ユーザおよびグループ)およびアクセス タイプのリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust Access Control に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。UACC クラスの有効なアクセス権限は、UACC クラスで定義するクラスに対して有効なアクセス タイプです。

ACL プロパティを変更するには、authorize コマンドまたは authorize- コマンドで access(*authority*)パラメータを使用します。

ALLOWACCS

このクラスに対して許可されるすべてのアクセス権のリストです。

AUDIT

eTrust Access Control の監査ログに記録されるアクセス イベントのタイプです。有効な値は以下のとおりです。

- all - すべてのアクセス要求が監査されます。
- success - 許可されたすべてのアクセス要求が監査されます。
- failure - 拒否されたアクセス要求のみが監査されます。この値がデフォルト値です。
- none - アクセス要求の監査は行われません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで audit パラメータを使用します。

CALACL

カレンダ アクセス制御リストです。これは、Unicenter TNG カレンダ ステータスに基づいてリソースへのアクセスが許可されているアクセサ(ユーザおよびグループ)のリストです。アクセス制御リストの各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust Access Control に定義されているすべてのユーザを ACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **カレンダ参照** - Unicenter TNG のカレンダへの参照。
- **許可されたアクセス** - アクセサに与えられる、リソースに対するアクセス権限。UACC クラスの有効なアクセス権限は、UACC クラスで定義するクラスに対して有効なアクセス タイプです。

カレンダが有効な場合にのみアクセスが許可されます。その他の場合はすべてのアクセスが拒否されます。

ACL アクセスに基づいて、ユーザまたはグループにリソースへのアクセスを許可するには、authorize コマンドで calendar パラメータを使用します。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。この情報が eTrust Access Control による権限付与に使用されることはありません。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

DEFACCS

リソースに対するデフォルトのアクセス権を定義します。eTrust Access Control に定義されていないアクセサ、またはリソースの ACL に登録されていないアクセサに与えるアクセス権を示します。有効な値については、リソースの ACL プロパティを参照してください。

NACL

リソースへのアクセスが許可されないアクセサ(ユーザおよびグループ)と、許可されないアクセス タイプのリストです。NACL の各要素には、以下の情報が含まれています。

- **アクセサ参照** - アクセサ(ユーザまたはグループ)への参照。eTrust Access Control に定義されているすべてのユーザを NACL に指定するには、アクセサ参照としてアスタリスク(*)を入力します。
- **許可されないアクセス** - アクセサが明示的にアクセスを許可されないリソースへのアクセスのタイプです。UACC クラスの有効なアクセス権限は、UACC クラスで定義するクラスに対して有効なアクセス タイプです。

NACL プロパティを変更するには、authorize コマンドで deniedaccess(*accesstype*) パラメータ、または authorize- コマンドで deniedaccess- パラメータを使用します。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

UACC

リソースに対するデフォルトのアクセス権です。eTrust Access Control に定義されていないアクセサ、またはリソースの ACL に登録されていないアクセサに与えるアクセス権を示します。有効な値については、リソースの ACL プロパティを参照してください。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで defaccess パラメータを使用します。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

USER_ATTR クラス

USER_ATTR クラスの各レコードは、eTrust Web Access Control ユーザ ディレクトリの有効なユーザ属性を定義します。

USER_ATTR クラスのレコードで変更できるプロパティについて以下に説明します。

変更可能なプロパティ

ATTR_PREDEFS

特定の属性に対して許可される値のリストです。

AUDIT

eTrust Access Control の監査ログに記録されるアクセス イベントのタイプです。有効な値は以下のとおりです。

- all - すべてのアクセス要求が監査されます。
- success - 許可されたすべてのアクセス要求が監査されます。
- failure - 拒否されたアクセス要求のみが監査されます。この値がデフォルト値です。
- none - アクセス要求の監査は行われません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで audit パラメータを使用します。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。この情報が eTrust Access Control による権限付与に使用されることはありません。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

DBFIELD

userdir データベースに登録されているフィールドの名前です。異なるデータベースには異なる属性を指定できるため、属性フィールドは同期させる必要があります。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

PARAMETER_TYPE

ユーザ属性が文字列か数値かを示します。

PRIORITY

ユーザ属性の優先順位です。PARAM_RULE オブジェクト(APPL、URL など)に権限ルールを設定する際、ユーザ属性によって参照される優先度と共にルールが定義されます。

USERATTR_FLAGS

属性に関する情報が含まれています。フラグには、以下の値を指定できます。

- aznchk - この属性が権限付与に使用されるかどうかを示します。
- predef(事前に定義済み)、freetex(自由形式のテキスト)、または userdir(ユーザ ディレクトリ) - これら 3 つの値で、ユーザ属性のソースを示します。
- user または group - これらの値を使用して、属性(アクセサ)がユーザかグループかを示します。

WARNING

警告モードを有効にするかどうかを示します。警告モードを有効にすると、すべてのアクセス要求が許可されます。アクセス要求がアクセス ルールに違反する場合は、レコードが監査ログに書き込まれます。

注: 警告モードの場合、eTrust Access Control では、リソース グループに対する警告メッセージは作成されません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで warning[-] パラメータを使用します。

変更できないプロパティ

ATTRNAME

属性の名前です。

CREATE_TIME

レコードが作成された日時です。

FIELDID

DB フィールドの ID です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

USER_DIR_PROP

ユーザのディレクトリの名前です。

USER_DIR クラス

USER_DIR クラスの各レコードは、eTrust Web Access Control ユーザ ディレクトリを定義します。

USER_DIR クラスのレコードのキーは、ディレクトリの名前です。USER_DIR クラスのレコードで変更できるプロパティについて以下に説明します。

変更可能なプロパティ

ADMIN_NAME

ディレクトリ管理者のログイン名です。

ADMIN_PWD

ディレクトリ管理者のパスワードです。パスワードは、テキスト形式の平文で格納されます。selang では表示されませんが、seadmapi の関数を使用して表示できます。

AUDIT

eTrust Access Control の監査ログに記録されるアクセス イベントのタイプです。有効な値は以下のとおりです。

- all - すべてのアクセス要求が監査されます。
- success - 許可されたすべてのアクセス要求が監査されます。
- failure - 拒否されたアクセス要求のみが監査されます。この値がデフォルト値です。
- none - アクセス要求の監査は行われません。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで audit パラメータを使用します。

AZNACL

権限 ACL です。リソースの説明に基づいてリソースへのアクセスを許可します。説明は、オブジェクトではなく認証エンジンに送信されます。オブジェクトは、ほとんどの場合データベースに存在しません。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。この情報が eTrust Access Control による権限付与に使用されることはありません。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで comment[-] パラメータを使用します。

CONTOBJ_CLS

コンテナ オブジェクトに継承されるクラスの名前です(LDAP で新規ログイン情報コンテナを作成するために必要)。

DIR_TYPE

ディレクトリのタイプです。有効な値は、ETRUST_AC、LDAP、ODBC、NT_Domain、または none です。

GRPOBJ_CLS

グループ オブジェクトに継承されるクラスの名前です(LDAP で新規グループを作成するために必要)。

LICONTOBJ_CLS

ログイン情報コンテナ オブジェクトに継承されるクラスの名前です(LDAP で新規ログイン情報コンテナを作成するために必要)。

LIOBJ_CLS

ログイン情報オブジェクトに継承されるクラスの名前です(LDAP で新規ログイン情報を作成するために必要)。

MAX_RET_ITEMS

取得される項目の最大数です。デフォルトは、ディレクトリ タイプによって異なります。

OWNER

レコードの所有者であるユーザまたはグループです。

このプロパティを変更するには、chres コマンド、editres コマンド、および newres コマンドで owner パラメータを使用します。

PATH

すべてのクエリを開始するための LDAP ツリー内の相対識別名です。

PORT_NUM

ディレクトリへのアクセスに使用するホスト コンピュータでのポート番号です。

TIMEOUT_CON

タイムアウト エラー メッセージを発行するまでに、システムがディレクトリへの接続を待つ時間(秒単位)です。

UACC

リソースに対するデフォルトのアクセス権です。eTrust Access Control に定義されていないアクセサ、またはリソースの ACL に登録されていないアクセサに与えるアクセス権を示します。有効な値については、リソースの ACL プロパティを参照してください。

このプロパティを変更するには、chres コマンド、editres コマンド、または newres コマンドで defaccess パラメータを使用します。

USERATTR_LIST

この USER_DIR オブジェクトで USER_DIR パラメータの値として作成された USER_ATTR クラスのオブジェクトのリストです。

USERDIR_HOST

ディレクトリのホスト コンピュータの名前です。このプロパティは、クラスのレコードに定義されている必要があります。

USROBJ_CLS

ユーザ オブジェクトに継承されるクラスの名前です(LDAP で新規ユーザを作成するために必要)。

VERSION

ディレクトリのバージョン番号です。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

ユーザ定義クラス

ユーザ定義クラスの各レコードは、必要に応じて独自に作成したクラスへのアクセス権を定義します。ユーザ定義のクラス名に関する唯一の制限は、すべて大文字の名前を指定できないことです。

たとえば、データベースを使用して独自のデータを格納および表示しているサイトがあるとします。各データベース ビュー(レコード)をユーザ定義クラスのメンバとして定義し、各データベース ビューを作成するために必要な権限の種類を指定することができます。eTrust Access Control は、ユーザにデータベース ビューの作成を許可する前に、ユーザの権限レベルをチェックします。

ユーザ定義クラスのレコードのキーは、レコードの名前です。

Unicenter TNG ユーザ定義クラス

eTrust Access Control では、リソースとして Unicenter TNG のアセット クラスを定義できます。Unicenter TNG ユーザ定義クラスは、作成または削除したり、アクティブまたは無効にすることが可能です。

Unicenter TNG ユーザ定義クラスは UACC クラスにあります。

変更可能なプロパティ

標準の eTrust Access Control クラスに定義される任意のプロパティをユーザ定義クラスに使用できます。

変更できないプロパティ

CREATE_TIME

レコードが作成された日時です。

UPDATE_TIME

レコードが最後に変更された日時です。

UPDATE_WHO

更新を実行した管理者です。

第 7 章: Windows 環境のクラスとプロパティ

このセクションには、以下のトピックが含まれます。

クラスとプロパティの情報

この章では、NT 環境データベースに定義されている、すべてのクラスのすべてのプロパティについて説明します。

注: このマニュアルで使用する「***NT 環境***」という用語は、selang の env nt コマンドまたはポリシー マネージャの[Windows NT]プログラム バーを使用してアクセスするデータベースを指しています。これは、ユーザ、グループ、およびリソースを管理する Windows オペレーティング システムのデータベースと同じです。

eTrust データベースに関する前の章と同様に、変更可能なプロパティ、それらのプロパティを更新するときに使用する selang のパラメータ、およびそれらのパラメータが指定されたコマンドに関する情報をクラス別に示します。これらのクラスで使用する selang のコマンドについては、「Windows 環境のクラスとプロパティ」の章を参照してください。

アクセサのクラスとプロパティ

eTrust Access Control では、ユーザの集合とグループの集合がそれぞれ 2 種類管理されます。eTrust 環境と NT 環境の両方で同じ名前のアクセサを作成できますが、アクセサのプロパティはそれぞれの環境で**異なります**。この章では、NT 環境に固有のプロパティについて説明します。

USER クラス

USER クラスには、Windows オペレーティング システムに定義されているすべてのユーザ レコードが含まれています。USER レコードのキーは、ユーザがシステムへのログイン時に入力するユーザ名です。

変更可能なプロパティ

USER クラスのレコードの変更可能なプロパティについて以下に説明します。また、プロパティを更新する selang のパラメータも示します。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。この情報が eTrust Access Control による権限付与に使用されることはありません。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで comment[-] パラメータを使用します。

COUNTRY

ユーザの国記述子を指定する文字列です。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 Access Control による権限付与に使用されることはありません。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで country パラメータを使用します。

DAYTIME

ユーザがリソースにアクセスできる日時を管理する、日付と時刻の制限です。USER クラスのレコードの DAYTIME プロパティの値は、GROUP クラスのレコードの値よりも優先されます。

注: このプロパティの情報は、入力された分単位の値が切り捨てられること以外は、eTrust 環境の DAYTIME プロパティの情報と同じです。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで restrictions(days and time) パラメータを使用します。

DIAL_CALLBACK

ユーザに提供するコール バック権限の種類。以下のオプションが定義されています。

NoCallBack

ユーザにはコール バック権限がありません。

SetByCaller

リモート ユーザは、ダイヤル イン時にコール バック用の電話番号を指定できます。

Call-back Phone Number

管理者はコール バック用の番号を設定します。

このプロパティを変更するには、chusr コマンドまたは editusr コマンドで gen_prop パラメータまたは gen_val パラメータを使用します。

DIAL_PERMISSION

RAS サーバにダイヤル インする権限。値に 0 を指定すると、ユーザは RAS サーバにダイヤル インできません。

このプロパティを変更するには、chusr コマンドまたは editusr コマンドで gen_prop パラメータまたは gen_val パラメータを使用します。

EXPIRE_DATE

USER クラスのレコードが失効して無効になる日付です。USER クラスのレコードの EXPIRE_DATE プロパティの値は、GROUP クラスのレコードの値よりも優先されます。失効したレコードを元に戻すには、chusr コマンドで expire- パラメータを使用します。失効したユーザを再開することはできません。一時停止したユーザは、再開日を指定することで再開できます。

このプロパティを変更するには、chusr コマンド、editusr コマンド、または newusr コマンドで expire パラメータか expire- パラメータを使用します。

FLAGS

特定の属性を指定するためにユーザのアカウントに割り当てることができるフラグ。各アカウントに複数のフラグを適用できます。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで flags パラメータを使用します。

FULL_NAME

ユーザに関連付けられたフル ネーム。フル ネームは、eTrust Access Control の監査ログ メッセージでユーザを識別するために使用されますが、権限付与に使用されることはありません。

このプロパティを変更するには、chusr コマンド、editusr コマンド、または newusr コマンドで name パラメータを使用します。

GID

グループの相対 ID が含まれている値。相対 ID は、グループの作成時にアカウント データベースによって決定されます。相対 ID によって、ドメイン内のアカウント マネージャに対してグループを一意に識別できます。

GROUPS

ユーザが属するグループのリスト。このプロパティで設定するグループ リストは、eTrust 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。

このプロパティを変更するには、join[-] コマンドで groupname パラメータを使用します。

HOME

ホーム ディレクトリは、ユーザがアクセスできるフォルダで、そのユーザのファイルとプログラムが格納されます。ホーム ディレクトリは、個々のユーザに割り当てたり、多くのユーザ間で共有したりすることができます。

HOMEDIR

ユーザのホーム ディレクトリを指定する文字列。ユーザは、自分のホーム ディレクトリに自動的にログインできます。

このプロパティを変更するには、chusr コマンド、editusr コマンド、または newusr コマンドで homedir パラメータを使用します。

HOME_DRIVE

ユーザのホーム ディレクトリのドライブを指定する文字列。ユーザは、自分のホーム ドライブおよびホーム ディレクトリに自動的にログインできます。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで homedrive パラメータを使用します。

ID

ユーザの相対 ID(RID)が含まれている値。RID は、ユーザの作成時にセキュリティ アカウント マネージャ(SAM)によって決定されます。RID によって、ユーザアカウントがドメイン内の SAM に対して一意に定義されます。

LOCATION

ユーザの所在地を格納するために使用する文字列です。この情報が eTrust Access Control による権限付与に使用されることはありません。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで location パラメータを使用します。

LOGON_SERVER

ユーザのログイン情報を確認するサーバを指定する文字列。ユーザがドメイン ワークステーションにログインすると、eTrust Access Control からサーバにログイン情報が送られ、ユーザがワークステーションを使用することが許可されます。

NAME

ユーザの名前。

ORGANIZATION

ユーザが所属する組織に関する情報を格納する文字列です。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 Access Control による権限付与に使用されることはありません。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで organization パラメータを使用します。

ORG_UNIT

ユーザが所属する組織単位に関する情報を格納する文字列です。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 Access Control による権限付与に使用されることはありません。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで org_unit パラメータを使用します。

PASSWD_EXPIRED

ユーザ アカウントの有効期限。

PGROUP

ユーザのプライマリ グループ ID。プライマリ グループは、ユーザが定義されているグループの 1 つです。プライマリ グループはグローバル グループである必要があります。この文字列には、スペースまたはカンマを指定できません。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで pgroup パラメータを使用します。

PHONE

ユーザの電話番号を格納するために使用できる文字列。この情報が権限付与に使用されることはありません。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで phone パラメータを使用します。

PRIVILEGES

ユーザに割り当てられた Windows 権限。特定の権限の詳細については、付録「Windows の値」を参照してください。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで privileges パラメータを使用します。

PROFILE

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、ローカル絶対パスまたは UNC パスを含めることができます。

このプロパティを変更するには、chusr コマンド、editusr コマンド、または newusr コマンドで profile パラメータを使用します。

RESUME_DATE

一時停止した USER アカウントが有効になる日付です。

RESUME_DATE および SUSPEND_DATE を組み合わせて指定する方法については、SUSPEND_DATE を参照してください。

SCRIPT

ユーザのログオン スクリプト ファイルのパスを指定する文字列。スクリプト ファイルには、.CMD ファイル、.EXE ファイル、または .BAT ファイルを指定できます。

TERMINALS

ユーザがログインできる端末のリストを指定する文字列。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで terminals パラメータを使用します。

TS_CONFIG_PGM

クライアントが初期化プログラムを指定できるかどうかを示す値。

TS_INITIAL_PGM ユーザ プロパティは初期化プログラムを示します。ユーザの初期化プログラムを指定すると、この初期化プログラムはユーザが実行できる唯一のプログラムとなり、ユーザがそのプログラムを終了すると端末サーバがそのユーザをログオフします。

この値が 1 に設定されている場合、クライアントは初期化プログラムを指定できます。この値が 0 に設定されている場合、クライアントは初期化プログラムを指定できません。

このプロパティを変更するには、chusr コマンドと editusr コマンドで gen_prop パラメータおよび gen_val パラメータを使用します。

TS_HOME_DIR

端末サーバにログオンするためのユーザのホーム ディレクトリのパス。この文字列には、ローカル パスまたは UNC パス(¥¥machine¥share¥path)を指定できます。

このプロパティを変更するには、chusr コマンドと editusr コマンドで gen_prop パラメータおよび gen_val パラメータを使用します。

TS_HOME_DRIVE

UNC パスが TS_HOME_DIR プロパティで指定されるドライブ（コロンの後にドライブ文字を指定）。

このプロパティを変更するには、chusr コマンドと editusr コマンドで gen_prop パラメータおよび gen_val パラメータを使用します。

TS_INITIAL_PGM

端末サービスがユーザのログオン時に実行する初期化プログラムのパス。

ユーザの初期化プログラムを指定すると、この初期化プログラムはユーザが実行できる唯一のプログラムとなります。ユーザがそのプログラムを終了すると端末サーバがそのユーザをログオフします。

TS_CONFIG_PGM プロパティが 1 に設定されている場合、クライアントは初期化プログラムを指定できます。

このプロパティを変更するには、chusr コマンドと editusr コマンドで gen_prop パラメータおよび gen_val パラメータを使用します。

TS_PROFILE_PATH

端末サーバにログオンするためのユーザのプロファイルのパス。パスで識別されるディレクトリは、ログオン前に手動で作成する必要があります。

このプロパティを変更するには、chusr コマンドと editusr コマンドで gen_prop パラメータおよび gen_val パラメータを使用します。

TS_WORKING_DIR

端末サービスがユーザのログオン時に実行する初期化プログラムの作業ディレクトリのパス。

このプロパティを変更するには、chusr コマンドと editusr コマンドで gen_prop パラメータおよび gen_val パラメータを使用します。

WORKSTATIONS

ユーザがログインできるワークステーションのリスト。

このプロパティを変更するには、chusr コマンド、editusr コマンド、および newusr コマンドで workstations パラメータを使用します。

変更できないプロパティ

以下のプロパティは Windows によって自動的に変更されますが、selang またはポリシー マネージャを使用して変更することはできません。

BAD_PW_COUNT

ユーザが間違ったパスワードを使用してアカウントにログインしようとした回数。値 -1 は、その値が不明であることを示します。

LAST_ACC_TIME

最後にログインが実行された日時です。

LAST_LOGOFF

最後にログオフが実行された日時です。

MAX_LOGINS

ユーザがこのアカウントに正常にログインした回数。値 -1 は、その値が不明であることを示します。

PW_LAST_CHANGE

パスワードが更新された日時です。

GROUP クラス

GROUP クラスには、Windows オペレーティング システムに定義されているすべてのグループ レコードが含まれています。GROUP クラスのレコードは、ユーザのすべてのグループを表します。

変更可能なプロパティ

NT 環境の GROUP クラスのレコードで変更できるプロパティについて以下に説明します。また、プロパティを更新する selang のパラメータについても説明します。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。この情報が eTrust Access Control による権限付与に使用されることはありません。

このプロパティを変更するには、chgrp コマンド、editgrp コマンド、および newgrp コマンドで comment パラメータまたは comment- パラメータを使用します。

FULL_NAME

ユーザに関連付けられたフル ネーム。フル ネームは、eTrust Access Control の監査ログ メッセージでユーザを識別するために使用されますが、権限付与に使用されることはありません。

このプロパティを変更するには、chusr コマンド、editusr コマンド、または newusr コマンドで name パラメータを使用します。

ISGLOBAL

グローバル グループを示します。このプロパティは、Windows のグループにのみ適用できます。このプロパティは、旧バージョンの eTrust Access Control の ISGLOBAL プロパティに代わるものです。

このプロパティを追加するには、newgrp コマンド（専用）のグローバル パラメータを使用します。

USERLIST

グループに所属するユーザおよびグローバル グループ（ローカル グループ専用）のリスト。このプロパティで設定するリストは、eTrust Access Control データベースで設定するリストとは異なる場合があります。

このプロパティを変更するには、join[-] コマンドで username(*groupname*) パラメータを使用します。

PRIVILEGES

グループに割り当てられた Windows 権限。特定の権限の詳細については、付録「Windows の値」を参照してください。

このプロパティを変更するには、chgrp コマンド、editgrp コマンド、および newgrp コマンドで privileges パラメータを使用します。

変更できないプロパティ

このレコードに含まれている以下のプロパティは、eTrust Access Control によって自動的に変更されるため、selang またはポリシー マネージャを使用して変更することはできません。

GID

グループの相対 ID が含まれている値。相対 ID は、グループの作成時にアカウント データベースによって決定されます。相対 ID によって、ドメイン内のアカウント マネージャに対してグループを一意に識別できます。

リソース クラスとプロパティ

COM クラス

COM クラスの各レコードでは、[コントロール パネル]-[ポート]で表示されるシリアル ポート(COM)またはパラレル ポート(LPT)を指定することによってデバイスを定義します。

注: eTrust Access Control を使用して、COM クラスに新しいオブジェクトを作成することはできません。

COM クラスのキーは、制御されるポートの名前です。COM クラスのレコードで変更できるプロパティについて以下に説明します。

変更可能なプロパティ

DACL

標準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とグループの名前、およびユーザまたはグループごとに与えられたアクセス権のレベルが登録されています。

このプロパティを変更するユーザは、リソースの所有者であるか、またはリソースへの特別なアクセス権(ACL を変更する権限)を持っている必要があります。

アクセス制御リストの各要素には、以下の情報が含まれています。

アクセス タイプ

リソースへのアクセス許可を示します。

- Allowed - リソースへの特別なアクセスを許可します。
- Denied - リソースへの特別なアクセスを許可しません。

アクセサ

アクセスが許可または許可されないユーザまたはグループの名前です。

アクセス

アクセサに与えられる、リソースに対するアクセス権限。COM クラスの有効なアクセス権限は、以下のとおりです。

- all - クラスに許可できるすべての操作を許可または許可しません。
- changeperm - リソースの ACL の変更をアクセサに許可または許可しません。
- delete - リソースの削除をアクセサに許可または許可しません。
- read - データを変更せずに、データを読み取ることをアクセサに許可または許可しません。

- takeown/chown/owner - 指定したデバイスの所有者の変更をアクセサに許可または許可しません。
- write - 指定したデバイスへのデータの書き込みをアクセサに許可または許可しません。

注: 空の ACL(エントリのない ACL)と ACL を持たないリソースの違いに注意してください。空の ACL の場合、アクセス権が明示的に与えられません。したがって、アクセスは暗黙的に拒否されます。ACL を持たないリソースの場合、保護がオブジェクトに割り当てられません。したがって、すべてのアクセス要求が許可されます。

このプロパティを変更するには、auth コマンドまたは auth- コマンドを使用します。

OWNER

リソースの所有者として指定されているユーザまたはグループ。

このプロパティを変更するには、chres コマンドおよび editres コマンドで owner パラメータを使用します。

変更できないプロパティ

DEV

デバイスのシリアル番号を示す文字列。

GID

指定したディスクのプライマリ グループ情報。

SACL

Windows システム アクセス制御リストは監査ディレクティブを示します。

DEVICE クラス

DEVICE クラスの各レコードは、Windows のハードウェア デバイス([コントロール パネル]-[デバイス]に表示されるデバイス)を定義します。

このクラスは、Windows ホストでのみ使用できます。

DEVICE クラスのレコードのキーは、制御されるデバイスの名前です。DEVICE クラスのレコードで変更できるプロパティについて以下に説明します。

変更可能なプロパティ

STARTUPTYPE

デバイスの起動方法(また、いつ起動するか)を定義します。以下のオプションがあります。

- automatic - システムの起動中にデバイスを自動的に起動します。
- boot - システムが起動するたびに、他のデバイスの起動前にデバイスを起動します。このオプションは、システムの動作に不可欠な、重要なデバイスに対して設定してください。
- disabled - ユーザがデバイスを起動できないようにします。disabled でデバイスを無効にしても、システムによるデバイスの起動は可能です。
- manual - ユーザまたは依存関係にあるデバイスによるデバイスの起動を許可します。
- system - システムが起動するたびに、Boot デバイスの起動後にデバイスを起動します。このオプションは、システムの動作に不可欠な、重要なデバイスに対して設定してください。

このプロパティを変更するには、chres コマンドまたは editres コマンドで starttype パラメータを使用します。

STATUS

現在のサービスの状態を変更します。オプションには、started、stopped、および paused があります。

このプロパティを変更するには、chres コマンドまたは editres コマンドで status パラメータを使用します。

IMAGEPATH

指定したデバイスの完全修飾パス。

PROFILE

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、ローカル絶対パスまたは UNC パスを含めることができます。

このプロパティを変更するには、chusr コマンド、editusr コマンド、または newusr コマンドで profile パラメータを使用します。

例

モデムの状態を表示するには、selang の以下のコマンドを入力します。

```
showres DEVICE modem
```

モデムをアクティブにするには、以下のコマンドを入力します。

```
chres device modem status(started)
```

DISK クラス

DISK クラスの各レコードは、システム ボリュームを定義します。ボリュームとは、プライマリ パーティション、拡張パーティションの論理ドライブ、ボリューム セット、ストライプ セット、ミラー セット、パリティ付きストライプ セットなど、Windows オペレーティング システム(サーバ版)を実行しているコンピュータで作成および使用できるエンティティを示す一般的な用語です。ボリュームには、1 つのドライブ文字が割り当てられます。また、ボリュームはファイル システムで使用するためにフォーマットされます。

注: eTrust Access Control を使用して、DISK クラスにオブジェクトを作成することはできません。

DISK クラスのキーは、割り当てられたドライブ文字(C:、D: など)です。DISK クラスのレコードで変更できるプロパティについて以下に説明します。

変更可能なプロパティ

DACL

標準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とグループの名前、およびユーザまたはグループごとに与えられたアクセス権のレベルが登録されています。

このプロパティを変更するユーザは、リソースの所有者であるか、またはリソースへの特別なアクセス権(ACL を変更する権限)を持っている必要があります。

アクセス制御リストの各要素には、以下の情報が含まれています。

アクセス タイプ

リソースへのアクセス許可を示します。

- Allowed - リソースへの特別なアクセスを許可します。
- Denied - リソースへの特別なアクセスを許可しない。

アクセサ

アクセスが許可または許可されないユーザまたはグループの名前です。

アクセス

アクセサに与えられる、リソースに対するアクセス権限。DISK クラスの有効なアクセス権限は、以下のとおりです。

- all - クラスに許可できるすべての操作を許可または許可しません。
- changeperm - リソースの ACL の変更をアクセサに許可または許可しません。
- delete - リソースの削除をアクセサに許可または許可しません。
- read - データを変更せずに、データを読み取ることをアクセサに許可または許可しません。

- takeown/chown/owner - ディスクの所有者の変更をアクセサに許可または拒否します。
- write - 指定したディスクへのデータの書き込みをアクセサに許可または拒否します。

注: 空の ACL(エントリのない ACL)と ACL を持たないリソースの違いに注意してください。空の ACL の場合、アクセス権が明示的に与えられません。したがって、アクセスは暗黙的に拒否されます。ACL を持たないリソースの場合、保護がオブジェクトに割り当てられません。したがって、すべてのアクセス要求が許可されます。

このプロパティを変更するには、auth コマンドまたは auth- コマンドを使用します。

OWNER

リソースの所有者として指定されているユーザまたはグループ。

このプロパティを変更するには、chres コマンドおよび editres コマンドで owner パラメータを使用します。

変更できないプロパティ

FILE_SYSTEM

ファイル システム(FAT または NTFS など)を指定する名前。

FREE_SPACE

ディスクの空き領域の合計容量(KB 単位)。

GID

指定したディスクのプライマリ グループ情報。

LABEL

指定したボリュームの名前。

LINK_NUMB

リンク数を示します。NTFS 以外のファイル システムの場合、このプロパティは常に 1 です。

TYPE

リムーバブル、固定、CD-ROM、RAM ディスク、またはネットワーク ドライブからディスクのタイプを示します。

USED_SPACE

ディスクの使用領域の合計容量(KB 単位)。

ATIME

レコードが最後にアクセスされた日時。

CTIME

作成時間。

MTIME

レコードが最後に変更された日時。

SACL

Windows システム アクセス制御リストは監査ディレクティブを示します。

DOMAIN クラス

DOMAIN クラスの各レコードは、共通のデータベースとセキュリティ ポリシー(ドメイン)を共有するコンピュータの集合を定義します。ドメインによって、ドメイン管理者が一元管理するユーザ アカウントとグループ アカウントへのアクセスが可能になります。各ドメインには一意の名前があります。

注: eTrust Access Control を使用して、DOMAIN クラスに新しいオブジェクトを作成することはできません。

DOMAIN レコードのキーは、ドメイン名です。DOMAIN クラスのレコードの変更できるプロパティについて以下に説明します。

変更可能なプロパティ

COMPUTERS

指定したドメインのメンバであるコンピュータを示します。

このプロパティを変更するには、chres コマンドまたは editres コマンドで computer パラメータまたは computer- パラメータを使用します。

DOMAIN_NAME

ドメイン名を定義します。

TRUSTED

信頼される側のドメインおよび信頼する側のドメインを示します。

信頼関係は、パス スルー認証を許可するドメイン間のリンクです。パス スルー認証では、信頼する側のドメインが信頼される側のドメインのログイン認証を認めます。信頼関係を結ぶと、1 つのドメイン内に 1 つのユーザ アカウントのみを持つユーザがネットワーク全体にアクセスできる場合があります。信頼される側のドメインの権限で定義されるユーザ アカウントとグローバル グループ、および信頼する側のドメイン内のリソース アクセス許可を提供できます。これは、これらのアカウントが、信頼する側のドメインのディレクトリ データベースに存在しない場合でも同様です。

このプロパティを変更するには、chres コマンドまたは editres コマンドで trusted パラメータまたは trusting- パラメータを使用します。このコマンドにはパスワードを指定する必要があります。

TRUSTING

Trusting ドメインとは、ターゲット ドメインを信頼するドメインです。

変更できないプロパティ

DOMAIN_USERS

指定したドメインのメンバであるユーザ アカウントおよびグループ アカウントを示します。

PDC

ドメイン内で最初に作成したコンピュータの名前。つまり、このコンピュータにはドメイン データのプライマリ格納域が含まれています。このコンピュータによって、ドメイン ログインが認証され、ドメインのディレクトリ データベースが保守されます。プライマリ ドメイン コントローラ(PDC)は、ドメイン上のすべてのコンピュータのアカウントに対して行われた変更を追跡します。これらの変更を直接受け取るのは、このコンピュータのみです。1 つのドメインには PDC が 1 つだけ存在します。

BDC

ドメインのディレクトリ データベースのコピーを受け取り、ドメインのすべてのアカウント情報とセキュリティ ポリシー情報が含まれているコンピュータの名前。コピーは、プライマリ ドメイン コントローラ(PDC)上のマスタ コピーと定期的かつ自動的に同期されます。バックアップ ドメイン コントローラ(BDC)も、ユーザ ログインを認証します。また、BDC は、必要に応じて PDC として機能することができます。1 つのドメインに複数の BDC を使用できます。

FILE クラス

FILE クラスの各レコードは、ファイル システム（FAT、NTFS、CDFS など）上のコンピュータの物理ドライブまたは論理ドライブを定義します。

注: eTrust Access Control を使用して、ディスク上に物理的にファイルを作成することはできません。

FILE クラスのレコードのキーは、レコードが保護するファイルまたはディレクトリの名前です。完全パスを指定する必要があります。FILE クラスのレコードの変更できるプロパティについて以下に説明します。

変更可能なプロパティ

DACL

標準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とグループの名前、およびユーザまたはグループごとに与えられたアクセス権のレベルが登録されています。

このプロパティを変更するユーザは、リソースの所有者であるか、またはリソースへの特別なアクセス権（ACL を変更する権限）を持っている必要があります。

注: FAT または FAT32 ファイル システムに存在するファイルに対してアクセス権を与えることはできません。

アクセス制御リストの各要素には、以下の情報が含まれています。

アクセス タイプ

リソースへのアクセス許可を示します。

- Allowed - リソースへの特別なアクセスを許可します。
- Denied - リソースへの特別なアクセスを許可しない。

アクセサ

アクセスが許可または許可されないユーザまたはグループの名前です。

アクセス

アクセサに与えられる、リソースに対するアクセス権限。FILE クラスの有効なアクセス権限は、以下のとおりです。

- all - クラスに許可できるすべての操作を許可または許可しません。
- changeperm - リソースの ACL の変更をアクセサに許可または許可しません。
- chmod - リソースの削除以外のすべての操作を許可または許可しません。
- chown - リソースの所有者の変更をアクセサに許可または許可しません。
- delete - リソースの削除をアクセサに許可または許可しません。

- execute - プログラムの実行を許可または許可しません。このアクセス タイプを使用するには、読み取りアクセス権限も必要です。
- read - ファイルまたはディレクトリを変更せずに、ファイルまたはディレクトリを使用することをアクセサに許可または許可しません。
- write - ファイルまたはディレクトリの変更をアクセサに許可または拒否します。
- update - read、write、および execute を組み合わせたアクセス権を許可または許可しません。

注: 空の ACL(エントリのない ACL)と ACL を持たないリソースの違いに注意してください。空の ACL の場合、アクセス権が明示的に与えられません。したがって、アクセスは暗黙的に拒否されます。ACL を持たないリソースの場合、保護がオブジェクトに割り当てられません。したがって、すべてのアクセス要求が許可されます。

このプロパティを変更するには、auth コマンドまたは auth- コマンドを使用します。

OWNER

リソースの所有者として指定されているユーザまたはグループ。

このプロパティを変更するには、chres コマンドおよび editres コマンドで owner パラメータを使用します。

変更できないプロパティ

ATTRIB

ファイルまたはディレクトリの属性を示します。以下の 1 つまたは複数の属性を指定できます。

- ARCHIVE
- COMPRESSED
- DIRECTORY
- HIDDEN
- NORMAL
- OFFLINE
- READONLY
- SYSTEM
- TEMPORARY

DEV

ファイルが存在するボリュームのシリアル番号。

ISDIR

ファイルがディレクトリかどうかを示します。

FILE_SYSTEM

ファイルが存在するファイル システムの名前。

INDEX

ファイルに関連付けられた一意の ID を示します。

ATIME

ファイルが最後にアクセスされた日時。

MTIME

ファイルが最後に変更された日時。

LINKS_NUMB

ファイルへのリンク数を示します。FAT ファイル システムの場合、このプロパティは常に 1 です。NTFS ファイル システムの場合、このプロパティは 2 以上です。

GID

ファイルのプライマリ グローバル グループの名前。

SIZE

ファイルのサイズ(バイト単位)。

CTIME

作成時間。

NAME

ファイル名。

SACL

Windows システム アクセス制御リストは監査ディレクティブを示します。

OU クラス

OU(組織単位)クラスには、ユーザ、グループ、コンピュータなどのオブジェクトが含まれます。OU クラスのオブジェクトは、プライマリ ドメイン コントローラ上で作成でき、子オブジェクトとして他のオブジェクト(グループなど)を持つことができます。したがって、OU クラスのオブジェクトはコンテナ オブジェクトです。

注: このクラスは、Active Directory がインストールされている Windows 2000 Advanced Server 端末でのみ使用できます。その他の構成のコンピュータで eTrust Access Control を実行している場合は、このクラスを適用できません。

ユーザまたはグループの管理

OU クラスを使用すると、USER、GROUP、および COMPUTER の 3 つのタイプのオブジェクトを管理できます。つまり、OU クラスを使用してこれらのオブジェクトのプロパティを作成、削除、および更新できます。

新しいユーザを作成するには nu(*username*)コマンドを使用できますが、OU クラスを使用してユーザを作成すると、指定した OU にユーザを簡単に作成できます。

このクラスのオブジェクトを変更するには、以下のように、newres コマンド、rmres コマンド、または chgres コマンドで OU パラメータを使用します。

```
nr OU OU name type(USER) name(creatingUserName)
rr OU OU name type(GROUP) name(existingGroupName)
cr OU OU name type(GROUP) name(existingGroupName) gen_prop(propertyName)
gen_val(propertyValue)
```

注: COMPUTER クラスの一般的なプロパティは変更できません。

指定した OU の既存のプロパティを参照するか、または指定した OU とその子 OU オブジェクトに存在するすべてのユーザ、グループ、およびコンピュータを参照するには、以下のコマンドを入力します。

```
sr OU OU name
```

プロパティ

OU クラスには、事前に定義されたプロパティがありません(他のクラスには事前に定義されたプロパティがあります)。ただし、以下の OU のプロパティを更新できます。

- Country/Region
- Description
- Desktop
- City
- Display Name
- Folder(読み取り専用プロパティ)
- Fax number
- Managed objects(読み取り専用プロパティ)
- Member of(読み取り専用プロパティ)
- Name(読み取り専用プロパティ)
- Postal address
- Postal code
- P.O. box
- State/Province
- Street
- Telephone
- Object changed(読み取り専用プロパティ)
- Object created(読み取り専用プロパティ)
- Web page

PRINTER クラス

PRINTER クラスの各レコードは、メディア上にビジュアル イメージを再現できる、Windows コンピュータ システムに接続されているデバイス(PRINTERS フォルダに表示されます)を定義します。

注: eTrust Access Control を使用して、PRINTER クラスの新しいオブジェクトを作成することはできません。

PRINTER クラスのレコードのキーは、ローカル プリンタの名前です。PRINTER クラスのレコードで変更できるプロパティについて以下に説明します。

変更可能なプロパティ

DACL

標準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とグループの名前、およびユーザまたはグループごとに与えられたアクセス権のレベルが登録されています。

このプロパティを変更するユーザは、リソースの所有者であるか、またはリソースへの特別なアクセス権(ACL を変更する権限)を持っている必要があります。

アクセス制御リストの各要素には、以下の情報が含まれています。

アクセス タイプ

リソースへのアクセス許可を示します。

- Allowed - リソースへの特別なアクセスを許可します。
- Denied - リソースへの特別なアクセスを許可しない。

アクセサ

アクセスが許可または許可されないユーザまたはグループの名前です。

アクセス

アクセサに与えられる、リソースに対するアクセス権限。PRINTER クラスの有効なアクセス権限は、以下のとおりです。

- all - クラスに許可できるすべての操作を許可または許可しません。
- manage - 指定したプリンタに対するデータ設定、印刷の一時停止、印刷の再開、すべての印刷ジョブのクリア、ACL の更新、プリンタのプロパティの変更など、プリンタでの管理操作の実行をアクセサに許可または許可しません。
- print - 印刷オプションを許可または許可しません。

注: 空の ACL(エントリのない ACL)と ACL を持たないリソースの違いに注意してください。空の ACL の場合、アクセス権が明示的に与えられません。したがって、アクセスは暗黙的に拒否されます。ACL を持たないリソースの場合、保護がオブジェクトに割り当てられません。したがって、すべてのアクセス要求が許可されます。

このプロパティを変更するには、auth コマンドまたは auth- コマンドを使用します。

COMMENT

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。この情報が eTrust Access Control による権限付与に使用されることはありません。

このプロパティを変更するには、chres コマンドまたは editres コマンドで comment パラメータまたは comment- パラメータを使用します。

LOCATION

プリンタの場所を示す文字列。この情報が eTrust Access Control による権限付与に使用されることはありません。

このプロパティを変更するには、chres コマンドまたは editres コマンドで location パラメータを使用します。このプロパティを削除するには、空白の ( ) を使用します。

OWNER

リソースの所有者として指定されているユーザまたはグループ。

このプロパティを変更するには、chres コマンドおよび editres コマンドで owner パラメータを使用します。

SHARE

プリンタの共有ポイントを識別する名前。プリンタにアクセスするユーザまたはグループは、その共有名を使用できます。

このプロパティを変更するには、chres コマンドまたは editres コマンドで share_name パラメータまたは share_name- パラメータを使用します。

NAME

プリンタ名。

SACL

Windows システム アクセス制御リストは監査ディレクティブを示します。

変更できないプロパティ

SERVER

プリンタを制御するサーバを識別する文字列。このプロパティが存在しない場合、プリンタはローカルで制御されます。

PROCESS クラス

PROCESS クラスの各レコードは、実行可能プログラム、一連の仮想メモリ アドレス、およびスレッドで構成されている(Windows のタスク マネージャに表示される)オブジェクトを定義します。

このクラスは、Windows ホストでのみ使用できます。eTrust Access Control を使用して、PROCESS クラスに新しいオブジェクトを作成することはできません。

PROCESS クラスのレコードのキーは、実行中のプログラムの実行可能モジュールの名前です。

注: PROCESS クラスのレコードには、変更可能なプロパティはありません。

変更できないプロパティ

PROCESS_ID

プロセスの一意の ID。プロセス ID 番号は再利用されるため、そのプロセスの有効期間のみプロセスが識別されます。

IMAGE_PATH

指定した実行可能モジュールの完全修飾パス。

REGKEY クラス

REGKEY クラスの各レコードは、Windows の環境設定情報が保存されているレジストリのキーのツリー構造を定義します。

REGKEY レコードのキーは、レジストリ キーの完全パスです。REGKEY クラスのレコードで変更できるプロパティについて以下に説明します。

注: ファイル名パターンの一部としてワイルドカードを使用できます。ワイルドカードは、「*」(0 個以上の文字)および「?」(任意の 1 文字)です。

変更可能なプロパティ

DACL

標準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とグループの名前、およびユーザまたはグループごとに与えられたアクセス権のレベルが登録されています。

このプロパティを変更するユーザは、リソースの所有者であるか、またはリソースへの特別なアクセス権(ACL を変更する権限)を持っている必要があります。

アクセス制御リストの各要素には、以下の情報が含まれています。

アクセス タイプ

リソースへのアクセス許可を示します。

- Allowed - リソースへの特別なアクセスを許可します。
- Denied - リソースへの特別なアクセスを許可しません。

アクセサ

アクセスが許可または許可されないユーザまたはグループの名前です。

アクセス

アクセサに与えられる、リソースに対するアクセス権限。REGKEY クラスの有効なアクセス権限は、以下のとおりです。

- all - アクセサに対して、クラスに許可できるすべての操作の実行を許可または許可しません。
- append/create/subkey - アクセサによるレジストリ キーのサブキーの作成または変更を許可または許可しません。
- changeperm/sec/dac/writedac/perm - アクセサによる ACL の変更(つまりアクセサの追加または削除)を許可または許可しません。
- chown/owner/takeownership - アクセサによるリソースの所有者の変更を許可または許可しません。
- delete - アクセサによるリソースの削除を許可または許可しません。

- enum - アクセサによるレジストリ キーのサブキーの列挙を許可または許可しません。
- link - アクセサによるレジストリ キーへのリンクの作成を許可または許可しません。
- notify - アクセサによるレジストリ キーの変更通知またはレジストリ キーのサブキーの要求を許可または許可しません。
- query - アクセサによるレジストリ キーの値のクエリを許可または許可しません。
- read - アクセサによるキーの内容の読み取りを許可または許可しません。ただし、変更は保存できなくなります。
- readcontrol/manage - アクセサによるレジストリ キーのセキュリティ記述子の情報(システム(監査)アクセス制御リストの情報は含まない)の読み取りを許可または許可しません。
- set - アクセサによるレジストリ キーの値の作成または設定を許可または許可しません。
- write - アクセサによるレジストリ キーとそのサブキーの変更を許可または許可しません。

注: 空の ACL(エントリのない ACL)と ACL を持たないリソースの違いに注意してください。空の ACL の場合、アクセス権が明示的に与えられません。したがって、アクセスは暗黙的に拒否されます。ACL を持たないリソースの場合、保護がオブジェクトに割り当てられません。したがって、すべてのアクセス要求が許可されます。

このプロパティを変更するには、auth コマンドまたは auth- コマンドを使用します。

SACL

Windows システム アクセス制御リストは監査ディレクティブを示します。

OWNER

リソースの所有者として指定されているユーザまたはグループ。

このプロパティを変更するには、newres コマンド、chres コマンド、および editres コマンドで owner パラメータを使用します。

変更できないプロパティ

SUBKEYS

キーの下に存在するレジストリ キー(サブキー)のリスト。

SUBVALUES

現在のレジストリ キーに記述されているレジストリ値のリスト。

REGVAL クラス

REGVAL クラスの各レコードは、レジストリ キーを記述するデータを定義します。このデータは、1 人または複数のユーザ、アプリケーション、およびハードウェア デバイスに関するシステム構成に必要な情報を格納します。レジストリ値には、操作中に頻繁に参照される情報が含まれています。

たとえば、以下のような情報が含まれています。

- 各ユーザのプロファイル
- コンピュータにインストールしたアプリケーションと、各アプリケーションで作成できるファイルのタイプ
- フォルダやアプリケーション アイコンのプロパティ シートの設定
- ハードウェア構成
- 使用されているポート

REGVAL レコードのキーは、レジストリ キーの完全パス名とその値です。

注: レジストリ キーやその値を間違って変更または削除すると、システム全体に影響する重大な問題を引き起こす可能性があり、問題を解決するためには Windows の再インストールが必要になる場合があります。

REGVAL クラスのレコードで変更できるプロパティについて以下に説明します。

変更可能なプロパティ

TYPE

データを格納する形式。レジストリ値にデータを格納するときに、格納するデータの型を示すために以下の値のいずれかを指定できます。

注: レジストリ値を作成または変更するときに、以下のデータ型を指定します。

DWORD

4 バイト長の数値で表されるデータ。このデータ型は、デバイス ドライバおよびサービスに関する多くのパラメータに使用されています。バイナリ、16 進数、または 10 進数の形式で表示できます。

STRING

読み取り可能なテキストを表す一連の文字。

MULTISTRING

複数の文字列。読み取り可能なテキストのリストまたは複数の値が含まれている値。各エントリは、Null 文字で区切られます。

BINARY

生のバイナリ データ。ハードウェア コンポーネントの情報の大部分は、バイナリ データとして格納され、16 進数形式または簡単に読み取れる形式で表示できます。

このプロパティを変更するには、newres コマンド、nechres コマンド、または editres コマンドでパラメータとして上記のデータ型のいずれかを使用します。

VALUE

Windows レジストリ値が保持する値。

SERVICE クラス

SERVICE クラスの各レコードは、Windows のサービス([コントロール パネル]-[サービス]で表示されるサービス)を定義します。

このクラスは、Windows ホストでのみ使用できます。

SERVICE クラスのレコードのキーは、制御されるサービスの名前です。SERVICE クラスのレコードで変更できるプロパティについて以下に説明します。

変更可能なプロパティ

ACCOUNT

サービスのログイン アカウントを変更します。大部分のサービスは、システム アカウントでログインする必要がありますが、特別なユーザ アカウントでログインするように設定できるサービスもあります。詳細については、関連する Microsoft Windows のマニュアルを参照してください。デフォルト値は LocalSystem です。

このプロパティを変更するには、chres コマンドまたは editres コマンドで account パラメータを使用します。

BINARY_NAME

サービスの実行可能ファイルを参照する完全パス。

IMAGEPATH

指定した実行可能モジュールの完全修飾パス。

INTERACTIVE

サービスが開始されている状態のときに、ログインしたすべてのユーザが使用できるユーザ インターフェースをデスクトップに表示します。このインターフェースは、サービスが LocalSystem アカウントとして実行されている場合にのみ使用可能です。

このプロパティを変更するには、chres コマンドまたは editres コマンドで interactive パラメータを使用します。

PROFILE

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。

このプロパティを変更するには、chusr コマンド、editusr コマンド、または newusr コマンドで profile パラメータを使用します。

REG_KEY

このプロパティは、Windows レジストリのサービス定義の場所を示します。

STARTUPTYPE

サービスを開始する方法(また、いつ開始するか)を示します。以下のオプションがあります。

- automatic - システムの起動中に自動的にサービスを開始します。
- disabled - ユーザまたは依存関係にあるサービスによってサービスを開始できないようにします。
- manual - ユーザまたは依存関係にあるサービスによるサービスの開始を許可します。
- このプロパティを変更するには、chres コマンドまたは editres コマンドで starttype パラメータを使用します。

STATUS

現在のサービスの状態を変更します。オプションには、started、stopped、および paused があります。

このプロパティを変更するには、chres コマンドまたは editres コマンドで status パラメータを使用します。

例

SeOSAgent サービスを手動で開始するように変更するには、selang の以下のコマンドを入力します。

```
chres SERVICE “SeosAgent” starttype(manual)
```

Directory Replicator のログイン アカウントを ReplAdmin に変更し、パスワードを *abcde* とするには、selang の以下のコマンドを入力します。

```
chres SERVICE directory replicator account(repladmin) domainpwd(abcde)
```

SESSION クラス

SESSION クラスの各レコードは、ローカル ホスト上のユーザ セッションを定義します。このレコードには、ユーザ名、コンピュータ名、接続経過時間、および使用中のリソースが含まれています。

このクラスは、Windows ホストでのみ使用できます。SESSION クラスのレコードで変更できるプロパティについて以下に説明します。

変更可能なプロパティ

IDLE

サーバとワークステーション間のネットワーク セッションを終了します。

このプロパティを変更するには、chres コマンドまたは editres コマンドで disconnect パラメータを使用します。

CNAME

セッションが確立されたホスト名です。

GUEST

セッションがゲスト アカウントで作成されたかどうかを示します。

OPENS

開いているセッションの数を示します。

RESOURCES

サーバ上の共有ファイルに関する情報を提供するプロパティ。この情報には、開いている共有リソースのパスや、リソースを開いたユーザまたはコンピュータが含まれています。

TIME

セッションが確立されてから経過した時間。

USER

ユーザの相対 ID(RID)が含まれている値。RID は、ユーザの作成時にセキュリティ アカウント マネージャ(SAM)によって決定されます。RID によって、ユーザ アカウントがドメイン内の SAM に対して一意に定義されます。

例

ローカル ホストのセッションからユーザ ZORRO を切断するには、selang の以下のコマンドを入力します。

```
chres SESSION zorro disconnect
```

注: ユーザの接続を切断すると、データが失われる可能性があります。接続を切断する前に、ユーザに警告することをお勧めします。

SHARE クラス

SHARE クラスの各レコードは、複数のデバイスまたはプログラムによって使用されるデバイス、データ、プログラムなどの共有リソースを定義します。Windows の場合、共有リソースとは、ディレクトリ、ファイル、プリンタ、名前付きパイプなど、ネットワーク ユーザが使用可能な任意のリソースを指します。また、共有はネットワーク ユーザが使用可能なサーバ上のリソースも指します。

SHARE クラスのレコードのキーは、リソースの共有名です。SHARE クラスのレコードで変更できるプロパティについて以下に説明します。

変更可能なプロパティ

DACL

標準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、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。

このプロパティを変更するユーザは、リソースの所有者であるか、またはリソースへの特別なアクセス権（ACL を変更する権限）を持っている必要があります。

アクセス制御リストの各要素には、以下の情報が含まれています。

アクセス タイプ

リソースに以下のアクセス許可を指定します。

- Allowed - リソースへの特別なアクセスを許可することを示します。
- Denied - リソースへの特別なアクセスを拒否することを示します。

アクセサ

アクセスが許可または許可されないユーザまたはグループの名前です。

アクセス

アクセサに与えられる、リソースに対するアクセス権限。PRINTER クラスの有効なアクセス権限は、以下のとおりです。

- all - アクセサに対して、クラスに許可できるすべての操作の実行を許可または許可しません。
- read - アクセサによるリソースの共有プロパティの読み取りを許可または許可しません。
- change - アクセサによるリソースの共有プロパティの変更、またはリソースからの共有の削除を許可または許可しません。

このプロパティを変更するには、auth コマンドまたは auth- コマンドを使用します。

MAX_USERS

共有リソースに対して可能な最大同時接続数。

注: このプロパティの値としてゼロ(0)を指定することはできません。ゼロを指定すると、Windows によって無視されます。

このプロパティを変更するには、newres コマンド、chres コマンド、または editres コマンドで max_users パラメータを使用します。

NAME

共有の名前を示します。

PATH

共有リソースのローカル パスを指定する文字列。ディスクの場合、これは共有になっているパスです。印刷キューの場合、これは共有になっている印刷キューの名前です。

このプロパティを変更するには、newres コマンド、chres コマンド、または editres コマンドで path パラメータを使用します。

REMARK

レコードに含める追加情報です。この文字列には、255 文字までの英数字を指定できます。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。

このプロパティを変更するには、newres コマンド、chres コマンド、および editres コマンドで comment パラメータまたは comment- パラメータを使用します。

変更できないプロパティ

CURR_USERS

リソースへの現在の接続数。

PERMISSION

共有レベルのセキュリティで実行しているサーバに対する共有リソースのアクセス許可を示す値。このプロパティは、以下の表に示す値のいずれかです。

ACCESS_READ

リソースのデータを読み取り、デフォルトで実行できます。

ACCESS_WRITE

リソースへのデータの書き込みができます。

ACCESS_CREATE

リソース(ファイルなど)のインスタンスを作成できます。つまり、リソースを作成したら、そのリソースにデータを書き込むことができます。

ACCESS_EXEC

リソースを実行できます。

ACCESS_DELETE

リソースを削除できます。

ACCESS_ATRIB

リソースの属性(ファイルを最後に変更した日時など)を変更できます。

ACCESS_PERM

ユーザまたはアプリケーションのリソースに割り当てられたアクセス許可(読み取り、書き込み、作成、実行、および削除)を変更できます。

ACCESS_ALL

リソースの読み取り、書き込み、作成、実行、および削除ができ、リソースの属性およびアクセス許可を変更できます。

ACCESS_NONE

アクセス許可を与えません。

RESOURCES

サーバ上の共有ファイルに関する情報を提供するプロパティ。この情報には、開いている共有リソースのパスや、リソースを開いたユーザまたはコンピュータが含まれます。

TYPE

共有のタイプです。共有リソースには、以下のタイプのいずれかを使用します。

- ファイル フォルダ - ディスク ドライブ。これには、サーバのリモート管理(ADMIN$)や、C$、D$ などの管理共有も使用できます。
- 印刷キュー - 印刷キュー。
- 通信デバイス - 通信デバイス。
- プロセス間通信(IPC)- プロセス間通信(IPC$)用に予約された特別な共有。

USERS

- 共有リソースに現在アクセス中のユーザに関する情報。この情報には、接続を確立したユーザの名前(USER)、サーバの共有リソースの共有名、またはクライアントのコンピュータ名(MACHINE)が含まれます。また、接続が確立されている秒数(TIME)、および接続の結果として現在開いているファイル数(INUSE)も含まれます。

付録 A: Windows の値

このセクションには、以下のトピックが含まれます。

Windows のファイル属性

chfile コマンドまたは editfile コマンドを使用してファイルに属性を割り当てることができます。属性によってファイルの特性が決まります。これらのコマンドの詳細については、このマニュアルの「Windows 環境の selang のコマンド」の章の chfile/editfile の説明を参照してください。

注: これらのファイル属性の完全名は FILE_ATTRIBUTE_name ですが、eTrust AC で入力する必要があるのは、*name* の部分（ARCHIVE や COMPRESSED など）のみです。

Windows で変更できないファイル属性とその説明を以下に示します。

FILE_ATTRIBUTE_ARCHIVE

バックアップ対象または削除対象としてマークが付けられたアーカイブ ファイル。

FILE_ATTRIBUTE_HIDDEN

隠しファイル。通常、隠しファイルは標準ディレクトリの内容一覧に含まれません。

FILE_ATTRIBUTE_NORMAL

他の属性がないファイル。この値は、単独で使用した場合にのみ有効です。

FILE_ATTRIBUTE_READONLY

読み取り-専用ファイル。アプリケーションで読み取りはできますが、書き込みまたは削除はできません。

FILE_ATTRIBUTE_SYSTEM

オペレーティング システム ファイルまたはオペレーティング システムのみが使用するファイル。

FILE_ATTRIBUTE_TEMPORARY

一時的な保存に使用されているファイル。

Windows で変更できないファイル属性とその説明を以下に示します。

FILE_ATTRIBUTE_COMPRESSED

圧縮ファイルまたは圧縮ディレクトリ。ファイルの場合は、ファイル内のすべてのデータが圧縮されていることを示します。ディレクトリの場合は、新規に作成されたすべてのファイルおよびサブディレクトリがデフォルトで圧縮されていることを示します。

FILE_ATTRIBUTE_DIRECTORY

ディレクトリ。

Windows のアカウント フラグ

chusr コマンド、editusr コマンド、および newusr コマンドを使用すると、ユーザのアカウントにフラグを割り当てることによって、アカウントの特定の属性を指定できます。各アカウントに複数のフラグを適用できます。これらのコマンドの詳細については、このマニュアルの「Windows 環境の selang のコマンド」の章の chusr/editusr/newusr の説明を参照してください。

注: eTrust AC では、フラグの完全名を入力する必要はありません。以下の表に示すショートカットを使用できます。

Windows で使用できるアカウント フラグは以下のとおりです。

ショートカット	フラグ	説明
blank	UF_PASSWRD_NOTREQD	ユーザのアカウントにパスワードが不要なことを示します。
cant_change	UF_PASSWORD_CANT_CHANGE	アカウントのパスワードをユーザが変更できないことを示します。
disable	UF_ACCOUNTDISABLE	ユーザのアカウントが無効であることを示します。
dont_expire	UF_DONT_EXPIRE_PASSWORD	このアカウントのパスワードが失効しないことを示します。
homedir	UF_HOMEDIR_REQUIRED	ホーム ディレクトリが必要なことを示します。Windows ではこの値は無視されます。
interdomain	UF_INTERDOMAIN_TRUST_ACCOUNT	アカウントを信頼するための許可を示します。
lockout	UF_LOCKOUT	ユーザのアカウントが現在ロックアウトされていることを示します。ロックアウトを解除するには、このフラグを削除します。
normal	UF_NORMAL_ACCOUNT	通常のユーザを表すデフォルトのアカウント タイプを示します。
notreq	UF_PASSWRD_NOTREQD	ユーザのアカウントにパスワードが不要なことを示します。
protect	UF_PASSWORD_CANT_CHANGE	アカウントのパスワードをユーザが変更できないことを示します。

ショートカット	フラグ	説明
script	UF_SCRIPT	ユーザがアプリケーションを起動したときに、ディスク マッピングを実行するログイン スクリプトがアクティブになることを示します。LAN Manager 2.0 または Windows では、このフラグを設定する必要があります。
server	UF_SERVER_TRUST_ACCOUNT	このドメイン内の Windows NT バックアップ ドメイン コントローラのアカウントを示します。
temp	UF_TEMP_DUPLICATE_ACCOUNT	他のドメインにアカウントを持つユーザを示します。このアカウントに対して、そのドメインへのアクセス権を与えますが、このアカウントは信頼できるアカウントではありません。
trust	UF_INTERDOMAIN_TRUST_ACCOUNT	アカウントを信頼するための許可を示します。
workstation	UF_WORKSTATION_TRUST_ACCOUNT	このドメインのメンバであるワークステーションまたはサーバのアカウントを示します。

Windows のアクセス許可

SHARE リソース タイプでは、アクセサに対してアクセス許可を与えることができます。SHARE リソース タイプの詳細については、「Windows 環境のクラスとプロパティ」の章を参照してください。

Windows で使用できるアクセス許可は以下のとおりです。

ACCESS_ALL

リソースの読み取り、書き込み、作成、実行、および削除ができ、リソースの属性およびアクセス許可を変更できます。

ACCESS_ATTRIB

リソースの属性を変更できます。

ACCESS_CREATE

リソースを作成できます（作成時にデータを書き込む許可を含む）。

ACCESS_DELETE

リソースを削除できます。

ACCESS_EXEC

リソースを実行できます。

ACCESS_NONE

アクセス許可がありません。

ACCESS_PERM

ユーザまたはアプリケーションに割り当てられたリソースに対するアクセス許可を変更できます。

ACCESS_READ

リソースのデータを読み取り、デフォルトで実行できます。

ACCESS_WRITE

リソースへのデータの書き込みができます。

Windows の権限

Windows の権限は、個々のユーザ アカウントおよびグループに割り当てることができます。管理者は、chusr コマンドまたは editusr コマンドを使用してユーザに、chgrp コマンドまたは editgrp コマンドを使用してグループに、それぞれ権限を割り当てることができます。グループに追加されたユーザには、そのグループに割り当てられたすべての権限が自動的に与えられます。これらのコマンドに関する詳細については、このマニュアルの「Windows 環境の selang のコマンド」の章を参照してください。

一覧に示されているとおりの権限名（ユーザ権限名）を使用できます。または名前の先頭に Se を、最後に Privilege を追加することもできます（BatchLogon、InteractiveLogon、NetworkLogon、および ServiceLogon は例外で、Privilege の代わりに Right を追加します）。

Windows で使用できる権限は以下のとおりです。

権限	デフォルトの割り当て	説明
AssignPrimaryToken	None	プロセスのセキュリティ アクセス トークンの変更をユーザに許可します。
Audit	None	セキュリティ監査を生成します。
Backup	Administrators Backup Operators	ファイルおよびディレクトリのバックアップをユーザに許可します。この権限はファイルおよびディレクトリのアクセス許可をすべて置き換えます。
BatchLogon	None	バッチ ジョブとしてのログインをユーザに許可します。
ChangeNotify	Everyone	通常、ファイルおよびサブディレクトリへのアクセス権は、上位から下位に向かって設定されます。つまり、特定のディレクトリへのアクセス権がないユーザは、そのディレクトリの下にあるサブディレクトリへのアクセス権も持ちません。しかし、この権限を使用すると、ユーザは親ディレクトリへのアクセス権がない場合でも、サブディレクトリにアクセスできます。
CreatePagefile	None	ページ ファイルの作成をユーザに許可します。セキュリティは、以下のキーに対するユーザのアクセス権によって決定されます。 ¥CurrentControlSet¥Control¥SessionManagement
CreatePermanent	None	¥¥Device などの特別で永続的なオブジェクトの作成をユーザに許可します。

権限	デフォルトの割り当て	説明
CreateToken	None	トークン オブジェクトを作成します。これを実行できるのは Local Security Authority のみです。Local Security Authority は、ユーザがシステムへのアクセスを許可されていることを確認します。この権限の使用を監査することはできません。C2 レベルの認証については、この権限をどのユーザにも割り当てないことをお勧めします。
Debug	Administrator	スレッドなどのプログラムまたはオブジェクトをデバッグします。この権限を監査することはできません。C2 レベルの認証については、システム管理者を含むどのユーザにもこの権限を割り当てないことをお勧めします。
IncreaseBasePriority	Administrators Power Users	プロセスの実行優先順位を上げることをユーザに許可します。
IncreaseQuota	None	オブジェクトのクォータを増やすことをユーザに許可します。
InteractiveLogon	Most groups	対話形式のログインをユーザに許可します。
LoadDriver	Administrators	デバイス ドライバのインストールおよび削除をユーザに許可します。
LockMemory	None	PAGEFILE.SYS などのバッキング ストア ファイルにページが自動的にバックアップされないように、コンピュータのメモリでページをロックすることをユーザに許可します。
MachineAccount	None	ドメインに新しいマシンを追加することをユーザに許可します。
NetworkLogon	Everyone	ユーザがネットワークのどこからでもコンピュータに接続することを許可します。したがって、ユーザは、コンピュータにログインするために特定の場所または特定の端末を使用する必要がありません。
ProfileSingleProcess	Administrators Power Users	ある 1 つのプロセスのパフォーマンスを監視するためにパフォーマンス モニタ ツールを使用することをユーザに許可します。
RemoteShutdownPrivilege	Administrators Power Users	Windows システムのリモートでの停止をユーザに許可します。
Restore	Administrators Backup Operators	バックアップされたファイルおよびディレクトリの復元をユーザに許可します。この権限はファイルおよびディレクトリのアクセス許可をすべて置き換えます。

権限	デフォルトの割り当て	説明
Security	Administrators	監査の対象とするリソース アクセス権の種類(ファイル アクセス権など)を指定すること、またセキュリティ ログを表示および消去することをユーザに許可します。 **注**: この権限は、Windows のユーザ マネージャで［原則］メニューの［監査］コマンドを使用してシステム監査ポリシーを設定することをユーザに許可するものではありません。管理者にはセキュリティ ログを表示および消去する権限が常に与えられます。
ServiceLogon	None	プロセスをサービスとしてシステムに登録できるようにします。
Shutdown	Administrators Backup Operators Everyone Power Users Users	システム コンソールからのシステム停止をユーザに許可します。
SystemEnvironment	Administrators	システム環境変数の変更をユーザに許可します。ユーザは各自のワークステーションでシステム環境を設定できます。また、同じワークステーションで作業する他のすべてのユーザが確実に同じ設定を使用できます。
SystemProfile	Administrators	システムに対するプロファイリング(パフォーマンスのサンプリング)の実行をユーザに許可します。
SystemTime	Administrators Power Users	コンピュータの内部時計の時間設定をユーザに許可します。
TakeOwnership	Administrators	ファイル、ディレクトリ、プリンタ、およびコンピュータ上のその他のオブジェクトの所有者になることをユーザに許可します。この権限は、オブジェクトを保護するすべての許可を置き換えます。
Tcb	None	オペレーティング システムで、安全で信頼できる部分としてプロセスを実行できるようにします。いくつかのサブシステムにこの権限が与えられます。

付録 B: レジストリ キー

このセクションには、以下のトピックが含まれます。

レジストリ ツリー

eTrust AC では、以下のレジストリ キーの下にレジストリ エントリが作成されます。

HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥eTrustAccessControl

レジストリ ツリーには、eTrust AC で使用される以下の環境設定キーとエントリが含まれています。

レジストリ キー	レジストリ エントリ	説明
eTrustAccessControl	CurrentVersion	製品の現在のバージョンとビルド。
	EncryptionPackage	暗号化 DLL の完全パス名。 **デフォルト**: ¥bin¥defenc.dll
current_version		
Agent		Agent キーのエントリ(およびすべてのサブキー)は内部でのみ使用されます。
Client	ConnectTo	クライアントの接続先である eTrust AC サービスがインストールされたホスト名。 **デフォルト**: localhost
Client¥ClientType	ActiveLanguage	ローカライズされたポリシー マネージャで現在使用されている言語。言語名は、ローカライズされたリソースがインストールされているディレクトリ名を表します(たとえば、「ENG」という値は言語リソース DLL が「..¥bin¥ENG」からロードされることを意味します)。
	AC_HelpFileName	eTrust AC のオンライン ヘルプ ファイル名。
	ACMODE	Administrator GUI に対して eTrust AC モードを有効または無効にするための切り替え設定。 **デフォルト**: 1

レジストリ キー	レジストリ エントリ	説明
	AZN_HelpFileAName	eTrust Web Access Control のオンライン ヘルプ ファイル名。
	AZNBARTITLE	AZN 動作モードのタイトル バーの名前。 **デフォルト**: Web AC
	AZNMode	ポリシー マネージャ GUI に対して eTrust Web Access Control モードを有効または無効にするための切り替え設定。 **デフォルト**: 0（eTrust AC インストールの場合）
	CompanyLogoImageFile	企業ロゴ ファイルの完全パス名。 **デフォルト**: ¥Data¥CompanyLogo.bmp
	COMMON_AboutImageFile	複数の製品を管理する際に使用するイメージ ファイルの名前。
	COMMON_HelpFileName	PM を使用して複数の製品を管理する際に使用するオンライン ヘルプ ファイルの名前。
	eAC_AboutImageFile	eTrust AC ABOUT ファイルの完全パス。 **デフォルト**: ¥Data¥eAC_About.bmp
	eAC_AboutMsg	Administrator GUI の[バージョン情報]ダイアログ ボックスに表示されるタイトル。 **デフォルト**: ポリシー マネージャ
	eAC_ApplicationName	Administrator GUI の完全な名前。 **デフォルト**: ポリシー マネージャ
	eAC_WebURL	eTrust AC サイトの URL。 **デフォルト**: www.casupport.jp/resources/etrustac/
	seAMVersion	[ヘルプ]-[バージョン情報]ダイアログ ボックスに表示される情報を設定します。
	SSO_AboutImageFile	[ヘルプ]-[バージョン情報]ダイアログ ボックスに表示される情報を設定します。
	SSO_AboutMsg	[ヘルプ]-[バージョン情報]ダイアログ ボックスに表示される情報を設定します。
	SSO_ApplicationName	eTrust Single Sign-On を管理する際にアプリケーション タイトル名を設定します。

レジストリ キー	レジストリ エントリ	説明
	SSO_CustomUserActionDLL	eTrust Single Sign-On を管理する場合、ユーザのカスタム アクションはメニューを使用して実行することができます。この値はカスタム アクションで DLL を設定します。
	SSO_MailTo	[ヘルプ]-[バージョン情報]ダイアログ ボックスに表示される情報を設定します。
	SSO_WebURL	[ヘルプ]-[バージョン情報]ダイアログ ボックスに表示される情報を設定します。
	SSOMODE	eTrust Single Sign-On を管理するための PM の操作モードを示します(AZNMode および ACMode と同じ)。
	WAC_GenericResources	eTrust WAC GUI で包括的なリソース サブ ツリーを有効または無効にするための切り替え設定。 **デフォルト**: 0
	WAC_AboutImageFile	eTrust AC ABOUT ファイルの完全パス。 **デフォルト**: ¥Data¥WAC_About.bmp
	WAC_AboutMsg	eTrust AC Administrator GUI の[バージョン情報]ダイアログ ボックスに表示されるタイトル。 **デフォルト**: ポリシー マネージャ
	WAC_ApplicationName	eTrust WAC 用 Administrator GUI アプリケーションのフル ネーム。 **デフォルト**: ポリシー マネージャ
	WAC_MailTo	eTrust WAC のサポートの電子メール アドレス。
	WAC_WebURL	eTrust AC サイトの URL。 **デフォルト**: www.casupport.jp/resources/etrustac/
	WS_AboutImageFile	[ヘルプ]-[バージョン情報]ダイアログ ボックスに表示される情報を設定します。
	WS_AboutMsg	[ヘルプ]-[バージョン情報]ダイアログ ボックスに表示される情報を設定します。
	WS_ApplicationName	現在は使用されていません。
	WS_MailTo	[ヘルプ]-[バージョン情報]ダイアログ ボックスに表示される情報を設定します。

レジストリ キー	レジストリ エントリ	説明
	WS_WebURL	[ヘルプ]-[バージョン情報]ダイアログ ボックスに表示される情報を設定します。
	WS_Mode	現在は使用されていません。
Client¥Standalone	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、eTrust AC 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
Dependency		eTrust AC 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 eTrust AC に依存する製品の名前になります。eTrust AC をアップグレードまたはアンインストールする場合、eTrust AC 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。 **デフォルト**: サブキーなし
devcalc	dms_command_retry_interval	DMS 通知コマンドの再試行間隔を秒数で示します。 **デフォルト**: 60
	init_ac_db	インストール プログラムによって作成された初期 eTrust AC データベースへのパスを示します。 **デフォルト**: *<eAC_Install_Dir>*¥data¥devcalc¥init_ac_db
	max_dms_command_retry	DMS 通知コマンドの再試行の最大回数を示します。 **デフォルト**: 3
	max_lines_request	get devcalc selang コマンドで返される偏差データの行数を示します。 **デフォルト**: 50

レジストリ キー	レジストリ エントリ	説明
eTrustAccessControl	admin_default_check	旧バージョンとの互換性のために使用されます。 この値が 1 に設定されている場合は、リモート端末リソースの DEFACCESS プロパティが ALL に設定されていても、eTrust AC は eTrust AC サーバへのログイン アクセスを拒否されます。 **デフォルト**: 0
	AdminInst	CA 社内用途のみ。
	auth_login	eTrust 管理上の目的でユーザを認証する方法を決定します。有効な値は以下のとおりです。 「native」- ネイティブ オペレーティング システムのユーザの場合、OS に対してユーザ パスワードをチェックします。 「eTrust」- ネイティブ オペレーティング システムに存在しないユーザの場合、eTrust AC データベースに対してパスワードをチェックします。 **デフォルト**: native
	auth_module_names	ネイティブの認証以外で認証を許可され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、認証の前に lca API コール内で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 モードで認証を行うその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 eTrust AC 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

レジストリ キー	レジストリ エントリ	説明
	eACPipeTranslator	古いパイプ名を使用する古いクライアントと新しいパイプ名を使用する新しいサーバとの間でアダプタとして動作するプログラム。この実行可能プログラムは、seosd に対して、およびパイプ サーバとして動作するすべての Policy Model に対して起動されます(このファイルは bin ディレクトリに配置する必要があります)。 デフォルト値はありません。
	Emulate	CA 社内用途のみ。この値は常に 0 である必要があります。 **デフォルト**: 0
	EnableNetworkRegScan	TCPIP に依存するすべてのサービスを seosdrv.sys に依存するように設定するために、SeOSWatchdog サービス ネットワーク スキャンを有効または無効にするための切り替え設定。 **デフォルト**: 1
	eTrustAccessControlServices	eTrust AC サービスのリスト。 **デフォルト**: SeOSAgent; SeOS Agent SeSudo; SeOS TDseoswd; SeOS Watchdog
	full_year	secons -tv、seaudit、および dbmgr ユーティリティを使用する場合に、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)を指定するキー。 **デフォルト**: yes

レジストリ キー	レジストリ エントリ	説明
	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。 このキーを変更しないと、ワークステーションはどの Policy Model Database からの更新も受け付けません。このキーを _NO_MASTER_ に設定すると、すべての Policy Model Database でこのワークステーションを更新できます。 デフォルト値はありません。 **注**: STOP が有効な場合にブローカ（STOPSignatureBrokerName エントリ）を指定しないと、親 Policy Model がブローカとして使用されます。
	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と、parent_pmd レジストリ キーの値が継承されます。 デフォルト値はありません。
	ReverseIpLookup	ユーザが端末からのログオンを許可されているかどうかを判断するために、クライアント 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、それに応じてログオンが許可されます。 no- ホスト名は解決せずに、クライアントから受け取ったホスト名を使用します（TERMINAL クラスを無効にしても同じ効果があります)。 **デフォルト**: yes

レジストリ キー	レジストリ エントリ	説明
	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 Database。 デフォルト値はありません。
	SeOSPath	eTrust AC のインストール ディレクトリ。
	SplashEnable	対話形式(GINA)のログオン 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、eTrust 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。 **デフォルト**: 0
	TrustedServices	Trusted プログラムのリスト。 デフォルト値はありません。
	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。 **デフォルト**: 1
Exits		
Exits¥Authenticate Password	Enable	パスワード ルール実施エージェント exit を有効または無効にするための切り替え設定。値 0 では exit が無効になります。それ以外の値では exit が有効になります。 **デフォルト**: 0

レジストリ キー	レジストリ エントリ	説明
	EnforcePasswordControl	eTrust AC クライアントを使用したパスワード ルール実施の状態。 値 0 は、パスワード ルール実施なしを示します。 値 1 は、一般ユーザが独自のパスワードを変更するときにパスワード ルール実施がアクティブになることを示します。 値 2 は、admin またはパスワード管理者が別のユーザのパスワードまたは自分のパスワードを変更するときにパスワード ルール実施がアクティブになることを示します。 値 3 は、値 1 と 2 を合わせたものを示します。 **デフォルト**: 1
Exits¥Engine	*名前なし*	SeOSEngine が存在することを示すエントリ。
Exits¥Remote Grace Info	DefaultWarningDays	この値は、segrace¥SegraceW ユーティリティのユーザにパスワード失効の警告を表示するデフォルトの日数です。これは、これらのユーティリティの 1 つが適用対象であり、ユーザのパスワードが、レジストリ値で指定された日数よりも少ない日数で失効する場合は、ユーザへの警告メッセージが表示されることを意味します。 **デフォルト**: 7
Exits¥Remote Shutdown	Path	リモート シャットダウン DLL の完全パス名。 **デフォルト**: ¥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	AcceptEmptyDomainLogin	ログイン セキュリティを強化するためのキー。ユーザがドメイン名を指定しないでログインすることを許可しません。 **デフォルト**: 0
	directory	ドライバの場所。 **デフォルト**: <system_drive>¥<Windows_path>¥system32¥drivers

レジストリ キー	レジストリ エントリ	説明
	FileCacheDisabled	汎用ファイル 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。 **デフォルト**: 0
	FileCacheRefreshPeriod	同じソースからの 2 つの監査メッセージ間の最小期間を定義する数値(ミリ秒単位)。 たとえば、この変数を 3000 に設定すると、ファイル監査イベントは最低 3 秒で解決されます。 **デフォルト**: 3000
	QueueTimeout	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。 **デフォルト**: 0
	RegistryCacheRefreshPeriod	同じソースからの 2 つの監査メッセージ間の最低限の期間を定義する数値(ミリ秒単位)。 たとえば、変数を 3000 に設定すると、レジストリ監査イベントは最低 3 秒で解決されます。 **デフォルト**: 3000
	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リスト。 デフォルト値はありません。
	SilentModeEnabled	メンテナンス モードがアクティブ(1)かどうかを示します。 **デフォルト**: 0(無効)
	SystemBypassRestricted	システム プロセスの省略を無効にするためのキー。デフォルトでは、eTrust AC がシステム プロセスを trusted であるとみなします。システム プロセスの省略を有効にするには、このキーをゼロ以外の値に設定します。 **デフォルト**: 0(無効)

レジストリ キー	レジストリ エントリ	説明
lang	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**: ¥data¥help
	HandleHomeDir	ネイティブ ユーザ アカウントの HOME_DIR プロパティが更新されホーム ディレクトリが作成されるかどうかを決定する値。 値を 0 に設定すると、ユーザの HOME_DIR プロパティのみが更新されます。値を 1 に設定するとユーザのプロパティが更新され、さらに、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。
	query_size	データベースへのクエリで一覧表示されるレコードの最大数。 **デフォルト**: 100
	SetBlockRun	Trusted プログラムであるかどうかのチェックを行うかどうかと、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	CA 社内用途のみ。このキーは、常に空である必要があります。
logmgr	audit_back	eTrust AC 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 eTrust AC のみです。 **デフォルト**: ¥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

レジストリ キー	レジストリ エントリ	説明
	audit_log	eTrust AC 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、eTrust AC 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 eTrust AC のみです。 **デフォルト**: ¥log¥seos.audit
	audit_size	eTrust AC の監査ログ ファイルの最大サイズ（KB 単位）。50KB 以上のサイズを指定してください。 **デフォルト**: 1024
	AuditFiltersFile	AC 監査フィルタ ファイルの名前。 **デフォルト**: ¥data¥AuditFilters.flt
	BackUp_Date	eTrust AC がバックアップを実行する基準。no、yes、daily、weekly、および monthly の 5 つの値のいずれかを指定できます。 no を指定すると、eTrust AC は audit_size レジストリ値に従ってバックアップを実行しますが、***その*** ファイルにはタイム スタンプを追加しません。 yes を指定すると、eTrust AC はサイズ制限レジストリ値 audit_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。 daily、weekly、または monthly を指定すると、eTrust AC 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、eTrust AC 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、その前に監査ログ ファイルが audit_size レジストリ値を超えた場合、eTrust AC 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**: no

レジストリ キー	レジストリ エントリ	説明
	error_back	eTrust AC のエラー バックアップ ファイルの名前。 **デフォルト**: 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	eTrust AC 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、eTrust AC 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 eTrust AC のみです。 **デフォルト**: ¥log¥seos.error
	error_size	eTrust AC 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に加えて、既存の PMD の監査イベントをルーティングするかどうかを示します。 「all」- ローカル セキュリティ サービスの監査イベントに加えて、Policy Model の監査イベントをルーティングします。 「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ルーティングします。 **デフォルト**: all
message	filename	eTrust AC 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**: ¥Data¥SeOS.msg
	WACFILENAME	eTrust AC Administrator GUI によって使用されるメッセージ ファイルの名前。 **デフォルト**: WAC.MSG

レジストリ キー	レジストリ エントリ	説明
	WACPATH	eTrust AC Administrator GUI のメッセージ ファイルが格納されるディレクトリ。 **デフォルト**: ¥Data¥
passwd	DefaultPgroup	CA 社内用途のみ。 **デフォルト**: other
	Dictionary	パスワードとして使用できない単語が格納されているファイルの完全パス。 **デフォルト**: ¥Data¥words
	EnforceViaEtrust	eTrust AC 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ためのキー。 **デフォルト**: 0(eTrust AC を使用する必要なし)
	PasswordTimeOut	eTrust AC パスワード フィルタが認証応答を待つ最大時間数(ミリ秒)。 **デフォルト**: 4000
	PasswordTimeOutAnswer	指定されたタイムアウト内に認証プロセスが応答しない場合、回答は LSA に送られます。 これを 0 に設定すると、パスワードの変更は拒否されます。これを 1 に設定すると、パスワードの変更は承認されます。 **デフォルト**: 0
	UseDict	辞書ファイルを使用するかどうかを指定するキー。 **デフォルト**: no
Pmd	_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。 **デフォルト**: ¥data¥
	MaximumPolicyModels	作成できる Policy Model の最大数。 **デフォルト**: 16

レジストリ キー	レジストリ エントリ	説明
	ShutdownWaitingTimeout	コンポーネントが正常にシャットダウンするのをこのコンピュータ上の Policy Model が待つ時間をミリ秒数で示します。Policy Model のコンポーネントがこの時間以内に正常にシャットダウンしない場合は、その Policy Model によって強制的にシャットダウンされます。 **デフォルト**: 60000(1 分)
	TCPReceiveTimeout	このコンピュータ上の Policy Model がサブスクライバからの応答を待つ時間を秒数で示します。Policy Model のサブスクライバがこの時間以内に応答しない場合、Policy Model はそのサブスクライバへの接続を終了します。 **デフォルト**: 0xFFFFFFFF(4294967295 秒、すなわち事実上永久的)
Pmd¥*pmdb_name*	_min_retries_	使用不可のサブスクライバに対する最小アクセス試行回数。アクセス試行がこの回数を超えると、sepmdd は非アクティブ状態になります。 **デフォルト**: 4
	_retry_timeout	使用不可のサブスクライバに連続してアクセスを試みる間隔(分単位)。(UNIX/Linux 専用) **デフォルト**: 30
	_shutoff_time_	sepmdd が非アクティブ状態で待つ時間(分単位)。この時間を過ぎると、sepmdd はサービスを停止します。UNIX/Linux の場合にのみ適用されます。 **デフォルト**: 1
	active_policy	Policy Model 名。
	Always_propagate	エラーが発生した場合に Policy Model がコマンドを伝達するかどうかを制御します。デフォルトでは、Policy Model は常にコマンドを伝達に送ります。このトークンを「no」に設定すると、エラー時にコマンドは送信されません。デフォルトではこのレジストリ値は作成されません。
	Auto_Truncate	更新ファイルから伝達されたエントリの切り捨てを有効または無効にするための切り替え設定。 **デフォルト**: Yes

レジストリ キー	レジストリ エントリ	説明
	Filter	更新ファイルのフィルタ ファイルの完全パス。 デフォルト値はありません。
	parent_pmd	更新の受け付け元の親 PMDB の名前。 デフォルト値はありません。
Pmd¥*pmdb_name*¥ logmgr	audit_back	Policy Model の監査設定。 logmgr レジストリ値の説明を参照してください。
	audit_group	Policy Model の監査設定。 logmgr レジストリ値の説明を参照してください。
	audit_log	Policy Model の監査設定。 logmgr レジストリ値の説明を参照してください。
	audit_size	Policy Model の監査設定。 logmgr レジストリ値の説明を参照してください。
	error_back	Policy Model のエラー設定。 logmgr レジストリ値の説明を参照してください。
	error_group	Policy Model のエラー設定。 logmgr レジストリ値の説明を参照してください。
	error_log	Policy Model のエラー設定。 logmgr レジストリ値の説明を参照してください。
	error_size	Policy Model のエラー設定。 logmgr レジストリ値の説明を参照してください。
Report		
Report¥acc_compare	Class_Name	クラスのリスト。 **デフォルト**: FILE PROGRAM
	HostName	データを取得するホストのリスト。 **デフォルト**: pmdb@localhost
	Object_pattern	オブジェクトの選択パターン(マスク)。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。 **デフォルト**: *

レジストリ キー	レジストリ エントリ	説明
Report¥accessor_report	Accessor	アクセサの選択パターン(マスク)。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。 **デフォルト**: *
	Class_Name	クラスのリスト。 **デフォルト**: PROGRAM FILE TERMINAL CONNECT GSUDO GTERMINAL HOST HOSTNET HOSTNP PROCESS SECLABEL SUDO SURROGATE TCP
	HostName	データを取得するホストのリスト。 **デフォルト**: localhost
	Object_pattern	オブジェクトの選択パターン(マスク)。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。 **デフォルト**: *
Report¥admin_report	HostName	データを取得するホストのリスト。 **デフォルト**: localhost
	Object_pattern	オブジェクトの選択パターン(マスク)。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。 **デフォルト**: *
	User_Mode	カンマで区切られたユーザ モードのリスト。 **デフォルト**: Admin
Report¥colors	background	CA 社内用途のみ。このキーは、変更しないでください。
	class_title	レポートの class_title の色を示します。 **デフォルト**: green
	logo	ロゴを作成します。ロゴは、完全パスで入力する必要があります。 **デフォルト**: ¥data¥logo.jpg
	title	レポートのタイトルの色を示します。 **デフォルト**: midnightblue

レジストリ キー	レジストリ エントリ	説明
Report¥disablelogins_report	HostName	データを取得するホストのリスト。 **デフォルト**: localhost
	Object_pattern	オブジェクトの選択パターン(マスク)。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。 **デフォルト**: *
	Properties	オブジェクトに関連付けられた属性。 **デフォルト**: GRACELOGIN MAXLOGINS INACTIVE SUSPEND_DATE EXPIRE_DATE RESUME_DATE
	User_Mode	カンマで区切られたユーザ モードのリスト。 **デフォルト**: *
Report¥dormant_report	Dormant_account	アカウントが休止状態とみなされる期間。 **デフォルト**: 7
	HostName	データを取得するホストのリスト。 **デフォルト**: localhost
	Object_pattern	オブジェクトの選択パターン(マスク)。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。 **デフォルト**: *
	User_Mode	カンマで区切られたユーザ モードのリスト。 デフォルト: *
Report¥grp_usr_compare	HostName	データを取得するホストのリスト。 **デフォルト**: localhost
	Object_pattern	オブジェクトの選択パターン(マスク)。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。 **デフォルト**: *
Report¥login_report	HostName	データを取得するホストのリスト。 **デフォルト**: localhost

レジストリ キー	レジストリ エントリ	説明
	Object_pattern	オブジェクトの選択パターン(マスク)。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。 **デフォルト**: *
	User_Mode	カンマで区切られたユーザ モードのリスト。 **デフォルト**: *
Report¥passwd_report	Days_to_change	パスワード変更を要求されるまでの残り日数。 **デフォルト**: 7
	HostName	データを取得するホストのリスト。 **デフォルト**: localhost
	Object_pattern	オブジェクトの選択パターン(マスク)。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。 **デフォルト**: *
	User_Mode	カンマで区切られたユーザ モードのリスト。 **デフォルト**: *
Report¥pmdb_compare	Class_Name	クラスのリスト。 **デフォルト**: USER GROUP FILE
	HostName	データを取得するホストのリスト。 **デフォルト**: pmdb@localhost
	Object_pattern	オブジェクトの選択パターン(マスク)。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。 **デフォルト**: *
Report¥res_compare	Class_Name	クラスのリスト。 **デフォルト**: FILE PROGRAM
	HostName	データを取得するホストのリスト。 **デフォルト**: localhost
	Object_pattern	オブジェクトの選択パターン(マスク)。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。 **デフォルト**: *

レジストリ キー	レジストリ エントリ	説明
Report¥untrust_report	HostName	データを取得するホストのリスト。 **デフォルト**: localhost
	Object_pattern	オブジェクトの選択パターン(マスク)。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。 **デフォルト**: *
Report¥usr_compare	HostName	データを取得するホストのリスト。 **デフォルト**: localhost
	Object_pattern	オブジェクトの選択パターン(マスク)。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。 **デフォルト**: *
	Properties	オブジェクトに関連付けられた属性。 **デフォルト**: AUDIT_MODE GROUPS OWNER
Report¥warning_report	Class_Name	クラスのリスト。 **デフォルト**: FILE TERMINAL CONNECT GSUDO GTERMINAL HOST HOSTNET HOSTNP PROCESS PROGRAM SECLABEL SUDO SURROGATE TCP
	HostName	データを取得するホストのリスト。 **デフォルト**: localhost
	Object_pattern	オブジェクトの選択パターン(マスク)。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。 **デフォルト**: *

レジストリ キー	レジストリ エントリ	説明
SeOSD	CreateNewClasses	seclassm ユーティリティを使用して作成した新しいクラスを eTrust AC データベースに追加できるかどうかを指定するキー。 **デフォルト**: yes **注**: 高度なポリシー ベース管理およびレポートを使用する場合は、eTrust AC データベースでクラスを追加または削除するときやクラス プロパティを追加または削除するときに、eTrust AC 初期データベース（init_ac_db）で同じ操作を行う必要があります。このデータベースは、ポリシー偏差計算に使用されます。このデータベースは、init_ac_db レジストリ エントリによって指定されているパスにあります。
	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 eTrust AC データベースに追加できるかどうかを指定するキー。 **デフォルト**: yes **注**: 高度なポリシー ベース管理およびレポートを使用する場合は、eTrust AC データベースでクラスを追加または削除するときやクラス プロパティを追加または削除するときに、eTrust AC 初期データベース（init_ac_db）で同じ操作を行う必要があります。このデータベースは、ポリシー偏差計算に使用されます。このデータベースは、init_ac_db レジストリ エントリによって指定されているパスにあります。
	dbdir	eTrust AC 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**: ¥data¥seosdb
	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、seosd 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、これらの名前を認証できます。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認証に使用します。HOSTNP クラスの場合、seosd は、実際の IP アドレスに解決されるパターンに（このレジストリで列挙された）すべてのドメイン名を一致させます。

レジストリ キー	レジストリ エントリ	説明
	EnablePolicyCache	この値は、認証エンジンでキャッシュされたレコードが使用されるか、データベースからのレコードが直接使用されるかを制御します。 オプション値: no - 認証エンジンではデータベース レコードが使用されます。 yes - 認証エンジンではキャッシュされたレコードが使用されます。 **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 を選択すると、eTrust AC 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 を選択すると、eTrust AC はすべての環境変数の解決を試み、警告メッセージが表示され、オブジェクトが作成されます。 2 を選択すると、eTrust AC 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 を選択すると、eTrust AC 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。
	GraceCountForMessage	[パスワードの変更]ダイアログ ボックスが表示されるまでの猶予ログインの残り回数を示します。 **注**: このエントリは、LogonInterceptionMethod エントリが 1 に設定されている場合にのみ有効です。 **デフォルト**: 0

レジストリ キー	レジストリ エントリ	説明
	HostResolutionRenewal	内部キャッシュの更新の時間。このレジストリ値は、ネットワーク インターセプト認証イベントで使用されます。
	HostResolutionTimeout	ネットワーク インターセプト イベント発生時に、認証エンジンが IP 逆引き参照要求を待つ時間。
	LogonInterceptionMethod	eTrust AC がログオン セキュリティ ポリシーを実施するログオン インターセプト メソッドを制御します。 オプション値: 0 - ログオン インターセプトはカーネル スペース内のドライバによって実行されます。 1 - ログオン インターセプトはユーザ モード スペース内のサブ認証 dll によって実行されます。 **デフォルト**: 0
	MaximumDiscreteFILELimit	eTrust AC データベースに作成できる個別 FILE レコードの数。 最小値をデフォルトにする必要があります。ユーザがこの値をデフォルトよりも小さな値に設定した場合、eTrust AC 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	eTrust AC 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。 最小値をデフォルトにする必要があります。ユーザがこの値をデフォルトよりも小さな値に設定した場合、eTrust AC 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

レジストリ キー	レジストリ エントリ	説明
	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にのみ、この値が適用されます。 この値を 0 に設定すると、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チェックされます。データベースに問題が検出された場合は、データベースは再構築されます。 この値を 1 に設定すると、ヒューリスティックな手順の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整合性チェックに従って再構築されます。 **デフォルト**: 1
	RefreshIPInterval	連続した自動 IP 更新要求の間隔(分単位)。 この値を 0 に設定すると、IP 更新は自動的には実行されません。1 ～ 30 の値を使用すると、eTrust AC は 30 分を使用します。これは値として設定できる最小値です。 **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 -refIP オプションを参照してください。（227 ページ）. **デフォルト**: 0
	ResponseFile	eACOexist.exe ユーティリティで使用する response.ini が保存さている場所。
	TerminalSearchOrder	この値は、認証プロセスでチェックする TERMINAL オブジェクトを認証エンジンで決定する方法を示します。 オプション値: name - 認証エンジンはデータベース内でまず TERMINAL 名を探します。それが見つからない場合は、データベース内で TERMINAL ip を探します。 IP - 認証エンジンはデータベース内でまず TERMINAL ip を探します。それが見つからない場合は、データベース内で TERMINAL 名を探します。 **デフォルト**: name

レジストリ キー	レジストリ エントリ	説明
	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**: ¥Log¥seosd.trace
	trace_file_type	トレース ファイルのタイプです。 トレース ファイルがすでに存在する場合に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作成されます。 **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**: ¥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)。空き容量がこの値を下回ると、eTrust AC ではトレースが無効になります。 **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、eTrust AC はトレース メッセージを生成しません。 file を選択すると、eTrust AC はトレース メッセージを生成し、eTrust AC 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、eTrust AC 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	PgmRest	プログラムのチェックを実行する間隔(秒単位)。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

レジストリ キー	レジストリ エントリ	説明
	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	セキュリティで保護されたファイルのチェックを実行する間隔(秒単位)。 **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	STOPLogFileName	Stack Overflow Protection(STOP)のための動的インシデント データベースの完全パスと名前を示します。 **デフォルト**: *<eAC_InstallDir>*¥Log¥STOPRTEvents.dat
	STOPIniFileName	STOP 初期設定ファイルの完全パスと名前を示します。このファイルには、STOP が有効になっている関数のリストが含まれています。 **デフォルト**: *<eAC_InstallDir>*¥Data¥stop.ini
	STOPLearningModeEnabled	STOP が特殊な ***学習*** モードで実行されるかどうかを示します。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正しく記録されますが、そのまま続行することができます。 **デフォルト**: 0(無効)
	STOPClientTraceEnabled	STOP クライアント モジュールでトレース ログが有効かどうかを示します。 **デフォルト**: 0(無効)
	STOPClientName	STOP クライアント モジュールの完全パスと名前を示します。 **デフォルト**: *<eAC_InstallDir>*¥bin¥detoured.dll

レジストリ キー	レジストリ エントリ	説明
	STOPOperationMode	STOP 実行の状態を示します。有効な値は以下のとおりです。 0 - STOP は無効ですが、ロードされます。 1 - STOP が有効です。 2 - STOP は無効で、ロードされません。 デフォルトは、インストール時に STOP を有効にしたかどうかによって異なります。 **注**: このエントリを値 2 に変更した場合や値 2 から変更した場合は、コンピュータを再起動する必要があります。
	STOPServerTraceEnabled	STOP サーバ モジュールでトレース ログが有効かどうかを示します。 **デフォルト**: 0(無効)
	STOPSignatureFileName	STOP シグネチャ ファイル(trusted インシデント データベース)の完全パスと名前を示します。 **デフォルト**: *<eAC_InstallDir>*¥Data¥stopsignature.dat
	STOPSignatureBrokerName	STOP シグネチャ データベースの取得元として使用するコンピュータのホスト名を示します。 **注**: このエントリが空(デフォルト)のままで、親 Policy Model(parent_pmd)が指定されている場合、STOP シグネチャ データベースはそのホストから取得されます。 デフォルト値はありません。
	STOPUpdateInterval	STOP シグネチャ データベースの更新を連続して 2 回試みる場合の間隔を分単位で示します。 **デフォルト**: 60
	STOPZeroSnapshotBypassEnabled	STOP が、ゼロ サイズのコードのスナップショットのインシデントを許可できるかどうかを示します。 **デフォルト**: 0(許可されません)
	STOPSehHandlingModeDisabled	STOP の SEH ベースの利用の拡張チェックが有効かどうかを示します。 **デフォルト**: 1(無効)

レジストリ キー	レジストリ エントリ	説明
	STOPClientTraceModulePath	STOP クライアント モジュールのトレース ログ モジュールの完全パスと名前を示します。 **デフォルト**: *<eAC_InstallDir>*¥bin¥STOPClientTrace.dll
Tracer	TraceCfgFile	eTrust AC モジュールをトレースするための初期化済み環境設定が含まれているファイルの完全パス。 **デフォルト**: ¥Data¥tracer.ini
	TraceEnabled	トレース メカニズムを有効または無効にするための切り替え設定。 **デフォルト**: 0
UCTNG	EvtManagerServer	Unicenter TNG ホストの名前。
	Integration	Unicenter TNG との統合を有効にし、監査データを送信するための切り替え設定。
	TNG_calendars	カレンダ機能を有効または無効にするための切り替え設定。
	TNG_refresh_interval	カレンダ ステータスを更新する時間間隔。 **デフォルト**: 10

追加レジストリ キー

eTrust AC 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 キー	値名 とタイプ	説明
HKEY_LOCAL_MACHINE¥ SYSTEM¥CurrentControlSet¥ Services¥SeosDrv¥Parameters¥KernelBuffersSize	REG_DWORD	eTrust AC 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 個のバッファが 256 MB の RAM に割り当てられます。各バッファの長さは 4096 バイトです。 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。
HKLM¥SYSTEM¥CurrentControlSet¥SeosDrv¥Parameters¥EnableTMBypass	REG_DWORD	このレジストリ キーは、サード パーティの AV 互換性の問題がある場合に使用できます。 **値**: 1 **注**: このレジストリ キーを変更する前にテクニカル サポートにご連絡ください。詳細については、テクニカル サポートの Web サイト（(http://www.caj.co.jp/support/)）をご覧ください。
HKLM¥SYSTEM¥CurrentControlSet¥SeosDrv¥Parameters¥TMDriverName	REG_SZ	このレジストリ キーは、サード パーティの AV 互換性の問題がある場合に使用できます。 値: <特定のドライバ名> **注**: ドライバの名前は、バージョンごとに異なる可能性があります。このレジストリ キーの正しい値を決定するには、テクニカル サポートに連絡し、インストールする AV ソフトウェアのバージョンをお知らせください。詳細については、テクニカル サポート（http://ca.com/support (http://www.caj.co.jp/support/)）にお問い合わせください。

索引

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

あ

か

さ

た

な

は

ま

や

ら

わ