CA Access Control

トラブルシューティング ガイド

r12.5

第 2 版

サードパーティに関する通知

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

CA 製品リファレンス

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。

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

ドキュメントの表記規則

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

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

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

形式	意味
斜体	ユーザが入力する必要のある情報
角かっこ（[]）で囲まれた文字列	オプションのオペランド

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

例: コマンドの表記規則

以下のコードは、本書でのコマンド表記規則の使用方法を示しています。

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

この例の内容

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

CA への連絡先

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

マニュアルの変更点

第 2 版

第 2 版は r12.5 の GA 版の発表と同時にリリースされました。

この版では、以下のトピックが更新されました。

- ポリシーのデプロイのトラブルシューティング (41 ページ) - この更新されたトピックでは、[復元]オプションに変更が加えられました。

第 1 版

このマニュアルの第 1 版は CA Access Control r12.5 と一緒にリリースされました。 このリリースには、この配布物が追加されました。

目次

第 1 章: 概要

このセクションには、以下のトピックが含まれています。

本書の内容

本書では、CA Access Control Premium Edition に関する一般的な問題の解決策および回避策を示します。

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

本書の対象読者

本書は、CA Access Control によって保護される環境の実装、設定、およびメンテナンスを行うときに発生する問題に対処するセキュリティ管理者およびシステム管理者を対象としています。

第 2 章: CA Access Control エンドポイントおよびサーバ コンポーネントのインストール

このセクションには、以下のトピックが含まれています。

UNIX へのインストール後に CA Access Control が自動的に起動しない

UNIX で有効

症状:

UNIX エンドポイントへのインストール後に CA Access Control が自動的に起動しません。

解決方法:

デフォルトでは、CA Access Control は UNIX エンドポイントでは自動的に起動しません。

UNIX コンピュータの起動時に seosd デーモンが自動的に起動するように設定するには、ACInstallDir/samples/system.init/sub-dir ディレクトリを使用します。sub-dir はご使用のオペレーティング システムに対応したディレクトリです。 各サブディレクトリには、オペレーティング システム上で CA Access Control を自動的に起動する方法を説明した Readme ファイルがあります。

注: CA Access Control の起動の詳細については、「実装ガイド」を参照してください。

CA Access Control サーバ コンポーネントを開けない

症状:

必要なすべての CA Access Control サービスの起動後に、Web ブラウザで CA Access Control エンタープライズ管理、CA Access Control エンドポイント管理、または CA Access Control パスワード マネージャを開くことができません。 同じサーバには JBoss および Oracle をインストールしました。

解決方法:

Oracle と JBoss はどちらもデフォルト ポートの 8080 を使用します。 この問題を修正には、Oracle と JBoss 間のポートの競合を解決する必要があります。 Oracle または JBoss のポートを変更する前に、より簡単に自社に実装できる変更はどちらであるかを検討する必要があります。

デフォルトの JBoss および Oracle ポートを変更するには、以下の手順に従います。

デフォルトのポート番号を変更する方法

1. コマンドウィンドウを開き、以下のディレクトリに移動します(JBossInstallDir は JBoss のインストール ディレクトリ)。

   JBossInstallDir/bin

2. JBoss を停止します。
   - (UNIX) shutdown.bat -S
   - (Windows) shutdown.sh -S
3. テキストエディタで次のファイルを開きます。

   JBossInstallDir/server/default/deploy/jbossweb-tomcat55.sar/server.xml

4. 以下のセクションのポート番号を変更します。

   ```
   <!-- A HTTP/1.1 Connector on port 8080 -->
      <Connector port="8080" address="${jboss.bind.address}"
   ```

5. ファイルを保存して閉じます。
6. テキストエディタで次のファイルを開きます。

   JBossInstallDir/server/default/deploy/httpha-invoker.sar/META-INF/jboss-service.xml

7. 以下の各行のポート番号を変更します。

```
<attribute name="InvokerURLSuffix">:8080/invoker/EJBInvokerServlet</attribute>
<attribute
name="InvokerURLSuffix">:8080/invoker/EJBInvokerHAServlet</attribute>
<attribute name="InvokerURLSuffix">:8080/invoker/JMXInvokerServlet</attribute>
<attribute
name="InvokerURLSuffix">:8080/invoker/readonly/JMXInvokerServlet</attribute>
<attribute
name="InvokerURLSuffix">:8080/invoker/JMXInvokerHAServlet</attribute>
```

8. ファイルを保存して閉じます。
9. JBoss を起動します。
10. (Windows)CA Access Control エンタープライズ管理、CA Access Control エンドポイント管理、CA Access Control パスワード マネージャのショートカットを以下の手順に従って変更します。
    a. [スタート]-[プログラム]-[CA]-[Access Control]をクリックし、該当するショートカットを右クリックします。

       たとえば、CA Access Control エンタープライズ管理 ショートカットを変更するには、[スタート]-[プログラム]-[CA]-[Access Control]を選択し、[エンタープライズ管理]を右クリックします。
    b. [プロパティ]をクリックします。
    c. URL フィールドのポート番号を新しい JBoss ポート番号に変更します。

デフォルトのポート番号を変更する方法

1. SQL コマンド ラインを起動します。
2. sysdba として Oracle に接続します:

```
connect / as sysdba
```

3. HTTP 通信に現在使用されているポートを確認します。

```
select dbms_xdb.gethttpport from dual;
```

4. 目的のポート番号に設定します。

```
exec dbms_xdb.sethttpport('portNumber');
```

5. データベースを停止して再起動します。

```
shutdown immediate
startup
```

Solaris 10 ログ ファイルに記録されたメッセージ

Solaris 10 で有効

症状:

「secons -s」を使用して CA Access Control を停止すると、「/var/adm/messages」ログファイルに記録されている CA Access Control メッセージが Solaris 10 コンピュータに表示されます。 使用しているコンピュータの SEOS_use_streams の値が yes に設定されます。

解決方法:

これらのメッセージは参考メッセージであり、障害またはエラーを示すものではありません。 対処の必要はありません。 メッセージとその意味を以下に示します。

- "SEOS: Restored tcp wput" "SEOS: Restored strrhead rput"

  SEOS_syscall 機能により、ネットワーク フックが無効にされたことを示します。

- "SEOS: Replaced tcp wput" "SEOS: Replaced strrhead rput"

  SEOS_syscall 機能により、ネットワーク フックが有効にされたことを示します。

インストール後に selang に接続できない

症状:

CA Access Control のインストール後に selang を起動するか、CA Access Control データベースに接続しようとすると、以下のエラーが発生します。

エラー: 初期化に失敗しました。終了します。
(localhost)
エラー: ログインできませんでした。
エラー: 端末 example.com からこのサイトを管理する権限がありません。

解決方法:

端末ルールが正しく定義されていません。 端末ルールをトラブルシューティングして問題を特定します。

端末ルールをトラブルシューティングする方法

1. CA Access Control を停止します。

   ```
   secons -s
   ```

2. selang をローカル モードで起動します。

   ```
   selang -l
   ```

   注: UNIX コンピュータ上で selang をローカル モードで実行するには、root ユーザである必要があります。

3. ローカル端末(terminal_name)用の TERMINAL レコードが作成されており、端末のアクセス権限が以下のように正しく定義されていることを確認します。

   ```
   showres TERMINAL terminal_name
   ```

   - レコードが存在しない場合は、ローカル端末用の TERMINAL レコードを作成します。

     ```
     editres TERMINAL terminal_name owner (name) defaccess (accessAuthority)
     ```

     注: 所有者はユーザまたはグループのいずれかです。 TERMINAL レコードに対するデフォルト アクセス権は none であるため、レコードの作成時にデフォルト アクセスを指定して、ユーザが端末からロックアウトされないようにしてください。

   - 端末アクセス権限が正しくない場合は、端末に対する正しいアクセス権限を定義します。

     ```
     authorize TERMINAL terminal_name uid(name) access(accessType)
     ```

4. (UNIX) [seosd] セクション中の terminal_default_ignore 設定の値を確認します。

   この設定値は、管理アクセスを許可するときに、CA Access Control が _default TERMINAL および特定の TERMINAL レコードの defaccess 値を考慮するかどうかを指定します。

   注: terminal_default_ignore 設定の詳細については、「リファレンス ガイド」を参照してください。

5. (UNIX) 以下の手順に従って、lookaside データベースが端末を反映していることを確認します。

   a. ホスト名固有の lookaside データベースを構築します。

      ```
      sebuilda -h
      ```

   b. lookaside データベースの端末エントリとホスト名が同じであることを確認します。

      ```
      sebuilda -H | grep hostname
      ```

      hosts lookaside データベース ファイルの内容が一覧表示されます。

6. CA Access Control を起動します。
   - （UNIX） seload
   - （Windows） seosd -start

注: これでもなお selang を起動できないか、または CA Access Control データベースに接続できない場合は、ご使用の OS 用の hosts ファイルの変更が必要な場合があります。 システム管理者またはネットワーク管理者に連絡してサポートを受けてください。

アンインストール中に手動でレジストリ キーを削除するときにエラーが発生する

Windows で有効

症状:

CA Access Control のアンインストール中にレジストリ キーを削除しようとすると、以下のエラー メッセージが表示されます。
データを開けません。キーを開こうとしてエラーが発生しました。

解決方法:

RemoveAC.exe ユーティリティを実行して CA Access Control レジストリ キーおよびディレクトリを削除します。 RemoveAC.exe ユーティリティでは製品はアンインストールされませんが、すべての CA Access Control レジストリ キーおよびディレクトリがコンピュータから削除されます。

注: RemoveAC.exe ユーティリティは、CA Access Control インストール パッケージには含まれていません。 詳細については、テクニカル サポート（http://ca.com/jp/support）にお問い合わせください。

InfoView に表示される「NULL ページ」エラー

症状:

CA Access Control レポートへのアクセスを試みると、InfoView に次のエラーが表示されます。

NULL ページ: レポート ソースからページを作成できません。

解決方法:

Windows の場合、CA Access Control Universe が適切に定義されていないか、またはインストールされていない場合があります。 CA Access ControlUniverse 用の接続をテストします。 接続が正常ではない場合は接続を編集し、正常である場合は接続を置き換えます。

Solaris の場合、bouser としてログインし、CASHCOMP/CommonReporting/bobje/setup/env.sh を以下のとおり編集します。

1. 以下の LIBRARYPATH を追加します。

   ```
   $MWHOME/lib-sunos5_optimized
   ```

2. BusinessObjects サービスを再起動します。

   ```
   cd$CASHCOMP/CommonReporting/bobje
   ./stopservers
   ./startservers
   ```

第 3 章: ポリシーおよびアクセス権限の作成

このセクションには、以下のトピックが含まれています。

保護されたリソースにユーザがアクセスできる

症状:

あるリソースのデフォルト アクセス権限として none を作成しましたが、スーパーユーザが今までどおりそのリソースにアクセスできます。

解決方法:

リソース アクセスに関する問題のトラブルシューティングを行います (60 ページ)。

読み取りアクセス チェックで /etc/passwd および /etc/group ファイルがバイパスされる

UNIX で有効

症状:

/etc/passwd および /etc/group ファイルに対するデフォルト アクセス権限 none を設定したルールを作成したにもかかわらず、これらのファイルに読み取りアクセスできてしまいます。

解決方法:

デフォルトでは、CA Access Control 認証エンジンは /etc/passwd および /etc/group システム ファイルに対する読み取りアクセス チェックをバイパスします。 CA Access Control がこれらのシステム ファイルに対する読み取りアクセス チェックをバイパスしないようにするには、seos.ini ファイルの [seosd] セクション中の bypass_system_files の値を no に変更します。

重要: CA Access Control がこれらのシステム ファイルに対する読み取りアクセス チェックをバイパスしないようにする場合、適切な許可が設定されていることを確認します。 適切な許可を設定せず、読み取りアクセス チェックのバイパスを停止した場合、CA Access Control 管理者と root ユーザを含むユーザがシステムにアクセスできなくなり、重要なシステム処理に失敗する場合があります。

エンタープライズ ユーザまたはグループがリソースにアクセスできないが、正しいアクセス ルールが設定されている

Windows で有効

症状:

エンタープライズ ユーザまたはグループがリソースにアクセスする許可を持っているのに、アクセスできません。

解決方法:

エンタープライズ アカウントが再利用されている可能性があります。データベース内の許可は、名前が同一で SID が異なる新規アカウントではなく、古いアカウントに適用されています。 この状況をチェックするには、再利用エンタープライズ アカウントを解決します。

注: 再利用エンタープライズ アカウントの詳細については、「Windows エンドポイント管理ガイド」を参照してください。

ログインに失敗したユーザをロックアウトできない

UNIX で有効

症状:

ログインの失敗が指定の回数に達した後にパスワード PMD でユーザを禁止するように serevu を設定しています。 しかし、正しくログインできない場合でもユーザがロックアウトされません。 pam_failed_logins.log ファイルを参照するために nodaemon オプションを指定して serevu を起動したときに、サーバが応答しません。

解決方法:

seos.ini ファイルの [seos] セクション中の passwd_pmd の値が正しくありません。 passwd_pmd の値を、sepass がパスワード更新を送るパスワード PMD の名前に設定します。

ユーザが時間制限を超えてコマンドを実行できる

症状:

グループに対して時間制限を設定したにもかかわらず、グループ メンバが許可された時間を超えて CA Access Control コマンドを実行できてしまいます。

解決方法:

制限期間中、CA Access Control はユーザが新しいログイン セッションを開始するのを防止しますが、切断を強制することはできません。 ユーザが制限期間中にリソースまたはコマンドにアクセスするのを防止するには、リソースまたはコマンドのリソース レコードを変更して時間制限を指定します。

注: CA Access Control は、ユーザの USER または XUSER レコードに時間制限が存在するかどうかを確認してから、そのユーザが属する GROUP または XGROUP に対する時間制限が存在するかどうかを確認します。

CA Access Control がすべてのユーザを root として認識する

UNIX で有効

症状:

root 以外のユーザに対して sewhoami ユーティリティを実行した場合、CA Access Control はこのユーザを root ユーザとして認識してしまいます。

解決方法:

この問題をトラブルシューティングするには、ログイン アプリケーションの LOGINAPPL レコードで以下を検証します。

- LOGINAPPL レコードの名前がログイン アプリケーションの名前である。
- LOGINAPPL レコードの LOGINPATH パラメータがログイン アプリケーションへの正確なフル パスを指定している。

  ログイン アプリケーションへのパスを調べるには、トレースを実行(73 ページ)し、次にログイン アプリケーションを使用して CA Access Control にログインしてログアウトします。トレースを参照してパスを取得します。
- LOGINAPPL レコードの LOGINSEQUENCE パラメータに、ログイン アプリケーション用の正しいログイン シーケンスが指定されている。 詳細については、テクニカル サポート(http://ca.com/jp/support)にお問い合わせください。

注: CA Access Control は、サードパーティ ログイン アプリケーション用の LOGINAPPL レコードを定義しません。 サードパーティ ログイン アプリケーションを使用する場合は、そのアプリケーション用の LOGINAPPL レコードを手動で定義してください。

1 つのグループだけにユーザをパスワード管理者として追加できない

症状:

あるユーザを特定のグループのパスワード管理者として指定したいのですが、以下のコマンドを実行すると、そのユーザがすべてのグループのパスワード管理者になってしまいます。

```
editusr userName pwmanager
```

解決方法:

ユーザをパスワード管理者として追加する対象グループの名前を以下のように指定します。

```
join userName group(groupName) pwmanager
```

Windows 管理者が CA Access Control パスワードを変更できる

Windows で有効

症状:

CA Access Control で保護された自分の Windows 環境で Windows 管理者が CA Access Control のパスワードを変更できてしまいます。

解決方法:

CA Access Control で指定するユーザだけが CA Access Control パスワードを変更できるようにするには、以下のキー EnforceViaeTrust レジストリ エントリの値を 1 に設定します。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥passwd
```

このレジストリ エントリは、CA Access Control を通さなければユーザ パスワードの更新または作成ができないかどうかを指定します。 このレジストリ エントリのデフォルト値は 0 です。この場合、CA Access Control を使用しなくてもユーザ パスワードを更新または変更できます。

グローバル パスワード ポリシーにより、保護されたシステムからユーザがロックされる

症状:

グローバル パスワード ポリシーを実装した場合、そのパスワード ポリシーが原因で、CA Access Control で保護されたシステムからユーザがロックされてしまいます。

解決方法:

CA Access Control で保護されたシステムにアクセスする必要があるユーザ用のパスワード ポリシーを別個に作成します。 これらのユーザに対するパスワード ポリシーを作成するには、プロファイル グループを使用します。

プロファイル グループを使用してパスワード ポリシーを実装するには、以下の手順に従います。

1. プロファイル グループを作成します。
2. プロファイル グループ用のパスワード ポリシーを設定します。
3. プロファイル グループにユーザを割り当てます。

   プロファイル グループに対して設定したパスワード ポリシーは、そのプロファイル グループに関連付けられているユーザに適用されます。

Active Directory ユーザが UNAB エンドポイントにログインできない

UNIX で有効

症状:

UNIX 属性を持つ Active Directory ユーザが UNAB エンドポイントにログインできません。 この問題は、以下の場合に発生する可能性があります。

- 新しい Active Directory ユーザを作成するとき
- user_container 環境設定で指定されていないコンテナにユーザを作成または移動するとき

  注: user_container 環境設定は、uxauth.ini ファイルの AD セクションにあります。
- ユーザを直接 Active Directory ドメインに作成または移動するとき(つまりユーザはコンテナに存在しない)

解決方法:

この問題を解決するには、以下の手順に従います。

1. Active Directory 内で、ユーザに UID および GID があることを確認します。
2. ユーザが保留されていないことを確認します。
3. UNAB がエンドポイントで起動していることを確認します。
   a. エンドポイントでコマンド プロンプト ウィンドウを開きます。
   b. 以下のコマンドを実行します。

      ```
      ./uxauthd -status
      ```

      UNAB の現在のステータスを示すメッセージが表示されます。
4. エンドポイントが Active Directory に登録されていることを確認します。

   注: エンドポイントが Active Directory に登録されていない場合、uxconsole -register ユーティリティを使用してホストを登録してください。

5. エンドポイント上の OS 用の名前またはパスワード キャッシュ デーモンを以下の手順に従って停止します。

   a. UNAB デーモンの uxauthd を停止します。

      ```
      ./uxauthd -stop
      ```

   b. NSS キャッシュ データベースを削除します。

      ```
      rm -rf /opt/CA/uxauth/etc/nss.db
      ```

   c. OS 用の名前またはパスワード キャッシュ デーモンがエンドポイント上で実行中かどうかを確認します。

      たとえば、Linux または Solaris エンドポイントの場合は nscd デーモンが実行中かどうかを確認します。 HP-UX エンドポイントの場合は、pwgrd デーモンが実行中かどうかを確認します。

   d. OS 用の名前またはパスワード キャッシュ デーモンが実行中の場合は、プロセスを強制終了します。

   e. uxauthd を起動します。

      ```
      ./uxauthd -start
      ```

第 4 章: CA Access Control データベースの管理

このセクションには、以下のトピックが含まれています。

selang クエリで返されるレコードが最大 100 個に限られる

症状:

100 を超えるレコードを返すはずの selang クエリを実行したときに、以下のメッセージが表示されます。

警告: 100 (クエリ サイズ制限) 項目のみが表示されています。

解決方法:

query_size 設定のデフォルト値は 100 です。 CA Access Control が selang クエリに対して返すレコードの数を増やすには、query_size 設定値を変更します。

query_size 設定は、以下の場所に存在します。

- (UNIX) seos.ini ファイルの [lang] セクション
- (Windows) 以下の lang サブキー

  HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥lang

CA Access Control データベース上のバックアップ処理により、監査ログに UTimes および拒否レコードが生成される

症状:

CA Access Control の実行中に OS バックアップ ツールを使用して CA Access Control データベースをバックアップした場合、CA Access Control は以下のメッセージのようなエントリを監査ログに送ります。

```
03 Mar 2008 15:58:01 D FILE          UTimes    69 10
/opt/CA/AccessControl/seosdb/seos_pvf.fre /usr/sbin/fbackup
```

注: 上記の例では UNIX パス名が使用されていますが、以下の解決方法は Windows コンピュータにも適用されます。

解決方法:

上記の監査メッセージは、バックアップ処理による UTimes ファイル日付スタンプの更新を CA Access Control が妨げたことを示しています。 CA Access Control はバックアップ自体を妨げてはいません。

このメッセージが監査ログに表示されないようにするには、以下の手順に従います。

- バックアッププログラムが非スーパーユーザによって実行される場合は、そのユーザに対して OPERATOR 属性が設定されていることを確認します。
- バックアッププログラムがスーパーユーザによって実行される場合は、バックアッププログラムに pgmtype (バックアップ)プロパティが指定された SPECIALPGM レコードが存在することを確認します。

データベースが正しくバックアップされるようにするには、dbmgr ユーティリティを使用してバックアップを実行します。

CA Access Control データベースが破損している

UNIX で有効

症状:

CA Access Control エラー ログに以下のメッセージと同じようなメッセージを見つけました。

```
seoswd: [ID 973226 auth.error] seosd との通信がタイムアウトになりました。 seosd を実行しています。
FATAL!
Inseosrt_InitDatabase (0x270)
警告: /Access Control のパス/seosdb/seos_cdf.dat が破損しました
```

解決方法:

以下の手順に従って、データベースの破損を修復します。

注: この手順は、データベースがデフォルトのインストール場所、/opt/CA/Access Control にインストールされていることを前提としています。

CA Access Control データベース破損を修復する方法

1. CA Access Control を停止します。

   ```
   secons -s
   ```

2. (オプション) 必須な場合はテクニカル サポートにデータベースを提供できるように、データベースを別の場所にバックアップします。

3. データベースがクローズとしてマークされていることを確認します。

   ```
   cd /opt/CA/Access Control/seosdb
   ```

   ```
   dbmgr -util -close
   ```

   注: CA Access Control が正しくシャットダウンされない場合、データベースがオープンとしてマークされる場合があります。

4. データベースをチェックします。

   ```
   dbmgr -util -check
   ```

5. 以下のいずれかの操作を実行します。

   - データベースをチェックしたときにエラー メッセージが表示されない場合は、ステップ 6 に進みます。
   - データベースをチェックしたときにエラー メッセージが表示された場合は、ステップ 6 および 7 を実行せず、代わりに データベースを再構築 (75 ページ) します。

6. データベース ファイルを再構築します。

   ```
   dbmgr -util -build all
   ```

7. データベース エンジンを再チェックします。

   ```
   dbmgr -util -check
   ```

8. CA Access Control を起動します。

   ```
   seload
   ```

注: データベースがまだ破損している場合は、さらに詳しい調査が必要となります。 詳細については、テクニカル サポート (http://ca.com/jp/support) にお問い合わせください。

第 5 章: リモート コンピュータへの接続

このセクションには、以下のトピックが含まれています。

リモートコンピュータから接続できない

症状:

リモート CA Access Control コンピュータに接続できません。

解決方法:

接続に関する問題のトラブルシューティングを行います (60 ページ)。

seosd との通信タイムアウトが syslog に継続的に表示される

Windows で有効

症状:

CA Access Control を実行しているときにコンピュータが遅くなり、以下のメッセージが syslog に表示されることがあります。

```
seoswd: seosd との通信がタイムアウトになりました。 seosd を実行しています。
seoswd: seosd に対して返された 5378 [Success] との間に通信上の問題が発生しました。
seoswd: 説明: seosd との通信がタイムアウトになりました。
```

解決方法:

CA Access Control がタイムアウトになる原因は、コンピュータ上のアンチウイルス ソフトウェアです。 アンチウイルス ソフトウェアで、以下の手順を行います。

- リアルタイム スキャンから CA Access Control ディレクトリを除外します。
- CA Access Control ディレクトリのリアルタイム(オン アクセス)スキャンを停止します。

CA Access Control がデフォルトで CA Access Control レジストリ キー、ファイル、およびインストール ディレクトリを保護するので、上記の操作を行ってもウイルスの脅威が増大することはありません。

アンチウイルス ソフトウェア用の SPECIALPGM レコードを作成し、SPECIALPGM レコードの PGMTYPE プロパティを pbf に設定することをお勧めします。 pbf プログラム タイプは、ファイル処理イベントに対するデータベース チェックをバイパスします。

最初の受信 FTP 接続を制御できない

UNIX で有効

症状:

CA Access Control を起動したときに、vsftpd からの最初の受信 FTP 接続を制御できません。 FTP 用の TCP ルールおよび vsftpd 用の HOST ルールは作成済みであり、vsftpd からの以後の FTP 接続は、その TCP または HOST ルールに基づいて CA Access Control によってすべて制御されます。

解決方法:

CA Access Control を起動する前に vsftpd を起動した場合、vsftpd は受信 FTP 接続に対する受け入れシステム コールにフックを配置します。 このフックが存在する場合、CA Access Control がインターセプトする前に vsftpd は最初の受信 FTP 接続を処理します。

FTP 接続の処理後、vsftpd は次の FTP 接続のために受け入れシステム コールを呼び出そうとします。 しかし、CA Access Control はこのシステム コールをインターセプトするので、以後の FTP 接続をすべて制御できます。

最初の受信 FTP 接続をインターセプトするには、以下のいずれかの回避策を使用します。

- vsftp を起動する前に CA Access Control を起動します。
- inetd や xinetd などのスーパーサーバ デーモンを使用して vsftpd を起動します。

  注: スーパーサーバ デーモンの設定の詳細については、ご使用の OS のベンダーに問い合わせてください。
- CA Access Control の起動後に tripAccept ユーティリティを実行します。

  tripAccept ユーティリティを実行するには、seos.ini ファイルの [SEOS_syscall] セクション中の call_tripAccept_from_seload トークンを有効にする必要があります。これを実行する前に、tripAccept ユーティリティ用の SPECIALPGM レコードを定義しておくことをお勧めします。

ローカル ホストとターゲット ホストのターゲットページが異なる

UNIX で有効

症状:

CA Access Control ホストに接続しようとすると、以下のメッセージが表示されます。

警告: ローカル マシンのコード ページがターゲット ホストのコード ページと異なっています。

解決方法:

ローカル ホストとターゲット ホストで、seos.ini ファイルの [seos] セクション中のロケール設定値が同じであることを確認します。

selang を使用してエンドポイントに接続できない

症状:

selang を使用してエンドポイントに接続しようとすると、以下のようなエラー メッセージが表示されます。

データをアンパックできませんでした

解決方法:

コンポーネント間通信を保護するために使用される暗号化に関する問題が存在します。CA Access Control コンピュータで、暗号化キーおよび暗号化方法の変更が最近加えられたかどうかを確認します。

注: 暗号化方法の詳細については、「実装ガイド」を参照してください。

第 6 章: PMD からのルールのデプロイ

このセクションには、以下のトピックが含まれています。

サブスクライバ PMDB がマスタ PMDB から更新を受信できない

症状:

階層 PMDB アーキテクチャを使用しています。 サブスクライバ PMDB がマスタ PMDB から更新を受信しません。 マスタ PMDB のエラー ログには以下のメッセージがあります。

親ではない PMDB からの更新を受け付けることはできません。

解決方法:

サブスクライバ PMDB がマスタ PMDB から更新を受信しない場合、以下の手順に従って問題をトラブルシューティングしてください。

PMDB の更新に関する問題をトラブルシューティングする方法

1. マスタ PMDB (master_pmdb_name)のサブスクライバのリストとそのステータスを表示します。

   ```
   sepmd -L master_pmdb_name
   ```

   注: このコマンドは、マスタ PMDB コンピュータで実行します。

2. サブスクライバのリストを参照して、使用できないサブスクライバを特定します。

3. 使用できない各サブスクライバで、parent_pmd 設定値が正しいことを確認します。

   parent_pmd 設定は以下の場所に存在します。

   - （UNIX）seos.ini および pmd.ini ファイルの [seos] セクション
   - （Windows）以下のレジストリ キー

     ```
     HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥AccessControl
     ```

   注: parent_pmd トークンに指定するホスト名は、マスタ PMDB のホスト名と正確に一致する必要があります。 ホスト名解決が正しく設定されていることを確認することによって、この問題を解決できる場合があります。 UNIX コンピュータを使用している場合、sehostinf ユーティリティを使用してマスタ PMDB のホスト名を検出できます。 詳細については、テクニカル サポート（http://ca.com/jp/support）にお問い合わせください。

問題がまだ存在する場合は、以下の手順に従います。

1. マスタ PMDB エラー ログを表示します。

   ```
   sepmd -e master_pmdb_name
   ```

2. エラー ログを参照し、使用できないサブスクライバについてレポートされたエラー コードをメモします。
3. 使用できないサブスクライバごとに、エラー コードに基づいて問題をトラブルシューティングします。

問題がまだ存在する場合は、以下の手順に従います。

1. マスタ PMDB が保持する使用できないサブスクライバのリストから問題のサブスクライバを削除します。

   ```
   sepmd -r pmdb_name subscriber_name
   ```

   親 PMDB は、そのサブスクライバに更新を送ろうとします。
2. 前の手順を繰り返します。
3. サブスクライバのリストまたは親 PMDB エラー ログに変更がある場合は、その変更に基づいて問題をトラブルシューティングします。

サブスクライバ エンドポイントの監査ログ中の失敗イベント

症状:

サブスクライバがマスタ PMDB から更新を受信しません。 サブスクライバの CA Access Control 監査ログに失敗イベントが記録されています。

解決方法:

PMDB ユーザは ADMIN 属性を持っていません。 PMDB ユーザに ADMIN 属性を付与するには、以下の selang コマンドを使用してユーザ レコードを編集します。

```
chusr userName admin
```

注: selang コマンドを実行するには、ADMIN 属性が必要です。 PMDB 更新をサブスクライバにデプロイするときに CA Access Control は TERMINAL ルールを省略します。

第 7 章: ポリシーのデプロイ

このセクションには、以下のトピックが含まれています。

ポリシーのデプロイのトラブルシューティング

ホストにポリシーを割り当てる場合、policyfetcher がデプロイメント タスクを取得し、ポリシー スクリプトを実行するまで、ポリシーは割り当てられたエンドポイント上にデプロイされません。 したがって、エンドポイントでポリシーが転送されたりデプロイされたりするときに、さまざまな理由でデプロイ エラーが発生する可能性があります。

ポリシー デプロイメント エラーを解決するために、拡張ポリシー管理では以下のようなトラブルシューティング アクションが用意されています。 これらのアクションは、CA Access Control エンタープライズ管理 または policydeploy ユーティリティのいずれかを使用して実行できます。 CA Access Control エンタープライズ管理 では、トラブルシューティング アクションは[ポリシー管理]タブの[ポリシー]サブタブにあります。

以下のようなトラブルシューティング アクションがあります。

- Redeploy - ポリシー スクリプトを含む新規デプロイメント タスクを作成し、作成したタスクをエンドポイントにデプロイします。

  エンドポイントでのポリシー デプロイ中にエラーが発生した場合に、このオプションを使用します。 つまり、selang ポリシー スクリプトの実行に失敗した場合です。 ポリシーのデプロイ解除を行うには、エンドポイントにおけるスクリプト エラーの原因を手動で解決しておく必要があります。

  注: このオプションは CA Access Control エンタープライズ管理 でのみ利用可能で、policydeploy ユーティリティではサポートされていません。

- Undeploy - ポリシーを対応するホストから割り当て解除せずに、指定されたエンドポイントからポリシーをデプロイ解除します。

  このオプションは、DMS 上のホストに割り当てられていないエンドポイントから任意のポリシーを削除するために使用します。

- Reset - エンドポイントをリセットします。 CA Access Control はホスト ステータスをリセットし、有効なポリシーをすべてデプロイ解除し、拡張ポリシー管理オブジェクトをすべて削除します。

  このオプションを使用すると、すべてのポリシー デプロイ プロパティおよび拡張ポリシー管理プロパティから、エンドポイントおよび DMS でのエンドポイント ステータスが削除されます。

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

  このオプションを使用するのは、エンドポイントを手動でリセット(CA Access Control またはオペレーティング システムを再インストール)して、DMS が示す、そのエンドポイントで有効なすべてのポリシーを再デプロイする場合です。

  注: 復元の実行前にホストのステータスはリセットされません。したがって、すでにいくつかのポリシーがホストに適用されている場合、復元はエラーになります。

DH または障害回復 DMS が再サブスクライブに失敗する

症状:

障害回復プロセスの一部として、DH を DMS に再サブスクライブするか、または障害回復 DMS を本稼働 DMS に再サブクライブしています。 以下のメッセージが表示されます。

サブスクライバ (dms@host 上) の再サブスクライブに失敗しました。
リストア操作を完了するには、subscriber@host (dms@host 上) の再サブスクライブをオフセット値で手動で実行してください。

解決方法:

このメッセージは、DH または障害復旧 DMS を実行中ではない親 DMS に再サブスクライブするときに表示されます。 メッセージ中のオフセット値を使用して、手動で DH を DMS に再サブスクライブするか、障害回復 DMS を実行中の DMS に再サブスクライブする必要があります。 オフセット値を指定すると、サブスクライバには、復元時にそのデータベースに存在しなかったコマンドだけが送られます。

親 DMS に DH または障害回復 DMS を再サブスクライブするには、親 DMS ホストで以下のコマンドを実行します:

```
sepmd -s parent_name child_name@host offset
```

例: DMS への DH のサブスクライブ

以下の例では、オフセット値 18028 で DMS__ に DH__@test.com をサブスクライブします。 以下のコマンドを DMS__ で実行します。

```
sepmd -s DMS__ DH__@test.com 18028
```

ポリシー ステータスが「実行されていません」になる

症状:

ポリシー検証を有効にしています。 ポリシーをデプロイするときに、そのポリシーがデプロイされず、ポリシー ステータスは「実行されていません」になります。

解決方法:

ポリシー検証によって 1 つ以上のエラーがポリシーに見つかりました。 ポリシーを正常にデプロイできるようにするには、これらのエラーを修正する必要があります。

ポリシーを正常にデプロイするには、以下の手順に従います。

1. エラーを確認します。

   エラーを修正する前に、それらがポリシーまたは CA Access Control データベースのどちらで発生したかを特定する必要があります。

   a. CA Access Control エンタープライズ管理 で、[ポリシー管理]、[ポリシー]サブタブを順にクリックし、左側のタスク メニューにある[デプロイ]ツリーを展開して、[デプロイ監査]をクリックします。

      [デプロイ監査]ページが表示されます。

   b. 検索範囲を定義して、[実行]をクリックします。

      定義した検索範囲と一致したデプロイ タスクのリストが表示されます。

   c. デプロイされなかったデプロイ タスクの名前をクリックします。

      デプロイに関する情報(ポリシー中のエラーを含む)が表示されます。

2. （オプション）エラーが CA Access Control データベースにある場合は、以下を実行します。
   a. CA Access Control データベース中のエラーを修正します。
   b. 以下のいずれかの操作を実行します。
      - policydeploy ユーティリティを使用してデプロイ タスクを修正します。

        デプロイ タスクを修正するとその失敗ステータスが削除され、その後デプロイが正常に実行されると、そのエンドポイントのポリシーのステータスが「デプロイされました」に変更されます。
      - CA Access Control エンタープライズ管理 または policydeploy ユーティリティを使用してポリシーをもう一度デプロイします。

        ポリシーを再デプロイすると、別のデプロイ タスクが作成されます。 エラーが発生した前のデプロイ タスクのステータスは失敗のままです。 デプロイが成功した場合、エンドポイント上のポリシー ステータスは「デプロイされました」です。
3. （オプション）エラーがポリシーにある場合は、以下を実行します。
   a. エラーを含んでいないポリシー バージョンを新しく作成します。
   b. CA Access Control エンタープライズ管理 または policydeploy ユーティリティを使用してポリシーをアップグレードします。

変数を含むルールがエンドポイント上でデプロイされない

症状:

変数が定義されたルールが含まれているポリシーを作成してエンドポイントにデプロイしましたが、そのルールがエンドポイントで実装されません。

解決方法:

ポリシーのデプロイに関する問題を解決するには、以下の手順に従います。

1. エンドポイントで policyfetcher セクション中の policyfetcher_enabled 設定の値が 1 であることを確認します。

   この値が 1 に設定されている場合、policyfetcher の実行が指定されています。 policyfetcher が実行されていない場合は、エンドポイントにポリシーをデプロイできません。
2. policyfetcher ログでエラーをチェックします。

   注: policyfetcher ログは ACInstallDir/Log ディレクトリにあります。ここで ACInstallDir は CA Access Control をインストールしたディレクトリです。

3. CA Access Control エンドポイント管理 を使用して、変数がエンドポイントで定義されていることを確認します。

   注: 変数がエンドポイントで定義されていない場合、ポリシー ステータスは「デプロイの一時停止中」です。

   変数がエンドポイント上で定義されない場合は、変数を定義する selang ルールを含む新規ポリシー バージョンを作成してエンドポイントにデプロイします。

4. 以下が真であることを確認します。

   - ポリシーがエンドポイントに割り当てられている。

     ポリシーがエンドポイントに割り当てられていない場合は、CA Access Control エンタープライズ管理 を使用してポリシーを割り当てます。

   - ポリシーのデプロイ スクリプトにエラーが存在しない。

     ポリシーのデプロイ スクリプトにエラーが含まれている場合は、エラーを修正する新規ポリシー バージョンを作成してエンドポイントにデプロイします。

   - ポリシー ステータスが非同期ではない。

     ポリシー ステータスが非同期の場合、変数値は CA Access Control エンドポイントで変更された可能性があります。 ポリシーを再デプロイして非同期ステータスをクリアします。

5. デプロイ情報を監査して、以下を確認します。

   - エンドポイントが正しくポリシーをコンパイルした。
   - ポリシー用の DEPLOYMENT オブジェクトにデプロイ エラーが存在しない。

   ポリシーが正しくコンパイルしなかったか、DEPLOYMENT オブジェクトにエラーが存在する場合は、エラーを修正してポリシーを再デプロイします。

6. CA Access Control を再起動します。

ビルトイン変数がリフレッシュされない

症状:

CA Access Control エンドポイントのシステム設定を変更しました。しかし、ビルトイン変数の値が新しいシステム設定の値に変わっていません。

解決方法:

この問題を解決するには、以下の手順に従います。

1. エンドポイントで policyfetcher セクション中の policyfetcher_enabled 設定の値が 1 であることを確認します。

   この値が 1 に設定されている場合、policyfetcher の実行が指定されています。 policyfetcher が実行されていない場合、CA Access Control データベース中の更新された変数をチェックできません。

2. 以下の手順に従って、システム設定の変更後に policyfetcher がハートビートを送信したことを確認します。

   a. CA Access Control エンタープライズ管理 で、[ワールド ビュー]をクリックし、ワールド ビュー タスクをクリックします。

      検索画面が表示されます。

   b. 必要に応じて、特定のデータを見つけるための検索条件を定義して、[実行]をクリックします。

      定義した検索条件と合致した結果がカテゴリ別に表示されます。

   c. [前回のステータス]列の更新時間が、システム設定を変更した時間より後であることを確認します。

      [前回のステータス]列の更新時間がシステム設定の変更時間より前である場合、policyfetcher はハートビートを送信しておらず、更新された変数値をまだチェックしていません。

      注: endpoint_heartbeat 設定を変更することでハートビートの間隔を変更できます。

3. CA Access Control を再起動してシステム設定が変更されたことを確認します。

DNSDOMAINNAME 変数に値が設定されない

症状:

ビルトイン <!DNSDOMAINNAME> 変数に値が設定されません。

解決方法:

エンドポイントに DNS ドメインが設定されていることを確認します。

Windows エンドポイントに DNS ドメインが設定されていることを確認するには、以下の手順に従います。

1. コマンド プロンプトを開き、以下のコマンドを実行します。

   ```
   ipconfig/all
   ```

2. プライマリ DNS サフィックスが正しい値に設定されていることを確認します。

UNIX エンドポイントに DNS ドメインが設定されていることを確認するには、/etc/resolv.conf ファイルを開いてドメインが適切な値に設定されていることを検証します。

DOMAINNAME 変数に値が設定されない

症状:

ビルトイン <!DOMAINNAME> 変数に値が設定されません。

解決方法:

エンドポイントがドメインに接続されていることを確認します。

Windows エンドポイントがドメインに接続されていることを確認するには、以下の手順に従います。

1. [マイ コンピュータ]を右クリックして[プロパティ]をクリックし、[コンピュータ名]タブをクリックして[変更]ボタンをクリックします。
2. [ドメイン]フィールドにドメインが表示されていることを確認します。

UNIX エンドポイントがドメインに接続されていることを確認するには、以下の手順に従います。

1. 以下のコマンドを実行します。

   ```
   ypcats hosts
   ```

2. エンドポイントがドメインに接続されていることを確認します。

HOSTNAME 変数に値が設定されない

症状:

ビルトイン <!HOSTNAME> 変数に値が設定されない、または完全修飾されません。

解決方法:

エンドポイントに完全修飾ホスト名が設定されていることを確認します。

Windows エンドポイントに全修飾ホスト名が設定されていることを確認するには、以下の手順に従います。

1. コマンド プロンプトを開き、以下のコマンドを実行します。

   ```
   ipconfig/all
   ```

2. プライマリ DNS サフィックスが正しい値に設定されていることを確認します。

UNIX エンドポイントがドメインに接続されていることを確認するには、以下のファイルにホスト名が完全修飾名で定義されていることをチェックします。

- /etc/hosts
- /etc/resolv.conf

HOSTIP 変数に値が設定されない

症状:

ビルトイン <!HOSTIP> 変数に値が設定されない、またはエンドポイント用のすべての IP アドレスが設定されません。

解決方法:

IP アドレスがエンドポイントに存在することを確認します。

IP アドレスが Windows エンドポイント上に存在することを確認するには、以下の手順に従います。

1. コマンド プロンプトを開き、以下のコマンドを実行します。

   ```
   ipconfig/all
   ```

2. IP アドレス(1 つまたは複数)が正しいことを確認します。

IP アドレスが UNIX エンドポイント上に存在することを確認するには、以下の手順に従います。

1. 以下のコマンドを実行します。

   ```
   ifconfig -a
   ```

2. IP アドレス(1 つまたは複数)が正しいことを確認します。

オペレーティング システム変数に値が設定されない

症状:

CA Access Control オペレーティング システム変数を定義してエンドポイントの場所を指定しました。 このオペレーティング システム変数をポリシーのルールの中で使用した場合、この変数に値が設定されないため、CA Access Control はルールを実行しません。

解決方法:

環境変数がエンドポイント上のオペレーティング システムに存在することを確認します。

環境変数がオペレーティング システムに存在することを検証する方法

1. CA Access Control 変数がオペレーティング システム変数(OSVAR タイプ)として定義されていることを確認します。
2. オペレーティング システム変数がオペレーティング システムに存在することを以下の手順に従って確認します。
   - (Windows)コマンド プロンプトを開き、以下のコマンドを実行します。

     ```
     set
     ```
   - (UNIX)コマンド プロンプトを開き、以下のコマンドを実行します。

     ```
     env
     ```

     注: このコマンドを実行するには root ユーザである必要があります。

レジストリ変数に値が設定されない

Windows で有効

症状:

CA Access Control レジストリ変数を定義してエンドポイントの場所を指定しました。 このレジストリ変数をポリシーのルールの中で使用した場合、この変数に値が設定されないため、CA Access Control はルールを実行しません。

解決方法:

レジストリ変数(REGVAL タイプ変数)は REG_SZ または REG_EXPAND_SZ のレジストリ タイプを指している必要があります。 レジストリ変数中に指定されているレジストリ値が REG_SZ または REG_EXPAND_SZ タイプであることを確認します。

第 8 章: 監査レコードの収集

このセクションには、以下のトピックが含まれています。

一部の監査ログ メッセージを収集サーバが受信しない

UNIX で有効

症状:

CA Access Control にエンドポイントを設定して、それらのローカル監査ログをセントラル ログ収集サーバにルーティングしていますが、サーバが一部の監査ログを受信しません。 selogrd は監査レコードを送出するように設定し、selogrcd は監査レコードを収集するように設定してあります。

解決方法:

selorgd (CA Access Control ログ ルーティング システム用の送出デーモン) をトラブルシューティングするには、以下の手順に従います。

- selogrd.cfg ファイルを確認します。 このファイルには、CA Access Control がセントラル ログ コレクタにルーティングする監査メッセージが指定されています。
- 各エンドポイントの監査ログを確認します。 監査ログに監査イベントが見当たらない場合は、audit.cfg ファイルを確認します。 audit.cfg ファイルには、CA Access Control が監査ログに書き込む監査イベントが設定されています。 audit.cfg ファイルによって、CA Access Control がある監査イベントを監査ログに書き込むことが禁止されている場合、その監査イベントはルーティングできません。
- selogrd (ログ ルーティング システム用の送出デーモン) を設定してデバッグ メッセージを出力し、問題を再現します。 デバッグ メッセージを出力するように selogrd を設定するには、以下のコマンドを使用します。

  ```
  selogrd -d
  ```

監査ログ メッセージを収集サーバが受信しない

UNIX で有効

症状:

CA Access Control にエンドポイントを設定して、それらのローカル監査ログをセントラル ログ収集サーバにルーティングしていますが、サーバが監査ログをまったく受信しません。selogrd は監査レコードを送出するように設定し、selogrcd は監査レコードを収集するように設定してあります。

解決方法:

selogrcd がログ収集サーバ上で実行中であることを確認します。

注: selogrcd が長期間にわたって実行されない場合、監査イベントがエンドポイントによって破棄されることがあります。

SID の解決に失敗する(イベント ビューア警告)

Windows で有効

症状:

Windows イベント ビューアのアプリケーション ログを表示すると、特定の SID のアカウント名への解決に失敗しましたという、CA Access Control からの警告メッセージが見つかります。

解決方法:

セキュリティ識別子(SID)とは、オペレーティング システムに対してユーザまたはグループを識別する数値です。 システム アクセス制御リスト(DACL)の各エントリは SID を持っていて、これによって、アクセスを許可、拒否、または監査するユーザまたはグループを識別します。

この警告は、オペレーティング システムが SID をアカウント名に変換できなかったとき(SID が指し示すユーザまたはグループが存在しなくなった場合など)に表示されます。問題のシステムおよび対応するドメイン コントローラが、SID 解決を正常に行えるように設定されていることを確認してください。

SID 解決タイムアウト(イベント ビューア警告)

Windows で有効

症状:

イベント ビューアのアプリケーション ログを表示すると、特定の SID のアカウント名への解決がタイムアウトしましたという、CA Access Control からの警告メッセージが見つかります。

解決方法:

セキュリティ識別子(SID)とは、オペレーティング システムに対してユーザまたはグループを識別する数値です。 システム アクセス制御リスト(DACL)の各エントリは SID を持っていて、これによって、アクセスを許可、拒否、または監査するユーザまたはグループを識別します。

この警告メッセージは、あらかじめ定義されたタイムアウト時間内に、オペレーティング システムが SID をアカウント名に変換できなかった場合に表示されます。 以下を確認してください。

- 問題のシステムおよび対応するドメイン コントローラが、SID 解決を正常に行えるように設定されている
- ネットワーク設定が正常に設定されている

さらに、以下のレジストリ キー中の DefLookupTimeout 環境設定の変更により、タイムアウトを増加させることができます。

```
HKEY_LOCAL_MACHINE¥Software¥ComputerAssociates¥AccessControl¥SeOSD
```

注: SID 解決のタイムアウトを延長すると、CA Access Control のパフォーマンスが低下する可能性があります。

selogrd を起動しようとするとエラー コード 4631 が表示される

UNIX で有効

症状:

selogrd を起動しようとしました。 しかし selogrd は起動せず、以下のエラー メッセージが表示されます。

エラー 4631 (0x1217) が /opt/CA/AccessControl/bin/selogrd の初期化中に発生しました。

解決方法:

selogrd を起動する前にローカル ホスト名を解決します。 ホスト名を解決するには、ホスト名をオペレーティング システム hosts ファイルに追加するか、NIS または DNS に対してホスト名を定義します。

監査ファイル サイズが 2GB を超えると監査ログが停止する

症状:

監査ファイル サイズが 2GB を超えると、CA Access Control は監査レコードの監査ファイルへの書き込みを停止します。

解決方法:

監査ファイルのサイズが 2GB を超えた場合、CA Access Control は監査レコードを監査ファイルに書き込むことができません。 CA Access Control 監査ファイルの最大サイズは、logmgr セクションの audit_size 設定によって KB 単位で指定されています。

seos.audit ファイルの最大サイズを 2GB に設定するには、logmgr セクションの audit_size 設定の値を 2097151 に設定します。

CA Access Control が監査ログに書き込むときにシステムが遅くなる

症状:

CA Access Control が監査ログに書き込むときにコンピュータが遅くなります。

解決方法:

CA Access Control が監査およびトレース データを書き込む間、システム内のほとんどのプロセスがブロックされる可能性があります。 CA Access Control が監査データおよびトレース データを書き込む時間を短縮するには、以下を実行します。

- 必要なリソースおよびアクセスのみに監査モードを設定します。
- 必要な場合にのみ、トレースを開きます。
- 処理速度が最も速いファイル システムに、監査ファイル、トレース ファイル、CA Access Control データベース ファイルを格納します。

第 9 章: パフォーマンスの調整

このセクションには、以下のトピックが含まれています。

CA Access Control の実行時にパフォーマンスが低下する

症状:

CA Access Control の実行中にコンピュータが遅くなります。 CA Access Control を停止すると、パフォーマンスは通常通りに戻ります。

解決方法:

性能の問題を診断するおよび修正するには、性能に関する問題のトラブルシューティングを行います (61 ページ)。

CA Access Control サーバ上のシステム負荷が高すぎる

症状:

CA Access Control サーバのシステム負荷を軽減する必要があります。

解決方法:

システム負荷を軽減するには、以下を行います。

- データベースの階層を深くしないようにします。

  ユーザおよびリソースの階層が深い場合、すべての依存関係を取得およびチェックするにはシステム負荷がかかります。

- 頻繁に使用されるディレクトリに対して一般的なルールの適用を避けます。

  頻繁に使用されるディレクトリに対して一般的なルールを定義した場合、CA Access Control は数多くのシステム アクションをチェックすることになります。 たとえば、/usr/lib/* を保護する一般的な保護ルールを記述した場合、CA Access Control はシステムのすべてのアクションをチェックします。

- （Solaris のみ）プロセス ファイル システム（/proc）に属するファイルに対するアクセス チェックを CA Access Control が省略するように指定します。

  プロセス ファイル システム（/proc）に属するファイルに対するアクセス チェックを CA Access Control が省略するように指定するには、seos.ini ファイルの［SEOS_syscall］セクションの proc_bypass 設定値を 0 に変更します。

  注: seos.ini ファイルのトークンの詳細については、「リファレンス ガイド」を参照してください。

付録 A: トラブルシューティングおよび保守の手順

このセクションには、以下のトピックが含まれています。

CA Access Control が正しくインストールされていることを確認する方法

Windows で有効

CA Access Control をインストールしたら、正しくインストールされていることをただちに確認する必要があります。 CA Access Control が正しくインストールされていることを確認するには、以下の手順に従います。

CA Access Control のインストールが正常に完了したら、以下の変更点に注目してください。

- 以下の Windows レジストリに新しいキーが追加されています。

  ```
  HKEY_LOCAL_MACHINE¥Software¥ComputerAssociates¥AccessControl
  ```

  CA Access Control が実行されている間、CA Access Control のキーおよびサブキーは保護されています。また、キーを変更できるのは、CA Access Control エンドポイント管理 を使用するか、selang コマンドの使用する場合のみです。 しかしながら、キーと値を読み取るために CA Access Control エンドポイント管理 または selang コマンドを使用する必要はありません。

- コンピュータを再起動すると、CA Access Control の複数の新しいサービスが自動的に開始されます。 これらのサービスには、Watchdog、Engine、および Agent が含まれます。この 3 つのサービスは必ずインストールされます。 タスクの委任などのその他のサービスは、インストール時に選択したオプションによってインストールされるかどうかが決まります。 CA Access Control サービスの表示名はすべて、「CA Access Control」で始まります。 Windows サービス マネージャを使用すれば、インストールされているサービスを確認し、それらのサービスが動作中であることを検証できます。

リソース アクセスの問題をトラブルシューティングする方法

リソース アクセスに関する問題の最も一般的な原因は、不適切なアクセス権限です。 リソース アクセス問題の一例として、保護されたリソースに対するデフォルト アクセス権が none であるにもかかわらず、root ユーザがこれらのリソースにアクセスできてしまうことがあります。 リソース アクセスの問題のトラブルシューティングに役立つプロセスを以下に示します。

1. 保護されたリソースの監査モードを「すべて監査」に変更します。

   ```
   chres CLASS ResourceName audit(all)
   ```

   監査モードを「すべて監査」に変更すると、監査ログが参照しやすくなります。

2. トレースを実行 (73 ページ)して問題を再現します。
3. トレース ファイルおよび監査ログで、保護されたリソースに対するアクセスを確認します。 ファイル中の情報に基づいて、リソース アクセスの問題の原因を解決します。

   注: SPECIALPGM オブジェクトは監査されないバイパスを提供しますが、これらのバイパスはトレース ファイルに表示されます。

注: 詳細については、テクニカル サポート (http://ca.com/jp/support) にお問い合わせください。

接続の問題をトラブルシューティングする方法

CA Access Control コンピュータ間の接続は、さまざまな要因の影響を受けます。 接続の問題には、リモート CA Access Control コンピュータに接続できない、リモート コンピュータとの接続がタイムアウトになる、といった現象が含まれます。 接続の問題の原因を特定するのに役立つプロセスを以下に示します。

注: 詳細については、テクニカル サポート (http://ca.com/jp/support) にお問い合わせください。

1. CA Access Control コンピュータで、以下の項目に対して最近変更が加えられたかどうかをチェックします。
   - 暗号化キー
   - 暗号化方法
   - TCP および UDP ポート
2. TCP、CONNECT、HOSTNET、または HOST クラスで、新しいルールまたは最近変更されたルールを確認します。
3. 接続の問題が存在するポートを特定します。
4. トレースを実行（73 ページ）し、トレース ファイルで以下を確認します。
   - CA Access Control が TCP ルールまたは他のルールに基づいてブロックした接続
   - 接続の問題があるポート番号の隣に表示される P（許可）以外のコード
5. CA Access Control 監査ログで、問題があるポートを示す D（拒否）レコードを確認します。
6. ファイアウォールが問題を抱えるポートをブロックしていないことを確認します。
7. OS のログ ファイルで、バインドできないポートによって発生したエラー メッセージを確認します。

詳細情報:

CA Access Control エージェント通信用のポート番号の変更（76 ページ）

パフォーマンスの問題をトラブルシューティングする方法

パフォーマンスに関する問題の原因を特定するには、以下の手順に従います。

注: 詳細については、テクニカル サポート（http://ca.com/jp/support）にお問い合わせください。

1. パフォーマンスの問題がいつ発生するかを特定します。 パフォーマンスが低下するのはいつですか?
   - OS を起動するとき
   - CA Access Control を起動するとき
   - CA Access Control の起動後しばらく経過したとき

- CA Access Control または OS がスケジュールされたプロセスを実行するとき
- （UNIX）CA Access Control カーネル拡張機能がロードされるとき
- CA Access Control デーモンまたはサービスがロードされるとき

2. CA Access Control がパフォーマンスの問題の原因であると特定した場合は、以下の事項を調べます。
   - パフォーマンスが低下したときに最もリソースを消費しているプロセスは何ですか?
   - その CA Access Control プロセスはライフサイクルを通して同じプロセス ID を保持していますか?
   - サードパーティのフィルタ ドライバがコンピュータにインストールされていますか?
   - システム監視アプリケーションがコンピュータにインストールされていますか?
3. CA Access Control データベースをチェックします。
   a. CA Access Control を停止します。
   b. データベースをチェックします。

      ```
      dbmgr -util -all
      ```

   c. データベースのインデックスを再作成します(74 ページ)。
   d. データベースを再構築します(75 ページ)。
   e. CA Access Control を再起動して、問題がまだ存在するかどうかを確認します。
4. （Windows）ドライバ インターセプトを無効にします。
   a. CA Access Control を停止します。
   b. UseFsiDrv レジストリ エントリの値を 0 に変更します。 UseFsiDrv レジストリ エントリは次のレジストリ キーにあります。

      ```
      HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥AccessControl
      ```

   c. CA Access Control を再起動して、問題がまだ存在するかどうかを確認します。

5. トレースを実行(73 ページ)して問題を再現します。 トレース ファイルで以下の事項を確認します。
   - 短期間中に繰り返されたイベント(数秒中の多数のファイル アクセスなど)。
   - 強制終了されたプロセス。
   - 以下の値のいずれか。
     - ACEEH -1
     - U= 負の値

     これらの値によって、CA Access Control がユーザ名を解決できない、または値をリソースに割り当てることができないことが指定される場合があります。

注: UNIX コンピュータ上での CA Access Control パフォーマンスの改善の詳細については、「UNIX エンドポイント管理ガイド」を参照してください。

レポート サービスの問題を解決する方法

CA Access Control レポート サービスを使用すると、各エンドポイント(ユーザ、グループ、およびリソース)のセキュリティ ステータスを一括して確認できます。 レポート サービスをトラブルシューティングする場合は、そのコンポーネントを 1 つずつ確認します。

レポート サービスのトラブルシューティングに役立つプロセスを以下に示します。

1. エンドポイントのオペレーティング システムに応じて、以下のいずれかを行います。
   - UNIX コンピュータ上のレポート エージェントのトラブルシューティング(64 ページ)
   - Windows コンピュータ上のレポート エージェントのトラブルシューティング(66 ページ)
2. 配布サーバをトラブルシューティングします(69 ページ)。
3. JBoss をトラブルシューティングします(71 ページ)。
4. レポート ポータルをトラブルシューティングします(72 ページ)。

UNIX コンピュータ上のレポート エージェントのトラブルシューティング

UNIX で有効

レポート エージェントは、エンドポイント上のローカル CA Access Control データベースおよびすべての Policy Model データベース(PMDB)のスケジュールされたスナップショットを収集し、次にこのスナップショットを配布サーバのレポート キューに XML 形式で送信します。

UNIX コンピュータ上のレポート エージェントをトラブルシューティングする方法

1. 以下の設定が正しいことを確認します。 これらの設定は、seos.ini ファイルの ReportAgent セクションに存在します。

   注: CA Access Control エンドポイント管理 または selang コマンドのいずれかを使用して、この設定値を検証できます。 しかし、この手順については、config 環境で selang コマンドを使用して設定を変更する方法をお勧めします。 selang コマンドを使用すると、CA Access Control の停止および再起動を行わずに設定値を変更できます。

   reportagent_enabled

   ローカル コンピュータでレポートが有効(1)になっているかどうかを指定します。

   デフォルト: 0

   重要: レポート エージェントの自動実行を有効にするには、この値を 1 に設定する必要があります。 この設定値が 0 である場合、レポート エージェントは配布サーバに対してデータベースのスケジュールされたスナップショットを送信しません。 しかし、この値が 0 である場合は、レポート エージェントをこのままデバッグ モードで実行できます。

   report_server

   配布サーバの URL を定義します。

   注: TCP 通信用のデフォルト ポートは 7222、SSL 通信用のデフォルト ポートは 7443 です。 配布サーバの URL に通信タイプ用の正しいポート番号が指定されていることを確認する必要があります。

   デフォルト: none

   例: tcp: //130.119.176.145: 7222。 この URL では、レポート エージェントは TCP プロトコルを使用して、IP アドレス 130.119.176.145 の配布サーバとポート 7222 上で通信します。

schedule

レポートが生成されてレポート サーバに送信される日時を定義します。

この設定は、次の形式で指定します。time@day[,day2][...]

デフォルト: 00:00@Sun,Mon,Tue,Wed,Thu,Fri,Sat

例:「19:22@Sun,Mon」と指定すると、レポートは毎日曜日と毎月曜日の午後 7:22 に生成されます。

send_queue

レポート エージェントがローカル データベースのスナップショットを送信する配布サーバ上のメッセージ キューの名前を定義します。

デフォルト: queue/snapshots

重要: この設定のデフォルト値は変更しないでください。

2. seos.ini ファイルの [daemons] セクションに以下の行が存在することを確認します(ACInstallDir は CA Access Control をインストールしたディレクトリです)。

```
ReportAgent = yes, ACInstallDir/lbin/report_agent.sh start
```

この行が存在する場合、レポート エージェント デーモンは CA Access Control の起動時に自動的に実行されます。

3. 以下のディレクトリに移動します(ACInstallDir は CA Access Control をインストールしたディレクトリです)。

```
ACInstallDir/lbin
```

4. レポート エージェント デーモンを停止します。

```
report_agent stop
```

5. 以下のディレクトリに移動します。

```
ACInstallDir/bin
```

6. 以下のコマンドを使用して、レポート エージェントをデバッグ モードで実行します。

```
reportagent -debug 0 -task 1 -now
```

reportagent

レポート エージェントを実行します。

-debug 0

レポート エージェントをデバッグ モードで実行し、出力をコンソールに表示するよう指定します。

注: レポート エージェント デーモンが有効になっている場合は、レポート エージェントをデバッグ モードで実行できません。

-task 1

CA Access Control レポートを生成するために、レポート エージェントが CA Access Control データベースに関する情報を収集および送信するよう指定します。

-now

レポート エージェントを今すぐ実行します。

7. レポート エージェントの出力を以下の手順に従って調べます。
   - 出力にエラーが含まれているかどうかを確認する
   - Send レポート パラメータ セクションの Send Queue および Report File パラメータに正しい名前が指定されていることを確認する
8. 以下のディレクトリに移動します。

   ```
   ACInstallDir/lbin
   ```

9. レポート エージェント デーモンを再起動します。

   ```
   report_agent start
   ```

Windows コンピュータ上のレポート エージェントのトラブルシューティング

Windows で有効

レポート エージェントは、エンドポイント上のローカル CA Access Control データベースおよびすべての Policy Model データベース(PMDB)のスケジュールされたスナップショットを収集し、次にこのスナップショットを配布サーバのレポート キューに XML 形式で送信します。

Windows コンピュータ上のレポート エージェントをトラブルシューティングする方法

1. 以下の設定が正しいことを確認します。 この設定は、以下のレジストリ キーに存在します。

   ```
   HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥ReportAgent
   ```

   注: CA Access Control エンドポイント管理 または selang コマンドのいずれかを使用して、この設定値を検証できます。 しかし、この手順については、config 環境で selang コマンドを使用して設定を変更する方法をお勧めします。 selang コマンドを使用すると、CA Access Control の停止および再起動を行わずに設定値を変更できます。

   reportagent_enabled

   ローカル コンピュータでレポートが有効(1)になっているかどうかを指定します。

   デフォルト: 0

重要: レポート エージェントの自動実行を有効にするには、この値を 1 に設定する必要があります。 この設定値が 0 である場合、レポート エージェントは配布サーバに対してデータベースのスケジュールされたスナップショットを送信しません。 しかし、この値が 0 である場合は、レポート エージェントをこのままデバッグ モードで実行できます。

schedule

レポートが生成されてレポート サーバに送信される日時を定義します。

この設定は、次の形式で指定します。time@day[,day2][...]

デフォルト: 00:00@Sun,Mon,Tue,Wed,Thu,Fri,Sat

例:「19:22@Sun,Mon」と指定すると、レポートは毎日曜日と毎月曜日の午後 7:22 に生成されます。

send_queue

レポート エージェントがローカル データベースのスナップショットを送信する配布サーバ上のメッセージ キューの名前を定義します。

デフォルト: queue/snapshots

重要: この設定のデフォルト値は変更しないでください。

2. 以下の設定が正しいことを確認します。 この設定は、以下のレジストリ キーに存在します。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Common¥communication
```

report_server

配布サーバの URL を定義します。

注: TCP 通信用のデフォルト ポートは 7222、SSL 通信用のデフォルト ポートは 7443 です。 配布サーバの URL に通信タイプ用の正しいポート番号が指定されていることを確認する必要があります。

デフォルト: none

例: tcp: //130.119.176.145: 7222。 この URL では、レポート エージェントは TCP プロトコルを使用して、IP アドレス 130.119.176.145 の配布サーバとポート 7222 上で通信します。

3. CA Access Control レポート エージェント サービスが開始されたことを確認します。
4. コマンド プロンプト ウィンドウを開き、CA Access Control を停止します。

```
secons -s
```

5. Windows サービス マネージャで CA Access Control レポート エージェント サービスを無効にします。

6. CA Access Control を起動します。

   ```
   seosd -start
   ```

   CA Access Control は起動しますが、レポート エージェント サービスは停止されます。

7. 以下のコマンドを使用して、レポート エージェントをデバッグ モードで実行します。

   ```
   reportagent -debug 0 -task 1 -now
   ```

   reportagent

   レポート エージェントを実行します。

   -debug 0

   レポート エージェントをデバッグ モードで実行し、出力をコンソールに表示するよう指定します。

   注: レポート エージェント サービスが起動している場合は、レポート エージェントをデバッグ モードで実行できません。

   -task 1

   CA Access Control レポートを生成するために、レポート エージェントが CA Access Control データベースに関する情報を収集および送信するよう指定します。

   -now

   レポート エージェントを今すぐ実行します。

8. レポート エージェントの出力を以下の手順に従って調べます。

   - 出力にエラーが含まれているかどうかを確認する
   - Send レポート パラメータ セクションの Send Queue および Report File パラメータに正しい名前が指定されていることを確認する

9. CA Access Control を停止します。

   ```
   secons -s
   ```

10. Windows サービス マネージャで CA Access Control レポート エージェント サービスを起動します。

    注: 自動スタートアップ タイプを選択する必要があります。

11. CA Access Control を起動します。

    ```
    seosd -start
    ```

    CA Access Control が起動し、レポート エージェント サービスが起動します。

配布サーバのトラブルシューティング

配布サーバでは、レポート エージェントがエンドポイントから送信する情報をメッセージキューが受信します。 その後、メッセージドリブン Java Beans（MDB）がメッセージキュー内のデータを読み取って中央データベースに書き込みます。

配布サーバをトラブルシューティングする方法

1. （UNIX） Tibco EMS 管理ツールを以下の手順に従って起動します。
   a. 以下のディレクトリに移動します。
      `/opt/CA/AccessControlServer/MessageQueue/tibco/ems/bin`
   b. 以下のコマンドを実行します。

      ```
      tibemsadmin
      ```
2. （UNIX） Tibco EMS 管理ツールを以下の手順に従って起動します。
   a. 以下のディレクトリに移動します。
      `C:¥Program Files¥CA¥AccessControlServer¥MessageQueue¥tibco¥ems¥bin`
   b. 以下のコマンドを実行します。

      ```
      tibemsadmin.exe
      ```
3. 以下のいずれかのコマンドを使用して、現在の環境に接続します。
   - 配布サーバがポート 7222（デフォルト ポート）でレポート エージェントをリスンする場合は、以下のコマンドを使用します。

     ```
     connect
     ```
   - 配布サーバがポート 7243 でレポート エージェントを SSL モードでリスンする場合は、以下のコマンドを使用します。

     ```
     connect SSL://7243
     ```
4. ユーザ名およびパスワードを入力します。

   注: デフォルト ユーザ名は admin で、パスワードは CA Access Control のインストール時に指定したパスワードです。

   ローカル Tibco 環境に接続されます。
5. 以下のコマンドを入力します。

   ```
   show queues
   ```

   配布サーバ上の Tibco キューのリストが表示されます。
6. エンドポイントでコマンド プロンプト ウィンドウを開き、以下のディレクトリに移動します（ACInstallDir は CA Access Control をインストールしたディレクトリです）。

   ```
   ACInstallDir/bin
   ```

7. エンドポイントでレポート エージェントを実行します。

```
reportagent -debug 0 -task 1 -now
```

reportagent

レポート エージェントを実行します。

-debug 0

レポート エージェントをデバッグ モードで実行し、出力をコンソールに表示するよう指定します。

-task 1

CA Access Control レポートを生成するために、レポート エージェントが CA Access Control データベースに関する情報を収集および送信するよう指定します。

-now

レポート エージェントを今すぐ実行します。

8. レポート エージェントの実行中に、tibemsadmin ユーティリティで queue/snapshots というキューを観察します。

- キューが増大する一方で縮小しない場合、JBoss が動作していない可能性があります。

  JBoss をトラブルシューティングする必要があります。

- キューが増大および縮小する場合、メッセージ キューは通常どおりに動作していると判断できます。

  レポート ポータルをトラブルシュートする必要があります。

  注: キューは急激に増大および縮小する場合があります。

- キューが増大しない場合、レポート エージェントが送信したスナップショットがメッセージ キューに届いていません。

  レポート エージェントをトラブルシュートする必要があります。

  注: 詳細については、テクニカル サポート(http://ca.com/jp/support) にお問い合わせください。

JBoss のトラブルシューティング

JBoss Web アプリケーション サーバ環境には、メッセージ キューからデータを読み取って中央レポート データベースに書き込むメッセージ ドリブン Java Beans（MDB）が存在します。

JBoss をトラブルシューティングする方法

1. JBoss が正しく起動することを以下のとおり確認します。
   - コマンド プロンプトから JBoss を起動する場合は、JBoss が起動するときの最初の出力を確認します。 出力にエラーが含まれていないことを確認します。
   - サービスとして JBoss を起動する場合は、ログ ファイルまたは tail コマンドを使用して、JBoss が起動したときの最初の出力を確認します。 出力にエラーが含まれていないことを確認します。
2. 以下のファイルを開いてエラーがあるかどうかを確認します（JBossInstallDir は JBoss をインストールしたディレクトリ）。

   JBossInstallDir/server/default/log/boot.log

   このファイルには、JBoss がマイクロカーネルをブートするたびに行ったステップが記録されます。
3. JAVA_HOME 変数が正しい場所に設定されていることを確認します。

   注: JAVA_HOME 変数が正しい場所に設定されているが、JBoss がこの変数を解決しない場合、JAVA_HOME 変数をより下位の場所（JDK インストール パス下の bin ディレクトリなど）に設定します。
4. 以下のファイルを開き、エラーが存在するかどうかを確認します。

   JBossInstallDir/server/default/log/server.log

   このファイルには、JBoss が JBoss Web アプリケーション サーバ環境で実行したアクションの一覧が記録されます。

   注： JBoss を起動するたびに新しい server.log ファイルが作成されます。
5. JBoss ポートが他のサービスで使用されるポートと競合していないことを確認します。

6. （オプション） JNP ポートが別のサービスと競合している場合は、以下の手順に従って JNP ポート 1099 を別のポートに変更します。

   a. テキストエディタで次のファイルを開きます。

      JBossInstallDir/server/default/conf/jboss-service.xml

   b. 以下のセクションのポート番号を変更します。

      ```
      <!-- The listening port for the bootstrap JNP service. Set this to -1 to run
      the NamingService without the JNP invoker listening port.-->
      <attribute name="Port">1099</attribute>
      ```

   c. ファイルを保存して閉じます。

7. （オプション） RMI ポートが別のサービスと競合している場合は、RMI ポート 1098 を別のポートに変更します。

   a. テキストエディタで次のファイルを開きます。

      JBossInstallDir/server/default/conf/jboss-service.xml

   b. 以下のセクションのポート番号を変更します。

      ```
      <!-- The port of the RMI naming service, 0 == anonymous -->
      <!-- attribute name="RmiPort">1098</attribute -->
      <attribute name="RmiPort">1098</attribute>
      ```

   c. ファイルを保存して閉じます。

レポート ポータルのトラブルシューティング

レポート ポータルを利用すると、配布サーバが中央データベースに格納するエンドポイント データにアクセスして、ビルトイン レポートを作成したり、そのデータを取得してカスタム レポートを作成したりできます。 そのために、CA Business Intelligence を使用します。

レポート ポータルをトラブルシューティングする方法

1. レポート インターフェース（BusinessObjects InfoView）にアクセスするための正しい URL を使用していることを確認します。 正しい URL は以下のとおりです。

   http://host:port/businessobjects/enterprise115/desktoplaunch

2. （Windows）InfoView にアクセスするための正しいメニュー オプションを使用していることを確認します。

   InfoView にアクセスするには、[スタート]-[プログラム]-[BusinessObjects XI Release 2]-[BusinessObjects Enterprise]-[BusinessObjects Enterprise Java InfoView]を選択します。

3. 以下のサービスが開始されることを確認します。

   - Apache Tomcat

- Central Management Server
- Connection Server
- Crystal Reports Cache Server
- Crystal Reports Job Server
- Crystal Reports Page Server
- Desktop Intelligence Cache Server
- Desktop Intelligence Job Server
- Desktop Intelligence Report Server
- Destination Job Server
- Event Server
- Input File Repository Server
- List of Values Job Server
- Output File Repository Server
- Program Job Server
- Report Application Server
- Web Intelligence Job Server
- Web Intelligence Report Server

4. CA Access ControlUniverse への接続をテストします。

   注: CA Access ControlUniverse が BusinessObjects Designer に表示されない場合、レポート パッケージはデプロイしないことがあります。 CA Access ControlUniverse への接続をテストし、レポート パッケージをデプロイする方法については、「実装ガイド」を参照してください。

トレースの実行

トレースを実行することで問題を解決できる場合があります。 CA Access Control は、seos.trace ファイル（ACInstallDir/log ディレクトリに存在する）にトレース レコードを書き込みます。

トレースを実行するには、以下の手順に従います。

1. トレース ファイルからレコードをすべて取り除きます。

   ```
   secons -tc
   ```

2. トレースを開始します。

```
secons -t+
```

3. 問題を再現します。
4. トレースを停止します。

```
secons -t-
```

5. トレース ファイルを参照します。

注: seosd セクション中の設定値でトレース ファイルを設定します。 seosd セクションの詳細については、「リファレンス ガイド」を参照してください。

CA Access Control データベースのインデックスの再作成

CA Access Control データベースには数多くの更新が加えられるので、データベース ファイルは次第に断片化していく場合があります。 データベースを最適化して速度と信頼性を高めるには、インデックスの再作成および データベースの再構築(75 ページ)を行います。 データベースのインデックス再作成は、3 ー 6 か月ごとに定期保守の一環として行い、さらにパフォーマンス上の問題が発生するたびに行ってください。

注: この手順では、CA Access Control データベースはデフォルトの場所(UNIX の場合は /opt/CA/AccessControl/seosdb、Windows の場合は C: ¥Program Files¥CA¥AccessControl¥Data¥seosdb)にインストールされます。 この手順を実行するには、root ユーザ(UNIX)または管理者(Windows)としてログインする必要があります。

CA Access Control データベースのインデックスを再作成する方法

1. CA Access Control を停止します。
2. 以下のディレクトリに移動します。
   - (UNIX) /opt/CA/AccessControl/seosdb
   - (Windows) C:¥Program Files¥CA¥AccessControl¥Data¥seosdb
3. データベースをバックアップします。

```
dbmgr -backup backup_directory
```

4. データベースにインデックスを付けます。

```
dbmgr -util -build seos_cdf.dat
dbmgr -util -build seos_odf.dat
dbmgr -util -build seos_pdf.dat
dbmgr -util -build seos_pvf.dat
```

注: UNIX コンピュータ上のデータベースのサイズをさらに縮小するには、sepurgdb ユーティリティを使用して未定義レコードの参照をデータベースから削除します。 sepurgdb 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。

CA Access Control データベースの再構築

CA Access Control データベースには数多くの更新が加えられるので、データベースファイルは次第に断片化していきます。 データベースを最適化して速度と信頼性を高めるには、インデックスの再作成(74 ページ)およびデータベースの再構築を行います。データベースの再構築は、3 ー 6 か月ごとに定期保守の一環として行ってください。

注: この手順では、CA Access Control データベースはデフォルトの場所(UNIX の場合は /opt/CA/AccessControl/seosdb、Windows の場合は C: ¥Program Files¥CA¥AccessControl¥Data¥seosdb)にインストールされます。 この手順を実行するには、root ユーザ(UNIX)または管理者(Windows)としてログインする必要があります。

CA Access Control データベースを再構築する方法

1. CA Access Control を停止します。
2. 以下のディレクトリに移動します。
   - (UNIX) /opt/CA/AccessControl/seosdb
   - (Windows) C:¥Program Files¥CA¥AccessControl¥Data¥seosdb
3. データベースをバックアップします。

   ```
   dbmgr -backup backup_directory
   ```
4. データベースからの既存のルールとユーザ関連データをエクスポートします。

   ```
   dbmgr -export -l -f exported_filename
   dbmgr -migrate -r migrated_filename
   ```
5. 以下のディレクトリに移動して、その下に seosdb_new という名前のディレクトリを作成します。
   - (UNIX) /opt/CA/AccessControl
   - (Windows) C:¥Program Files¥CA¥AccessControl¥Data
6. seosdb_new ディレクトリにデータベースを作成します。

   ```
   dbmgr -create -cq
   ```
7. exported_filename および migrated_filename ファイルを seosdb_new ディレクトリにコピーします。
8. 古いデータベースからエクスポートした既存のルールとユーザ関連データを新しいデータベースにインポートします。

   ```
   selang -l -f exported_filename
   dbmgr -migrate -w migrated_filename
   ```
9. seosdb ディレクトリの名前を seosdb_old に変更します。
10. seosdb_new ディレクトリの名前を seosdb に変更します。
11. CA Access Control を起動します。

CA Access Control エージェント通信用のポート番号の変更

CA Access Control クライアント アプリケーション（selang、policydeploy、devcalc など）および CA Access Control エージェントは、ポート 8891 上で通信します。 このポートを変更することはお勧めしません。 このポートを変更する必要がある場合は、以下の手順に従います。

CA Access Control エージェント通信用のポート番号を変更する方法

1. テキストエディタで次のファイルを開きます。
   - (UNIX) /etc/services
   - (Windows) %SystemRoot%¥drivers¥etc¥services
2. このファイルに以下のファイルを追加します。

   ```
   seoslang2 port-number/ tcp
   ```
3. ファイルを保存して閉じます。
4. CA Access Control デーモンまたはサービスを再起動します。

診断情報

CA Access Control サポート ユーティリティは、CA Access Control インストールに関する情報を収集します。 このユーティリティが収集した情報は、インストールの問題の原因を特定するのに役立ちます。

CA Access Control サポート ユーティリティは CA Access Control インストール パッケージには含まれていません。 詳細については、テクニカル サポート（http://ca.com/jp/support）にお問い合わせください。