CA Application Performance Management

セキュリティ ガイド

リリース 9.5

CA Technologies 製品リファレンス

このドキュメントは、以下の CA Technologies 製品および機能に関するものです。

- CA Application Performance Management （CA APM）
- CA Application Performance Management ChangeDetector （CA APM ChangeDetector）
- CA Application Performance Management ErrorDetector （CA APM ErrorDetector）
- CA Application Performance Management for CA Database Performance （CA APM for CA Database Performance）
- CA Application Performance Management for CA SiteMinder® （CA APM for CA SiteMinder®）
- CA Application Performance Management for CA SiteMinder® Application Server Agents （CA APM for CA SiteMinder® ASA）
- CA Application Performance Management for IBM CICS Transaction Gateway （CA APM for IBM CICS Transaction Gateway）
- CA Application Performance Management for IBM WebSphere Application Server （CA APM for IBM WebSphere Application Server）
- CA Application Performance Management for IBM WebSphere Distributed Environments （CA APM for IBM WebSphere Distributed Environments）
- CA Application Performance Management for IBM WebSphere MQ （CA APM for IBM WebSphere MQ）
- CA Application Performance Management for IBM WebSphere Portal （CA APM for IBM WebSphere Portal）
- CA Application Performance Management for IBM WebSphere Process Server （CA APM for IBM WebSphere Process Server）
- CA Application Performance Management for IBM z/OS® （CA APM for IBM z/OS®）
- CA Application Performance Management for Microsoft SharePoint （CA APM for Microsoft SharePoint）
- CA Application Performance Management for Oracle Databases （CA APM for Oracle Databases）

- CA Application Performance Management for Oracle Service Bus （CA APM for Oracle Service Bus）
- CA Application Performance Management for Oracle WebLogic Portal （CA APM for Oracle WebLogic Portal）
- CA Application Performance Management for Oracle WebLogic Server （CA APM for Oracle WebLogic Server）
- CA Application Performance Management for SOA （CA APM for SOA）
- CA Application Performance Management for TIBCO BusinessWorks （CA APM for TIBCO BusinessWorks）
- CA Application Performance Management for TIBCO Enterprise Message Service （CA APM for TIBCO Enterprise Message Service）
- CA Application Performance Management for Web Servers （CA APM for Web Servers）
- CA Application Performance Management for webMethods Broker （CA APM for webMethods Broker）
- CA Application Performance Management for webMethods Integration Server （CA APM for webMethods Integration Server）
- CA Application Performance Management Integration for CA CMDB （CA APM Integration for CA CMDB）
- CA Application Performance Management Integration for CA NSM（CA APM Integration for CA NSM）
- CA Application Performance Management LeakHunter （CA APM LeakHunter）
- CA Application Performance Management Transaction Generator （CA APM TG）
- CA Cross-Enterprise Application Performance Management
- CA Customer Experience Manager （CA CEM）
- CA Embedded Entitlements Manager （CA EEM）
- CA eHealth® Performance Manager （CA eHealth）
- CA Insight™ Database Performance Monitor for DB2 for z/OS®
- CA Introscope®
- CA SiteMinder®
- CA Spectrum® Infrastructure Manager （CA Spectrum）

- CA SYSVIEW® Performance Management （CA SYSVIEW）

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。

目次

第 1 章: CA APM のセキュリティの概要

この章では、セキュリティに関連する用語と、CA Technologies Application Performance Management （CA APM）のセキュリティ オプションについて説明します。

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 APM のセキュリティの概要

CA APM は、以下のセキュリティ メカニズムを使用して、CA Introscope® と CA CEM のセキュリティを保護します。

- Introscope および CA CEM への、ユーザ/グループベースの認証と許可によるアクセス
  - *users.xml* ファイルを使用したファイルベースのローカルによるセキュリティ

    詳細については、「ローカルによるセキュリティを使用した Introscope のセキュリティ保護 (P. 41)」および「CA CEM のローカルによる認証および許可 (P. 157)」を参照してください。
  - LDAP

    詳細については、「LDAP による Introscope のセキュリティ保護 (P. 57)」を参照してください。

- CA EEM

  詳細については、「CA EEM による Introscope のセキュリティ保護 (P. 70)」および「CA CEM の CA EEM による認証および許可 (P. 146)」を参照してください。

  注: CA APM は EEM 8.4 SP4 SDK を提供し、EEM サーバ バージョン 8.4 SP4 以降で認定されています。

  また、以下の CA EEM ガイドも参照してください。これらは、CA サポートサイトからダウンロードする CA EEM アプリケーションに付属しています。

  - *CA Embedded Entitlements Manager Getting Started Guide*
  - *CA Embedded Entitlements Manager Release Notes*

- Enterprise Manager のセキュリティ
  - Manager of Managers （MOM）とコレクタ間のセキュリティ保護された認証のための公開鍵および秘密鍵
    詳細については、「セキュリティ保護された認証のための公開鍵および秘密鍵の構成 (P. 35)」を参照してください。
  - Enterprise Manager への接続をセキュリティ保護するために必要なユーザ許可

    詳細については、「Introscope がセキュリティをチェックする仕組み (P. 40)」を参照してください。
  - コレクタと MOM 間の通信の難読化
  - Enterprise Manager とブラウザ間のセキュリティ保護された通信のための構成プロパティ

    詳細については、「HTTPS のみによる Enterprise Manager アクセスの制限 (P. 175)」のトピックと、「CA APM 設定および管理ガイド」の「*Enterprise Manager Web サーバの構成*」を参照してください。
  - エージェントと Enterprise Manager 間のセキュリティ保護された通信のための構成プロパティ

    詳細については、「*CA APM Java Agent 実装ガイド*」または「*CA APM .NET Agent 実装ガイド*」を参照してください。

- 特定のユーザが特定の Introscope ドメインを表示できるようにする構成プロパティ

  詳細については、「Introscope ドメインの定義と構成 (P. 25)」および「Introscope のドメインとセキュリティについて (P. 38)」を参照してください。

- 特定のユーザが特定の Enterprise Manager をシャットダウンできるようにする構成プロパティ

  詳細については、「Enterprise Manager サーバ権限の構成 (P. 54)」を参照してください。

- 特定のユーザがアプリケーション問題切り分けマップに特定のフロントエンドとビジネス サービスを表示できるようにする構成プロパティ

  詳細については、「アプリケーション問題切り分けマップのセキュリティ保護 (P. 128)」を参照してください。

- 特定のユーザが動的インスツルメンテーションを実行できるようにする構成プロパティ

  詳細については、「domains.xml での Introscope ドメイン権限の構成 (P. 50)」を参照してください。

- 特定のユーザがスレッド ダンプを実行できるようにする構成プロパティ

  詳細については、「domains.xml での Introscope ドメイン権限の構成 (P. 50)」を参照してください。

- CA CEM のセキュリティ
  - TIM がインストールされる Windows または Linux マシンの root パスワード保護

    詳細については、「*CA APM インストールおよびアップグレード ガイド*」の「*Installing the Operating System for a new TIM*」を参照してください。

  - Enterprise Manager と TIM 間の通信をセキュリティ保護する構成プロパティ

    詳細については、「HTTPS を介した TIM 通信の構成 (P. 174)」を参照してください。

- APM データベース内の CA CEM データは暗号化され、FIPS 規格に適合しています。 詳細については、「FIPS 140-2 準拠の暗号化 (P. 170)」を参照してください。

- APM データベースのセキュリティ
  - APM データベースのパスワード保護

    詳細については、「APM インストールおよびアップグレード ガイド」の「*PostgreSQL データベース パスワードの変更*」を参照してください。

  - Enterprise Manager 接続のセキュリティ保護

    詳細については、「CA APM インストールおよびアップグレード ガイド」で、*tess-db-cfg.xml* ファイルでの暗号化パスワードの設定に関する情報を参照してください。

- CA Introscope® および CA CEM アプリケーションの監視
  - ビジネス サービス ベースのセキュリティにはユーザ許可が必要です。 詳細については、「デフォルトの CA EEM CEM アクセス ポリシー (P. 151)」のトピックと、「*CA APM 設定および管理ガイド*」を参照してください。

CA APM のセキュリティおよび権限の概要

認証と許可で構成される CA APM のセキュリティは、個々のユーザおよび指定された一連のユーザであるユーザ グループ（アプリケーション管理者、システム管理者、アナリストなど）が、Introscope および CA CEM に安全にログインできるようにします。 権限は、ユーザとグループが特定の Introscope タスクを実行できるようにします。

ユーザ認証について

*認証*は安全にユーザを識別するメカニズムです。認証によって、Introscope と CA CEM に対して以下のような質問に対する回答が提供されます。

- このユーザは誰か。
- このユーザは本当に本人か。

認証システムは、認証対象のユーザおよび認証システムだけが把握している固有の情報に依存します。 ユーザの身元を確認するため、認証側のシステムは通常、固有の情報を提供するようにユーザに促します。 提供された情報が正しいことを認証側のシステムで確認できる場合、ユーザは認証済みと見なされます。

ユーザ許可について

*許可*は、あるシステム内で制御されるセキュリティ保護されたリソース（アプリケーション、ページ、データなど）に対し、特定の認証済みユーザが許可されるべきアクセスのレベルを、そのシステムで決定するためのメカニズムです。 言い換えると、許可は、リソースに対してアクションを実行する権限をユーザが持っているかどうかチェックするプロセスです。

任意のタイプの一連のリソースに対してアクションを実行する権限を特定のユーザまたはグループに与えるときは、*アクセス ポリシー*を使用します。

たとえば、データベース管理システムでは、特定のユーザにはデータベースからの情報の取得を許可し、データベース内のデータの変更を禁止する機能を与える一方、他のユーザにはデータの変更を許可する機能を与えるように設計される場合があります。 許可システムでは、以下のような質問に対する回答を提供することによって、権限が付与されます。

- ユーザ *X* は、リソース *R* にアクセスすることを許可されているか。
- ユーザ *X* は、操作 *P* を実行することを許可されているか。
- ユーザ *X* は、リソース *R* に対して操作 *P* を実行することを許可されているか。

セキュリティ領域について

セキュリティ領域は、ユーザ、ユーザ グループ、およびユーザの認証、許可、または認証と許可を行うアクセス ポリシーのソースを規定します。

realms.xml ファイルで CA APM のセキュリティ領域を 1 つ以上構成します。Introscope および CA CEM では、*realms.xml* で構成されたセキュリティ領域を使用して、ユーザの認証と許可の方法を決定します。 ユーザが Introscope または CA CEM のいずれかにログインするとき、ログインされるアプリケーションの側では、realms.xml 内で定義された順序で各セキュリティ領域をチェックします。アプリケーションは、指定の ID を持つユーザが存在するかどうかを確認します。 入力されたユーザ パスワードが特定のセキュリティ領域について提供された値と一致した場合、認証は成功します。 以下の条件のいずれかが該当する場合、認証は失敗します。

- 定義された領域内にその名前のユーザが存在しない。
- 領域内にユーザは存在してもパスワードが正しくない。

realms.xml での領域の構成については、以下のトピックを参照してください。

- realms.xml でのローカルによる認証の構成（P. 43）
- realms.xml での LDAP による認証の構成（P. 59）
- realms.xml での CA EEM による認証の構成（P. 76）

Introscope のセキュリティをデプロイするには、以下の 3 つのセキュリティ領域のいずれか 1 つまたはサポートされている任意の組み合わせを使用します。

- **ローカルの XML ファイル（ローカル）：** ローカルによるセキュリティは、ローカルによる認証とローカル許可から構成されます。Enterprise Manager の *<EM_Home>/config* ディレクトリに格納される XML ファイルを使用します。
  - ローカルによる認証の場合、XML ファイルを使用して、ユーザ名とパスワードの情報を各 Enterprise Manager にローカルに格納します。 デフォルトのファイル名は *users.xml* です。 実行時、Introscope はローカル ファイル（*users.xml*）をチェックして、CA APM ユーザを認証します。
  - ローカル許可の場合、Introscope は 2 つの XML ファイルを各 Enterprise Manager にローカルに格納します。 Introscope では、ドメイン権限用に *domains.xml*、サーバ権限用に *server.xml* を使用します。 実行時、Introscope はローカル ファイル（*domains.xml* と *server.xml*）をチェックして、CA APM ユーザを許可します。

Introscope のデフォルトはローカルによるセキュリティです (P. 41)。

重要: デフォルト CA APM ログインを、Workstation、WebView、Web Start Workstation、または CEM コンソールから Enterprise Manager に変更することをお勧めします。 これに従わず、Introscope のローカルによるセキュリティのみを使用する場合、個人情報の盗難にあう危険性が高くなります。 そのため、セキュリティ メカニズムとして CA EEM をお勧めします (P. 20)。

- **Lightweight Directory Access Protocol（LDAP）：** TCP/IP 上で実行されるディレクトリ サービスを照会および変更するためのアプリケーション プロトコル。

  ローカルの XML ファイルを許可に使用する場合、LDAP のセキュリティ領域は CA APM ユーザを認証するためだけに使用できます。 詳細については、「LDAP による Introscope のセキュリティ保護 (P. 57)」を参照してください。

- **CA Embedded Entitlements Manager （CA EEM）：** 一般的なアクセス ポリシーの管理、認証、および許可の各サービスを他のアプリケーションが共有できるようにする CA Technologies アプリケーション

  注: CA EEM による Introscope のセキュリティ保護はオプションですが、使用することをお勧めします。 CA EEM は業界標準のソリューションであり、ユーザ管理のためのユーザ インターフェースと、許可のためのきめの細かい権限設定を可能にする一元化されたストレージを備えているからです。 Introscope のアプリケーション問題切り分けマップのセキュリティを保護する場合は、CA EEM をデプロイします。

  CA EEM をデプロイすると、CA APM ユーザを認証および許可できます。

  また、認証に LDAP、許可に CA EEM が使用されるように CA EEM を構成することもできます。 詳細については、「LDAP を使用した CA EEM による認証の構成 (P. 80)」を参照してください。

以下の表に、Introscope セキュリティ領域がサポートする主な機能を示します。

セキュリティ領域によってサポートされている機能	CA EEM	LDAP	ローカル
複数の Enterprise Manager によって共有される一元化されたセキュリティ サーバ	○	○	×

セキュリティ領域によってサポートされている機能	CA EEM	LDAP	ローカル
セキュリティ領域は常に利用可能	×	×	○ Enterprise Manager 内で実行されるため、常に利用可能
フェールオーバのサポート	○	○	適用不可
SiteMinder との統合	○	×	×
きめの細かい権限をサポート 以下のきめの細かい権限タイプをサポートします。 ■ アプリケーション問題切り分けマップの権限 ■ ビジネス サービス ベースのセキュリティ ■ 柔軟な CA CEM 権限	○	適用不可	×
業界基準ソリューション	○	○	×
監査の考慮	○	○	×
ユーザ管理のためのユーザ インターフェースを含む	○	○	×
アクセス ポリシー管理のためのユーザ インターフェースを含む	○	適用不可	×

CA CEM のセキュリティをデプロイするには、以下の 2 つのセキュリティ領域のいずれか 1 つまたはサポートされている任意の組み合わせを使用します。

- **ローカルの XML ファイル（ローカル）：** ローカルによるセキュリティは、ローカルによる認証とローカル許可から構成されます。Enterprise Manager の *<EM_Home>/config* ディレクトリに格納される XML ファイルを使用します。
  - ローカルによる認証および許可の場合、XML ファイルを使用して、ユーザ名とパスワードの情報を各 Enterprise Manager にローカルに格納します。 デフォルトの 4 つの CEM セキュリティ グループ、およびこれらのグループに属するユーザも、このファイルで定義します。デフォルトのファイル名は *users.xml* です。 許可チェックは、デフォルトの 4 つのセキュリティ グループに対して定義されたメンバシップに基づいて行われます。 実行時、このローカル ファイル（*users.xml*）を使用して、CA CEM ユーザの認証および許可が行われます。

  Introscope のデフォルトはローカルによるセキュリティです。

- **CA Embedded Entitlements Manager （CA EEM）：** 一般的なアクセス ポリシーの管理、認証、および許可の各サービスを他のアプリケーションが共有できるようにする CA Technologies アプリケーション。

  注: CA Technologies はいくつかの理由で CA APM のセキュリティ保護に CA EEM を使用することをお勧めします。 CA EEM は業界標準のソリューションであり、ユーザ管理のためのユーザ インターフェースと、許可のためのきめの細かい権限設定を可能にする一元化されたストレージを備えているからです。
  - CA EEM をデプロイすると、CA APM ユーザを認証および許可できます。
  - CA SiteMinder と CA EEM を許可に使用して、CA EEM 認証を設定します (P. 80)。
  - 認証専用に CA EEM、許可にローカルの XML ファイル (P. 125)を構成します。

  CA EEM の詳細については、「CA EEM による Introscope のセキュリティ保護 (P. 70)」を参照してください。

CA APM にはシングル ログイン機能があります。CA CEM および Introscope の両方へのアクセスを許可されているユーザが、再度ログインする必要なしに 2 つのアプリケーション間を移動できます。CA CEM または Introscope のユーザ認証が完了すると同時に、CA APM は、ユーザの ID およびユーザを認証した領域の名前を入手します。 Introscope は、ユーザが属するグループを取得するためにこの情報を使用します。 CA APM は、ユーザを許可するために以下のいずれかの方法を使用します。

- CA EEM の場合、ユーザのアクセス ポリシー
- ローカルによるセキュリティの場合、1 つ以上の CA CEM のセキュリティ ユーザ グループに属していること

CA APM のセキュリティを設定する際、単一または混合のどちらのセキュリティ領域をデプロイするかを決める必要があります。 CA APM ユーザが Introscope にアクセスできるようにするには、ローカル領域または CA EEM 領域のいずれかをデプロイします。

注: CA EEM による認証と許可の両方をデプロイすることをお勧めします。詳細については、「CA EEM で CA APM をセキュリティ保護することの利点 (P. 20)」を参照してください。

CA EEM で CA APM をセキュリティ保護することの利点

CA EEM が備えている以下の特長により、CA APM のセキュリティには CA EEM をデプロイすることをお勧めします。

- ユーザ ID とアクセス ポリシーを管理するための一般的なアプローチの共有化
- CA APM のセキュリティの一元化

  CA EEM による認証では複数の Enterprise Manager で 1 つの CA EEM サーバを共有することが可能なため、一元化された CA APM のセキュリティをデプロイできます。

- 効果的なアクセス管理および資格情報アクセス管理
  - ビジネス サービス ベースのセキュリティでは、アクセス ポリシーを使用して、ビジネス サービスおよびその関連データにアクセスできる CA CEM のセキュリティ グループを制御できます。
  - アプリケーションのセキュリティは、誰がどのアプリケーションにアクセスできるかということに限定することはできません。 効果的なアクセス管理を行うには、アクセス権を取得した各ユーザがアプリケーション内のどのリソースに対してどのようなアクションを実行できるかということもセキュリティ ポリシーによって制御する必要があります。CA EEM は、ビジネス アプリケーション ポートフォリオの中で柔軟性のあるきめの細かい許可ポリシーを実装するための標準的な手段を提供します。
  - プロセス内の許可チェックおよび資格情報のポリシーは、アプリケーションの Embedded Entitlements のクライアントの領域に安全にキャッシュされ、次に、アプリケーション内でローカルに評価、実行されます。 これにより、オフライン アプリケーションのアクセス ポリシーの適用が可能になります。
  - アプリケーション固有のポリシーの区別
    CA EEM では、アプリケーション固有のポリシー データをその中央リポジトリに分離して、ポリシーおよび管理コントロールの区別を確実にすると同時に、柔軟性のあるアプリケーション管理を実現します。
- 単一の ID リポジトリ

  CA EEM には、ユーザ ID の信頼できる単一の情報源として使用できるリポジトリが含まれます。 選択肢として、この単一の情報源に、Microsoft Active Directory、Novell eDirectory、SunONE Directory などの外部ディレクトリを使用することもできます。

- エンタープライズの統合

  CA EEM を他の CA のセキュリティ ソリューションと共にデプロイすることで、一連の複雑なビジネス アプリケーションにまたがって一貫性のある Identity and Access Management （IAM）を実現できます。 これには、今日の開発環境において、適応可能で、柔軟で、扱いやすく、利用可能な、CA EEM のようなセキュリティ ツールが必要です。

  - CA SiteMinder の統合

    ネイティブ統合により、Embedded Entitlements のクライアント アプリケーションは、CA SiteMinder によって使用されるように構成されたユーザ ストア内のユーザおよびグループ情報にアクセスできるようになります。また、CA SiteMinder のクレデンシャルを使用した認証および CA SiteMinder Web アプリケーションでのシングル サインオンのサポートが可能になります。

  - C#、C++、および Java の SDK

    CA EEM は C#、C++、および Java の開発環境をサポートしています。 CA EEM による認証、許可、イベント管理、および管理の各 API に関する C#、C++、および Java の詳細なリファレンスが用意されています。 サンプル コードと XML スクリプトに加えて、セキュリティ機能をアプリケーションに埋め込む方法に関するチュートリアルが含まれます。

- 管理 Web UI

  CA EEM が提供する Web ベースの単一管理インターフェースによって、アプリケーション セキュリティ ポリシー、ユーザ ストア、および監査ルールを確立および管理するコストが最小限に抑えられます。 セキュリティ ポリシー管理をアプリケーション自体から切り離すことで、ビジネス要件の進化に合わせて一貫したセキュリティ レベルを維持でき、アプリケーション コードの再開発も必要ありません。

  - Web UI の共有

    CA EEM は、すべてのアプリケーション間ですぐに共有できる Web UI を備えています。この Web UI を使用して、ユーザとグループを管理し、アクセス ポリシーを定義および管理します。また、CA EEM SDK を使用して、管理 UI コンポーネントをカスタム Web ページに埋め込むこともできます。

- 管理のスコープ

  管理者が表示または操作する権限を、特定のアプリケーション、ユーザ、リソース、またはポリシーに制限できます。

- 権限のチェック

  セキュリティ ポリシーをテストし、詳細なポリシー デバッグ情報を表示することで、ポリシーによって希望の結果がもたらされるかどうかを確認してから、適用できます。

第 2 章: Introscope ドメインの定義と構成

この章では、Introscope のセキュリティを設定する前の Introscope ドメインの定義と構成について説明します。 また、MOM、コレクタ、および Workstation の間でセキュリティ保護された認証を行うための公開鍵と秘密鍵の設定について説明します。

このセクションには、以下のトピックが含まれています。

Introscope ドメインの定義と構成

Introscope はドメインを使用して、エージェントと監視ロジックを分割し、どの CA APM ユーザがどの情報を表示できるかを定義します。 Introscope エージェントのマッピングは、*<EM_Home>/config* ディレクトリにある *domains.xml* ファイルで Perl5 の正規表現を使用して行います。使用しているセキュリティ領域にかかわらず、ドメインを定義するときは *domains.xml* を使用します。

Introscope のセキュリティを設定するときは、ドメインの構成に加えて、ドメインの権限も構成します。 ローカルによるセキュリティの場合は、*domains.xml* ファイルでドメインの権限を構成します。 詳細については、「domains.xml での Introscope ドメイン権限の構成 (P. 50)」を参照してください。 Introscope のセキュリティに CA EEM をデプロイする場合、*domains.xml* 内のドメイン権限は Enterprise Manager によって無視されるため、代わりに CA EEM 内でドメイン権限を構成します。詳細については、「CA EEM APM ドメイン リソース アクセス ポリシーの作成と削除 (P. 111)」を参照してください。

ドメインの種類

Introscope には、以下の 2 種類のドメインがあります。

- *スーパードメイン*-- *スーパードメイン*は、システム内のユーザ定義のドメインをすべて含む上位集合ドメインです。すべてのエージェントは*スーパードメイン*に表示されますが、ユーザ定義のドメインに表示される場合もあります。 Introscope のデフォルト構成では、*スーパードメイン*が唯一のドメインです。その他のドメインを構成しない場合は、すべてのエージェントが*スーパードメイン*にマップされます。
- ユーザ定義のドメイン -- 新しいドメインは *<EM_Home>/config* ディレクトリにある *domains.xml* ファイルで定義します。 *domains.xml* ファイルに、個々のドメインのマッピングを、正規表現を利用して指定します。

ドメインの定義に関するルール

domains.xml ファイルにドメインを定義する際に適用されるルールは、以下のとおりです。

- ドメイン定義時には、XML ファイルの適切なルールに従う必要があります。
- ドメイン名では大文字と小文字が区別されます。
- ドメインは、ルート XML ドメインのエレメントの内側に配置する必要があります。
- *ドメイン*または*スーパードメイン*内に、それぞれ複数のエージェントをマップできます。 *ドメイン*がエージェントと一致するように構成されている場合、そのエージェントはその *ドメイン*にマップされ、*スーパードメイン*にも表示されます。

  注: トランザクション追跡を開始すると、そのようなエージェントは［トランザクション追跡］ウィンドウ内のユーザ定義ドメインに加えられます。
- エージェントは常に、割り当て先の最初のドメインにマップされます。ドメインが割り当てられていない場合、エージェントは*スーパードメイン*にマップされます。ユーザ定義のドメインが割り当てられている場合、エージェントはユーザ定義のドメインにマップされます。

- 現在の *スーパードメイン エージェント マッピング* (デフォルトではすべてのエージェントに一致するように構成) を変更しない場合、新しく定義するドメインは、*<SuperDomain>* タグの前に定義されます。
- *domains.xml* ファイルの正規表現の誤りなどの問題が原因で、どのマッピング条件にも一致しなかったエージェントは、*スーパードメイン*にマップされます。

クラスタ内およびクラスタ間の同一の domains.xml の使用

クラスタ内に MOM とコレクタをデプロイするときや、クラスタ内およびクラスタ間にオプションの CDV をデプロイするときは、domains.xml に関する以下の重要なルールを理解しておきます。

重要: CA APM のクラスタ内およびクラスタ全体で、MOM、コレクタ、および CDV 用に別々の domains.xml ファイルを用意しないでください。

MOM は、ライブ エージェント（クラスタに現在データを送信しているエージェント）についてクラスタ内で異なるドメインを処理できます。しかし、MOM とコレクタとで履歴エージェント用の異なるドメインを持つことにより、履歴データの MOM ビューにおいて一貫性が保たれなくなる可能性があります。 このような混合ドメインを持つクラスタでは、コレクタ上の履歴エージェントは追跡されません。したがってこれらのデータは、履歴エージェントを明示的にマウントしない限り、MOM によって作成された Workstation グラフには表示されません。 この状況を回避するために、CA Technologies では、クラスタ内の MOM およびすべてのコレクタ上に同一の domains.xml ファイルを配置することを強く推奨します。 こうすることで、特定のコレクタに関連する Workstation 上の履歴データを表示するために履歴エージェントをマウントしなくても、ライブ エージェントおよび履歴エージェントのデータが常に MOM Workstation から参照できるようになります。

クロス クラスタ データ ビューア（CDV）をデプロイする場合、CDV の domains.xml ファイルには以下のドメインが含まれている必要があります。

- CDV の接続先となる全コレクタの全ドメイン。
- CDV のデータ収集元となるコレクタが含まれる全クラスタにまたがる全ドメイン。

あるドメインがコレクタの domains.xml ファイル内に存在し、CDV の domains.xml ファイル内に存在しない場合、以下のことが起こります。

- CDV は、存在しないコレクタ ドメインのデータを収集しません。

CDV Workstation は、存在しないコレクタ ドメインのデータを表示しません。

エージェントの定義とドメインへのマッピング

ドメインを定義し、ドメインにエージェントをマップするために domains.xml ファイルを使用します。

以下の手順に従います。

1. *<EM_Home>/config* ディレクトリに移動します。
2. *domains.xml* ファイルを開きます。
3. 「ドメインの定義に関するルール (P. 26)」と以下のプロパティを使用して、ドメインを定義します。

   name

   ドメインの名前

   このプロパティのルール

   - 英数字、および下線（_）とダッシュ（-）を使用できます。
   - スペースは使用できません。

   description

   ドメインの簡単な説明

   引用符を除くすべての半角文字を使用できます。

   注: XML タグはすべて大文字と小文字が区別されます。

4. 追加のドメインについて手順 3 を繰り返します。
5. スーパードメイン マッピングが domains.xml の最後に定義されていることを確認します。これにより、domains.xml はスーパードメインにエージェントをマッピングする前に特定のドメインにエージェントをマッピングできます。

   たとえば、以下のスーパードメイン マッピングが domains.xml の先頭に配置されている場合、XML ファイルの残りが処理される前にすべてのエージェントがスーパードメインの下に配置されます。

   ```
   <SuperDomain>
              <agent mapping="(.*)"/>
              <grant group="Admin" permission="full"/>
   </SuperDomain>
   ```

   domains.xml の最後にこのスーパードメイン マッピングを配置することによって、スーパードメインは一致しないエージェントをすべてキャッチします。
6. *domains.xml* ファイルを保存し、閉じます。
7. Enterprise Manager を再起動して、新しいドメインがロードされるようにします。

注: *domains.xml* ファイル内に構文エラーなどのエラーがあると、Enterprise Manager は起動しません。

新規ドメイン用の domains.xml 構文

ドメイン用の構文

```
<domain name="Domainname" description="Domain description">
<agent mapping="host¥|process¥|agentname or matching agents"/>
<grant user="username" permission="permission"/>
</domain>
```

管理モジュールとドメインとの関連付け

新しい管理モジュールを作成するときは、その所属先のドメインを指定することができます。

管理モジュールをドメインに関連付けるには、*domains.xml* に定義したドメインと名前が同じディレクトリを作成し、この新しく作成したディレクトリに管理モジュールを移動します。

以下の手順に従います。

1. *<EM_Home>/config/modules* ディレクトリに、前のセクションで作成したドメインと名前が一致するディレクトリを作成します。

   たとえば、前の手順で定義したドメインの名前が「PetstoreA」であれば、以下に示すように、同じ PetstoreA という名前のディレクトリを作成します。

   `<EM_Home>/config/modules/PetstoreA`

   注: このドメイン ディレクトリの名前は、*domains.xml* ファイルに定義されているドメイン名と正確に一致している必要があります。スペルの誤りがなく、大文字と小文字が正しく区別されていることが必要です。正確に一致していない場合、このディレクトリに置かれた管理モジュールはロードされません。

2. 必要な管理モジュールを *<EM_Home>/config/modules* ディレクトリから、作成した新しいディレクトリに移動します。

3. Enterprise Manager を再起動します。これで、新しいドメインがロードされます。

新しく定義したドメインへのサンプル管理モジュールの追加

新規に定義したばかりのドメインには管理モジュールが一切含まれていません。 新規に定義したドメインにデフォルトのサンプル ダッシュボードを表示させる場合は、新しいドメインにサンプル管理モジュールをコピーする必要があります。

以下の手順に従います。

1. *<EM_Home>/config/modules/* ディレクトリに移動します。
2. 新しく定義したドメインの適切なモジュール ディレクトリに *SampleManagementModule.jar* ファイルをコピーします。

   たとえば、PetstoreA という名前のドメインを定義した場合は、以下のディレクトリに *SampleManagementModule.jar* をコピーします。
   <EM_Home>/config/modules/PetstoreA
3. Enterprise Manager を再起動して、新しい管理モジュールをロードします。

重要: 新しいドメインにコピーしたサンプル管理モジュールは、元のサンプル管理モジュールには一切リンクされていません。 元のサンプル管理モジュールに加えた変更は、他のドメインに配置されたサンプル管理モジュールのコピーには反映されません。この逆についても同様です。

エージェントのドメイン マッピングの変更

ドメインの削除または 2 つのドメインのマージを行った後に、エージェントを別のドメインにマップし直す場合、以下のような影響があります。

- 削除したドメインにマップされていたエージェントが、再割り当てされず、まだレポートを続けている場合、そのエージェントは*スーパー ドメイン*に表示されます。
- エージェントに SNMP コレクションが関連付けられている場合、SNMP MIB の再発行が必要になります。
- エージェントが別のドメインに移動されると、そのエージェントが保持していたシャットオフ情報はすべて失われます。

ドメインの削除

ドメインの削除が必要になるのは、以下の場合です。

- エージェントを別のドメインに割り当てた場合
- 2 つのドメインをマージした場合

以下の手順に従います。

1. Enterprise Manager をシャットダウンします。
2. <EM_Home>/config ディレクトリに移動します。
3. domains.xml ファイルからドメインを削除します。
4. 必要に応じて、マップされているエージェントを別のドメインに割り当て直します。
5. 削除したドメインに対応するドメイン ディレクトリを <EM_Home>/config/modules ディレクトリから削除します。
6. Enterprise Manager を再起動します。

2 つのドメインのマージ

2 つのドメインをマージするには、すべてのエージェント マッピング情報を 1 つのドメインにマージする作業と、関連付けられている管理モジュールをすべて 1 つのドメインに移動する作業を行う必要があります。

以下の手順に従います。

1. Enterprise Manager をシャットダウンします。
2. *<EM_Home>/config* ディレクトリの *domains.xml* ファイルを開きます。
3. 移動元ドメイン（ここでは Domain A とします）が定義されている部分で、エージェント マッピング情報が指定されている XML コードをコピーします。
4. 移動先ドメイン（ここでは Domain B とします）が定義されている部分で、エージェント マッピング情報が指定されている XML コードのコピーを貼り付けます。
5. 移動元ドメイン（ドメイン A）から、エージェント マッピング情報が指定されている XML コードを削除します。

6. 管理モジュールを *<EM_Home>/config/modules/* 内の移動元ドメイン（Domain A など）ディレクトリから移動先ドメイン（Domain B など）に移動します。

   注: 移動する管理モジュールと同じ名前の管理モジュールが移動先ドメインのディレクトリにすでに存在している場合は、移動元ドメインに存在する方の管理モジュールの名前を変更する必要があります。同じ名前の管理モジュールが 2 つある場合、Enterprise Manager は起動しません。

7. *domains.xml* から、移動元ドメインを削除します。
8. Enterprise Manager を再起動します。

異なる Introscope システム間でのドメインの複製

複製先となる Introscope システムのドメイン構成を、複製元となる Introscope システムのドメイン構成とまったく同じにする場合は、以下の手順に従います（つまり、*domains.xml* ファイルに定義されたドメインをすべてまったく同じにする場合）。

以下の手順に従います。

1. 複製元 Introscope システムの *<EM_Home>/config/domains.xml* ファイルを複製先 Introscope システムの同じディレクトリにコピーします。
2. 複製元 Introscope システムの *<EM_Home>/config/shutoff/MetricShutoffConfiguration.xml* ファイルがある場合は、複製先 Introscope システムの同じディレクトリにコピーします。
3. 複製元 Introscope システムの *<EM_Home>/config/modules/<domain>* ディレクトリの内容を複製先 Introscope システムにコピーします。
4. Enterprise Manager を再起動します。

Introscope システム間における複製なしでのドメインの移動

古い Introscope システムと新しい Introscope システム間のドメイン構成がわずかに異なる場合、これらのシステム間で複製を行わずにドメインを移動するには、以下の手順に従います。

以下の手順に従います。

1. 移動元 Introscope システムの *<EM_Home>/config* ディレクトリ内の *domains.xml* ファイルを開きます。
2. ドメイン情報をコピーします。
3. 移動先 Introscope システムの *<EM_Home>/config* ディレクトリ内の *domains.xml* ファイルを開きます。
4. コピーしたドメイン情報を *domains.xml* ファイルに貼り付けます。
5. 移動元 Introscope システムの *<EM_Home>/config/modules* にある管理モジュール用ディレクトリと同じディレクトリを、移動先 Introscope システムの同じ場所に新しく作成します。
6. 移動対象のドメインに属する管理モジュールをコピーし、移動先 Introscope システムの対応するドメイン ディレクトリにそれらを貼り付けます。
7. 移動元 Introscope システムから、移動対象のドメインを削除します。
8. Enterprise Manager を再起動します。

エージェント フェールオーバとユーザ/ドメイン構成

エージェント フェールオーバ機能を使用してユーザとパスワードを定義する場合は、指定されたフェールオーバ Enterprise Manager 全体で、*domains.xml*、*server.xml* および *users.xml* ファイルが同期されていることを確認します。

エージェント フェールオーバの詳細については、環境に応じて、「*CA APM Java Agent 実装ガイド*」または「*CA APM .NET Agent 実装ガイド*」の「*Configuring Agent Failover*」を参照してください。

セキュリティ保護された認証のための公開鍵および秘密鍵の構成

クラスタ化された環境において、MOM、コレクタ、および Workstation 間の通信プロトコルは、セキュリティ保護された認証のために公開鍵と秘密鍵を使用します。

注: 公開鍵と秘密鍵はログイン時にパスワードをセキュリティ保護するためだけに使用されます。すべての通信をセキュリティ保護するには、SSL が必要です。

コレクタのデフォルトの秘密鍵について

各コレクタは、MOM が接続に使用するパスワードを復号化するための秘密鍵を使用します。 公開鍵と秘密鍵は一対のセットである必要があります。 コレクタ Enterprise Manager の秘密鍵は *IntroscopeEnterpriseManager.properties* ファイルの *introscope.enterprisemanager.clustering.privatekey* プロパティで定義されます。

デフォルト値は、以下のとおりです。

```
config/internal/server/EM.private
```

セキュリティを強化するためにコレクタ用の公開鍵と秘密鍵の新しいセットを生成する場合を除き、秘密鍵を再構成する必要はありません。秘密鍵の再構成の詳細については、「公開鍵と秘密鍵の新しいセットの生成 (P. 36)」を参照してください。
introscope.enterprisemanager.clustering.privatekey プロパティの詳細については、「CA APM 設定および管理ガイド」を参照してください。

注: CA APM の公開鍵と秘密鍵は期限切れになりません。

公開鍵と秘密鍵の新しいセットの生成

CA APM 環境のセキュリティを強化するには、コレクタごとに公開鍵と秘密鍵の新しいセットを生成し、公開鍵を MOM に配置し、MOM のコレクタ プロパティを更新できます。

以下の手順に従います。

1. Introscope インストール ディレクトリに移動します。
2. コマンド プロンプトで、以下のコマンドを入力します。

   ```
   java -classpath
   product¥enterprisemanager¥plugins¥com.wily.introscope.em.client14_9.5.0.jar;l
   ib¥CLWorkstation.jar;product¥enterprisemanager¥configuration¥org.eclipse.osgi
   ¥bundles¥24¥1¥.cp¥lib¥WilyBouncyCastle.jar
   com.wily.util.encryption.KeyGenerator EM.public EM.private
   ```

3. コレクタ用の新しいキーを生成する場合は、MOM の *IntroscopeEnterpriseManager.properties* ファイルの *introscope.enterprisemanager.clustering.login.em1.publicKey* プロパティで指定された場所に公開鍵をコピーします。

   注: MOM 用の新しいキーを生成する場合、この手順は適用されません。

4. 公開鍵と秘密鍵をコピーし、Enterprise Manager の *<EM_Home>¥config¥internal¥server* に貼り付けます。

第 3 章: Introscope のセキュリティ保護

この章では、Introscope のセキュリティおよび権限を提供するためにデプロイできる認証と許可のメカニズムの構成について説明します。 また、アプリケーション問題切り分けマップのセキュリティおよび Introscope SSO について説明します。

このセクションには、以下のトピックが含まれています。

Introscope のセキュリティおよび権限の概要

認証と許可で構成される Introscope のセキュリティは、個々のユーザおよび指定された一連のユーザであるユーザ グループ（アプリケーション管理者、システム管理者、アナリストなど）が、Introscope に安全にログインできるようにします。 権限は、ユーザとグループが特定の Introscope タスクを実行できるようにします。

Introscope のセキュリティの背景情報については、「CA CEM のセキュリティの概要 (P. 11)」を参照してください。

Introscope ドメインおよびセキュリティについて

Introscope はドメインを使用して、エージェントと管理ロジックを分割し、どのユーザがどの情報を表示できるかを定義します。 ドメインへのエージェントのマッピングは、*domains.xml* ファイルで Perl5 の正規表現を使用して行います。

ドメインにエージェントをマップしたら、ドメイン権限を定義し、付与します。 許可プロセス時、Introscope は権限チェックを実行します。

Introscope ドメインの設定については、「Introscope ドメインの定義と構成 (P. 25)」を参照してください。

Introscope 権限の構成について

Introscope では、権限によって、どのタスク ユーザまたはグループが Workstation 内のモニタリング ロジックの構成や Enterprise Manager 管理タスクの処理などを実行できるかが決まります。 Introscope 権限の定義は、ドメインと Enterprise Manager について行います。 次に、ユーザ権限とドメイン権限を、ドメイン、Enterprise Manager、またはその両方に付与します。

ドメイン アクセス権と Investigator ツリー

Investigator ツリーは、与えられているドメイン権限が異なるユーザまたはグループごとに違ったように表示されます。

- *スーパードメイン*権限の読み取り権以上を与えられているユーザまたはグループは、Investigator ツリーのすべての定義済みドメインの内容を表示できます。
- 複数のドメインの権限が与えられているユーザまたはグループは、Investigator ツリーでそれらのドメインのドメイン情報を表示できます。
- ユーザまたはグループは、1 つ以上のドメインについて読み取り権以上の権限を持っている必要があります。持っていない場合、Workstation または WebView にログインして Investigator ツリーとコンソールを表示することができません。

ローカル許可の権限の構成は、*domains.xml* と *server.xml* を使用して行います。CA EEM による許可の権限の構成は、Safex ツールまたは CA EEM ユーザ インターフェースを使用して行います。権限の設定の詳細については、以下のトピックを参照してください。

- domains.xml での Introscope ドメイン権限の構成（P. 50）
- Enterprise Manager サーバ権限の構成（P. 54）
- CA EEM による許可の構成（P. 82）
- ローカルによるセキュリティから CA EEM によるセキュリティへの移行（P. 124）

Introscope のデフォルトのセキュリティ構成

Introscope のデフォルトのセキュリティ構成は、*realms.xml* ファイルで行います。 認証と許可の両方に使用されるローカルの XML ファイル（*<EM_Home>/config* ディレクトリ内）は、Introscope のデフォルト セキュリティ領域です。デフォルトのセキュリティ構成を使用するには、「ローカルによるセキュリティを使用した Introscope のセキュリティ保護 (P. 41)」を参照してください。

Introscope のデフォルトのセキュリティ構成が組織の要件を満たしていない場合は、*realms.xml* を構成して、認証と許可に CA EEM、LDAP、またはサポートされている領域の適切な組み合わせが使用されるようにすることができます。

Introscope のセキュリティの構成には、たとえば以下の方法をお勧めします。

- ローカルによるセキュリティのデフォルト設定を変更する。 詳細については、「ローカルによる認証の構成について（P. 41）」を参照してください。
- ローカルによるセキュリティを使用した認証を認証用の LDAP サーバに置き換える。詳細については、「LDAP による Introscope のセキュリティ保護（P. 57）」を参照してください。
- ローカルによるセキュリティを CA EEM による認証および許可に置き換える。詳細については、「CA EEM による Introscope のセキュリティ保護（P. 70）」を参照してください。

Introscope がセキュリティをチェックする仕組み

Introscope は、構成されたセキュリティ領域を確認することによって、すべてのセキュリティ チェックを開始します。 CA EEM による認証と SiteMinder による許可または LDAP による認証とローカル許可など、実装したセキュリティ領域を Introscope が認識した後は、セキュリティ実装に基づいて適切なセキュリティ チェックと権限チェックを実行します。

Introscope のセキュリティおよび権限チェックの一般的なプロセスは、以下の手順で構成されます。

1. 認証の開始時、*realms.xml* をチェックしてセキュリティ領域を確認し、一部のユーザ情報を取得します。
2. 認証の終了時、*users.xml* ファイル（ローカル）、LDAP サーバ、または CA EEM サーバから、ユーザ、グループ、およびユーザ グループのマッピングを取得します。

   注: CA EEM を LDAP サーバに統合する設定を行った場合は、認証に LDAP、許可に CA EEM を使用できます。 詳細については、「LDAP を使用した CA EEM による認証の構成 (P. 80)」を参照してください。

   注: CA EEM を SiteMinder に統合する設定を行った場合は、認証に SiteMinder、許可に CA EEM を使用できます。 詳細については、「CA SiteMinder による CA EEM による認証の構成 (P. 80)」を参照してください。
3. 許可の開始時、Enterprise Manager の *users.xml* ファイル（ローカル）または CA EEM からパスワードを取得します。
4. 許可の終了時、Enterprise Manager の *domains.xml* および *server.xml* ファイル（ローカル）または CA EEM から、ドメイン権限と Enterprise Manager 権限を取得します。

ローカルによるセキュリティを使用した Introscope のセキュリティ保護

Introscope のセキュリティの背景知識を理解したら、今度はセキュリティデプロイの計画に入ることができます。

以下の手順に従います。

1. 必要に応じて、*realms.xml* でローカル領域をセキュリティ領域として構成します。

   注: ローカル領域は *realms.xml* 内のデフォルトの Introscope 領域です。

2. *users.xml* でパスワードを使用してユーザとグループを設定します。
3. *domains.xml* でドメイン権限を割り当てます。
4. *server.xml* で Enterprise Manager サーバ権限を割り当てます。
5. CA APM のグループ、ユーザ、ドメイン、およびサーバと、それらに関連付けられている権限を必要に応じて追加、削除、または編集することによって、Introscope のセキュリティを確保します。

ローカルによる認証の構成について

ローカルによる認証は、Introscope においてデフォルトで使用される認証方法です。 ローカルによる認証を使用する場合、CA APM ユーザおよびパスワードは *users.xml* に格納されます。

ただし、電子メールや電話番号などのユーザの詳細情報は、ローカル領域では管理されません。 また、ローカル領域では、名前が同じでパスワードも同じ 2 人のユーザを管理することはできませんが、名前が同じでパスワードが異なる 2 人のユーザを管理することはできます。名前が同じでパスワードが異なる 2 人のユーザは、ローカル領域で別個のユーザとして認識されます。

ユーザとグループの定義およびパスワードの生成の詳細については、「users.xml での CA APM ユーザおよびグループの構成 (P. 46)」を参照してください。

ローカルによる認証の設定変更は、随時反映されます。CA APM ユーザがログインを試みると、そのユーザが入力したログイン情報と、*users.xml* ファイルに保存されている情報が比較されます。この比較は、認証要求があるたびに行われるようになっています。

以前にインストールした Introscope システムからユーザを移行する場合は、移行が完了するまで、*users.xml* ファイルの名前と場所を変更しないでください。

realms.xml でのローカルによる認証の構成

realms.xml を構成するときは、以下のルールに従います。

重要: これらのルールのいずれかに従わなかった場合、Enterprise Manager は起動しません。

- *descriptor=* の値は大文字と小文字が区別されます。
  - たとえば、*descriptor=Local Users and Groups Realm* と *descriptor=local users and groups realm* とは異なります。
- ローカル領域の場合、*descriptor=* の値は *Local Users and Groups Realm* である必要があります。
- 複数の領域がある場合、領域タグ内の *id=* の値は領域ごとに一意である必要があります。 例：

```
<realm descriptor="EEM Realm" id="EEM" active="true">
        <property name="username">
          <value>EiamAdmin</value
        </property>
           <property name="host">
            <value>localhost</value>
        </property>
        <property name="appname">
            <value>APM</value>
        </property>
        <property name="enableAuthorization">
            <value>true</value>
        </property>
        <property name="plainTextPasswords">
            <value>false</value>
        </property>
        <property name="password">
            <value>YhCVozLDYThTJk3icaAaY9/5MhJRqQ1X</value>
        </property>
    </realm>
    <realm descriptor="Local Users and Groups Realm" id="Local Users and Groups"
active="true">
        <property name="usersFile">
            <value>users.xml</value>
        </property>
    </realm>
```

以下の手順に従います。

1. *<EM_Home>/config* ディレクトリの *realms.xml* ファイルを開きます。
2. 次の記述が *realms.xm* の 3 番目のエントリとして存在することを確認します。

   ```
   <realm active="true" descriptor="Local Users and Groups Realm" id="Local Users and Groups">
   ```

3. 以下のプロパティを適宜設定します。

   usersFile

   ユーザが格納される *<EM_Home>/config* ディレクトリを基準にした相対パスで指定されるファイル名。デフォルトでは、*users.xml* です。

   注: このファイルにはグループ定義も含まれます。

   注: セキュリティ領域の複数のファイルを使用することについては、「セキュリティ領域の複数ファイルの使用について (P. 45)」を参照してください。

4. *realms.xml* ファイルへの変更内容を保存し、Enterprise Manager を再起動して変更を適用します。

ローカルによる認証が有効になった realms.xml 構文

realms.xml ファイルからのサンプル コードを以下に示します。

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<realms xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="0.1"
xsi:noNamespaceSchemaLocation="realms0.1.xsd">
    <realm descriptor="Local Users and Groups Realm" id="Local Users and Groups"
active="true">
        <property name="usersFile">
            <value>users.xml</value>
        </property>
    </realm>
```

セキュリティ領域の複数ファイルの使用について

すべてのセキュリティ領域について *realms.xml* ファイルにファイルが 1 つしか記述されていない場合は、このトピックを無視してください。

場合によっては複数の領域を設定することがありますが、たとえば、ユーザに基本的な権限を与えるデフォルト領域と、別の権限を与える第 2 の領域が必要な場合です。また、2 台の LDAP サーバがあり、その両方のセキュリティをテストすることもあります。 あるいは、これまでローカルによるセキュリティを使用していて、CA EEM に移行する際にローカルによるセキュリティを維持したい場合もあると思います。

realms.xml にセキュリティ領域として 2 つのファイルが記述されているときは、最初のファイルが認証および許可プロセスで使用されます。 同じパスワードを持つ User A という名前の 2 人のユーザがいる場合は、*realms.xml* 内で最初に記述されているファイルで見つかったパスワードが使用されます。 たとえば、*CEM45.xml* の前に *users.xml* が記述されていれば、*realms.xml* は *users.xml* で見つかったパスワードを使用して認証を行います。

ローカル領域の場合、電子メールや電話番号などのユーザの詳細情報は、*users.xml* でも *CEM45.xml* でも管理されません。また、ローカル領域では、名前が同じでパスワードも同じ 2 人のユーザを管理することはできません。ただし、名前が同じでパスワードが異なる 2 人のユーザを管理することはできます

同様に、*users.xml* および *CEM45.xml* 内の異なるユーザ グループに属する User A という名前の 2 人のユーザがいる場合は、*realms.xml* 内で最初に記述されているファイルで見つかったユーザ グループが使用されます。 たとえば、*CEM45.xml* の前に *users.xml* を記述したとしましょう。*users.xml* には、CEM システム管理者ユーザ グループに属する Admin という名前のユーザが登録されています。 *CEM45.xml* には、CEM アナリストユーザ グループに属する Admin という名前のユーザが登録されています。 この場合は、*realms.xml* 内の *users.xml* ユーザ グループが使用され、CEM システム管理者ユーザ グループに関連付けられた権限が、Admin という名前のユーザに与えられます。

users.xml での CA APM ユーザおよびグループの構成

ユーザ名とパスワードは、ユーザごとおよびグループごとに定義します。

注: *admin* ユーザを作成するときには、ユーザおよび権限は大文字と小文字が区別されないことに注意してください。*admin* または *Admin* のどちらのログイン名を使用してログインした場合でも、同じユーザ ロールの権限が適用されます。

CA APM のデフォルトのユーザ構成では、以下のユーザが定義されています。

- *Admin* （パスワードなし）
- *Guest* （*Guest* がパスワード）

以下の手順に従います。

1. *<EM_Home>/config* ディレクトリに移動します。
2. *users.xml* ファイルを開きます。
3. このユーザおよびグループの名前付けプロパティを使用してユーザ名を定義します。

   注: XML タグはすべて大文字と小文字が区別されます。

   ユーザとグループ用の構文例については、「ユーザ用の users.xml 構文 (P. 49)」および「グループ用の users.xml 構文 (P. 49)」を参照してください。
4. このプロパティを使用して、各ユーザまたはグループのパスワードを設定します。

   注: XML タグはすべて大文字と小文字が区別されます。

   password

   ユーザ パスワードです。

   以下のルールがこのプロパティに適用されます。

   - 引用符を除くすべての半角文字を使用できます。
   - デフォルトで、パスワードは暗号化されています。クリアテキストでもなく、難読化されてもいません（オプションで、エンコードしたパスワードを生成できます）。

- パスワードに使用できる文字は、XML で使用可能な文字です。
- パスワードの値は空にすることができます。

ベスト プラクティス： 組織のパスワード ポリシーに従います。

ローカルによる認証で使用する users.xml ファイル内のパスワードは、暗号化して格納されます。暗号化パスワードは、MD5Encoder ユーティリティを使用して生成するか、Introscope によって自動的に生成されるようにすることができます。 Introscope に付属する MD5 スクリプトは、入力をプレーン テキストで受け取り、それを暗号化された形式で出力します。

- 以下の条件がユーザの状況に該当する場合、手順 5 （暗号化されたパスワードの手動設定）の説明に従います。
  - *users.xml* で多数のユーザをすでに暗号化している。
  - 1 つまたは少数のパスワードのみ変更する。
- それ以外の場合は、すべてのユーザのパスワードをクリア テキストに戻します。
- 以下の条件がユーザの状況に該当する場合、手順 6 （プレーン テキスト パスワードの設定）の説明に従います。
  - 多数のユーザおよびパスワードを同時に作成または変更する。

5. 暗号化されたパスワードを手動で設定します。

   a. *users.xml* ファイルで *plaintextPasswords="false"* を設定します。

   b. *<EM_Home>/tools* ディレクトリ内にある適切なスクリプトを実行します。

      - Windows の場合、*MD5Encoder.bat* <パスワード>
      - UNIX の場合、*MD5encoder.sh* <パスワード>

      注: MD5Encoder.sh スクリプトを実行する場合、円記号を使用してパスワード内の特殊文字をエスケープします。たとえば、パスワードが *pa$word* の場合、スクリプトを正しく実行するためにドル記号（$）の前に円記号を配置します。 正しいコマンド ラインは以下のとおりです。
      ./MD5Encoder.sh pa¥$word

   c. 生成された暗号化パスワードをコピーし、users.xml ファイルの 2 行目に貼り付けます。

   たとえば、以下のようになります。

   ```
   <user password="5b5ab9639b79259f54bc39515540aeaf" name="john"/>
   ```

   構文例については、「パスワードが暗号化された users.xml 構文 (P. 49)」を参照してください。

6. プレーン テキストのパスワードを設定し、Introscope によって暗号化パスワードが自動的に生成されるようにします。

   a. *users.xml* ファイルで *plaintextPasswords="true"* を設定します。

   重要: *plainTextPasswords="true"* を設定すると、Introscope によってすべてのパスワードが暗号化されます。すべてのパスワードをプレーン テキストで設定します。そうしないと、すでに暗号化されているパスワードが Introscope によって暗号化されます。

   b. すべてのユーザのパスワードをプレーン テキストに設定します。

   たとえば、以下のようになります。

   ```
   <user password="John Jones Password" name="john"/>
   ```

   Enterprise Manager が次回 *users.xml* ファイルを読み取るとき（起動時またはユーザの認証時）に、以下のアクションを実行します。

   - Enterprise Manager はプレーン テキスト パスワードを暗号化して、*users.xml* を書き換えます。
   - Enterprise Manager は *plainTextPasswords* 属性を *false* にリセットします。

7. ユーザおよびグループを追加するには、ユーザ名を定義する手順 3、および各ユーザのパスワードを設定する手順 4 を繰り返します。
8. *users.xml* ファイルを保存して閉じます。

   users.xml ファイルの内容への変更は、Enterprise Manager を再起動しなくても有効となります。

注: *users.xml* ファイルにエラーがあると、Enterprise Manager は起動しません。

ユーザ用の users.xml 構文

```
<users>
    <user password="adb831a7fdd83dd1e2a39ce7591dff8" name="Guest"/>
    <user password="" name="Admin"/>
</users>
```

グループ用の users.xml 構文

```
<groups>
    <group description="Administrator Group" name="Admin">
        <user name="Admin"/>
    </group>
</groups>
```

パスワードが暗号化された users.xml 構文

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<principals xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
plainTextPasswords="false" version="0.3"
xsi:noNamespaceSchemaLocation="users0.3.xsd">
    <users>
        <user password="adb831a7fdd83dd1e2a39ce7591dff8" name="Guest"/>
        <user password="" name="Admin"/>
    </users>
    <groups>
        <group description="Administrator Group" name="Admin">
            <user name="Admin"/>
        </group>
    </groups>
</principals>
```

domains.xml での CA Introscope® ドメイン権限の構成

権限が適用されるのは、CA APM ユーザまたはグループがログインするときです。 CA APM ユーザまたはグループがログインしている間に変更が行なわれた場合、その変更は次回ログイン時まで認識されません。つまり、セッション中に権限が変更されても、CA Introscope® はセッションを終了しません。

CA Introscope® の権限は動的であり、ログイン試行のたびに *domains.xml* ファイルと *server.xml* ファイルが Enterprise Manager によってチェックされます。 したがって、権限の変更は Enterprise Manager を再起動しなくても行うことができます。

ユーザはドメインに対する権限を以下の順序で与えられます。

- ユーザを指定する各ドメインに記述されたすべての権限
- ユーザが所属するグループの各ドメインに記述されたすべての権限

また、これらのルールはドメインへのアクセス時に適用されます。

- 権限の観点から言うと、*スーパードメイン*は、ほかのすべてのドメインと同じように扱われます。
- スーパードメインへのアクセス権を持つユーザまたはグループに与えられた権限は、すべてのユーザ定義ドメインでも使用できます。
- 1 人のユーザまたは 1 つのグループは、1 つのドメインに対して複数の権限を持つことができます。
- 1 人のユーザまたは 1 つのグループは、複数のドメインで権限を持つことができます。

以下の手順に従います。

1. XML 編集プログラムを使用して、*<EM_Home>/config* ディレクトリの *domains.xml* ファイルを開きます。
2. ドメインごとに以下のプロパティを使用して、ユーザまたはグループの権限を定義します。

   注: ユーザまたはグループが複数の権限を持っている場合は、ユーザ/権限の組み合わせごとに設定行を 1 行追加します。

   read

   ユーザまたはグループは、ドメイン内のすべてのエージェントとビジネス ロジックを表示できます。

   この権限で実行できるタスクには以下のものがあります。

   - Investigator ツリーの表示 (ユーザがアクセス権を持つドメイン内のエージェントが表示されます)
   - Workstation コンソールでのダッシュボードの表示
   - Investigator のプレビュー ペインでのメトリック データとエレメント データの表示 (Investigator ツリー内の特定リソースのデフォルト ビューである、上位 N 件を示すフィルタされたビューの表示を含みます)
   - 管理モジュール、エージェント、またはエレメントの設定の表示
   - アラート メッセージの参照
   - 履歴 Data Viewer での履歴データの更新および拡大/縮小表示
   - 履歴 Data Viewer の履歴データの範囲に関するオプションの変更
   - グラフでのメトリックの表示/非表示の切り替え
   - Data Viewer でのメトリックの前面/背面移動
   - グループとユーザの基本設定の変更 (ホーム ダッシュボードの設定や、管理モジュール名をダッシュボード名と共に表示するかどうかなど)

   注: read 権限を持つユーザまたはグループは、Workstation のすべてのコマンドを参照できます。 ただし、アクセス権を持たないコマンドは無効になります。

write

write 権限を持つユーザまたはグループは、read 権限を持つユーザまたはグループが実行可能な操作をすべて実行できますが、以下のタスクも行うことができます。

- ドメイン内のすべてのエージェントとビジネス ロジックの表示
- ダッシュボードの作成および編集
- ドメイン内のすべてのモニタリング ロジックの編集

run_tracer

ユーザまたはグループは、エージェントについてトランザクション追跡セッションを開始できます。

注: この権限には、read 権限も割り当てる必要があります。

historical_agent_control

ユーザまたはグループはエージェント（複数可）をマウントおよびマウント解除できます。

注: この権限には、read 権限も割り当てる必要があります。

live_agent_control

ユーザまたはグループは、ドメイン内のメトリック、リソース、およびエージェントの報告をシャットオフできます。

注: この権限には、read 権限も割り当てる必要があります。

dynamic_instrumentation

ユーザまたはグループは動的インスツルメンテーションを実行できます。

動的インスツルメンテーションについては、「CA APM Java エージェント実装ガイド」または「CA APM .NET エージェント実装ガイド」を参照してください。

thread_dump

ユーザまたはグループは［スレッド ダンプ］タブを参照および使用できます。

スレッド ダンプの使用および設定については、「CA APM Workstation ユーザ ガイド」および「CA APM Java エージェント実装ガイド」を参照してください。

full

ユーザまたはグループは、ドメインに対するすべての権限を持ちます。

注: XML タグはすべて大文字と小文字が区別されます。

3. ユーザまたはグループを追加するたびに、手順 2 （「ドメインごとに以下のプロパティを使用して ...」）を繰り返します。
4. *domains.xml* ファイルを保存し、閉じます。

   CA APM ユーザのログイン時、Enterprise Manager は、ユーザが適切なドメイン権限を持っているかどうかを *domains.xml* ファイルでチェックします。

注: *domains.xml* ファイルに構文エラーなどのエラーがあると、Enterprise Manager は起動しません。

CA APM ユーザおよびグループのドメイン権限用のデフォルトの domains.xml 構文

デフォルトのドメイン構成では、以下のように定義されています。

- ユーザまたはグループ「*Admin*」は、スーパードメインに対する「full」権限を持ちます。
- ユーザまたはグループ「*Guest*」は、スーパードメインに対する「read」（表示のみ）権限を持ちます。

注: SAP ユーザまたはグループの権限は少し異なっており、以下のとおりです。

- ユーザまたはグループ「*sapsupport*」は、スーパードメインに対する「full」権限を持ちます。
- ユーザまたはグループ「*Admin*」は、スーパードメインに対する「read」（表示のみ）権限を持ちます。
- ユーザまたはグループ「*sapsupport*」は CEM システム管理者および管理者グループのメンバなので、CEM コンソールへのアクセス権限が付与されます。

ドメインのユーザまたはグループの権限を構成する構文は以下のとおりです。

```
<grant group="Admin" permission="full"/>
<grant user="Guest" permission="read"/>
```

オプションの CA APM ドメイン構成用の domains.xml 構文

この後に示すドメイン権限の構成例では、以下のユーザに次のようにドメイン権限が与えられています。

- bsmith： HRApplication ドメインに対する「*full*」権限
- fjones : HRApplication ドメインに対する「*read*」権限および「*run_tracer*」権限
- jlo： スーパードメインに対する「*write*」権限
- pdiddy： スーパードメインに対する「*read*」権限
- swonder： 「*dynamic_instrumentation*」権限
- cstevens： 「*thread_dump*」権限

domains.xml ファイルの定義例:

```
<?xml version="1.0" encoding="UTF-8"?>
<domains xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="domains0.3.xsd" version="0.3">
   <domain name="HRApplication" description="">
      <agent mapping="(.*)HRAppAgent(.*)" />
<grant user="bsmith" permission="full" />
<grant user="fjones" permission="read" />
<grant user="fjones" permission="run_tracer" />
<grant user="swonder" permission="dynamic_instrumentation" />
<grant user="cstevens" permission="thread_dump" />
   </domain>
  <SuperDomain>
      <agent mapping="(.*)"/>
      <grant user="jlo" permission="write"/>
      <grant user="pdiddy" permission="read"/>
  </SuperDomain>
</domains>
```

server.xml での Enterprise Manager サーバ権限の構成

以下のサーバ権限は、Enterprise Manager の操作に関連するアクティビティについて定義されます。

- Enterprise Manager のシャットダウン
- MIB ファイルの発行
- APM ステータス コンソールへのアクセス

以下の手順に従います。

1. XML 編集プログラムを使用して、*<EM_Home>/config* ディレクトリの *server.xml* ファイルを開きます。
2. 必要に応じて、以下のプロパティを使用して、各 CA APM ユーザまたはグループの権限を定義します。

   注: XML タグはすべて大文字と小文字が区別されます。

   shutdown

   ユーザまたはグループは Enterprise Manager をシャットダウンできます。

   publish_mib

   ユーザまたはグループは SNMP コレクション データを MIB に発行できます。

   MIB を発行するには、SNMP コレクションを作成する必要があります。このタスクを行うには、SNMP コレクションの保存先のドメインに対する書き込みアクセス権が必要です。

   apm_status_console_control

   ユーザまたはグループは、APM ステータス アラート アイコンの表示、APM ステータス コンソールの使用、APM ステータス コンソール CLW コマンドの実行を行えます。

   注: メトリック ブラウザ ツリーでアクティブなクランプのメトリック情報を表示するには、domains.xml のスーパードメイン権限 (P. 50)を持っている必要があります。

   full

   ユーザまたはグループは Enterprise Manager サーバに対するすべての権限を持ちます。
3. ユーザを追加するたびに手順 2 （「必要に応じて、以下のプロパティを使用して、各 CA APM ユーザ ...」）を繰り返します。
4. *server.xml* ファイルを保存して閉じます。

   注: *server.xml* ファイルに構文エラーなどのエラーがあると、Enterprise Manager は起動しません。

サーバ権限用の server.xml 構文

ユーザのサーバ アクセス権を設定するための構文は、以下のとおりです。

```
<grant user="username" permission="full">
```

ユーザまたはグループは Enterprise Manager の複数の権限を持つことができます。 複数のアクセス権を付与するには、ユーザ/アクセス権またはグループ/アクセス権のペアごとに 1 行を使用します。

デフォルトのサーバ構成用の server.xml 構文

デフォルトのサーバ構成では、「Admin」ユーザまたはグループは「full」権限を持ちます。

オプションのサーバ構成用の server.xml 構文

以下の例では、さまざまな CA APM ユーザに別々の権限を与える方法を示します。

- bsmith： 「*shutdown*」アクセス権
- tjones： 「*publish_mib*」権限
- cstevens： 「*apm_status_console_control*」権限

server.xml ファイルは以下の例のようになります。

```
<?xml version="1.0" encoding="UTF-8"?> <server
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="users0.1.xsd" version="0.1">
<grant user="bsmith" permission="shutdown" />
<grant user="tjones" permission="publish_mib" />
<grant user="cstevens" permission="apm_status_console_control" />
</server>
```

LDAP による Introscope のセキュリティ保護

LDAP はユーザ認証のみサポートします。Introscope のセキュリティのデプロイで Enterprise Manager が認証の目的で LDAP サーバに直接接続するようにする場合、許可にはローカルによるセキュリティを使用する必要があります。 許可にローカルによるセキュリティを使用することは、以下を意味します。

- Introscope の場合、LDAP サーバ上でユーザとグループを作成し、domains.xml ファイルで権限を割り当てる必要があります。
- CA CEM の場合、LDAP サーバ上でユーザおよび 4 つのデフォルト セキュリティ グループすべてを作成する必要があります。 たとえば、LDAP サーバ上で、cemadmin ユーザと CEM システム管理者セキュリティ グループを作成します。次に、CEM システム管理者セキュリティ グループのメンバとして cemadmin を割り当てます。これによって、cemadmin に CEM システム管理者セキュリティ グループの権限を付与します。 CA CEM の 4 つのデフォルト セキュリティ グループについては、「デフォルトの CA CEM のセキュリティ ユーザ グループに関連付けられるメニュー項目と権限 (P. 143)」を参照してください。

注: CA EEM を使用して Introscope のセキュリティをデプロイ済みで、CA EEM サーバが LDAP サーバに統合されている場合は、LDAP によって認証が行われるように CA EEM サーバを構成できます。 この場合、Enterprise Manager は、LDAP サーバに接続せず、LDAP サーバを認識しません。 詳細については、「LDAP を使用した CA EEM による認証の構成 (P. 80)」を参照してください。 このような状況の場合、Introscope は許可に CA EEM を使用します。

重要: ローカルによるセキュリティを許可に使用すると、アプリケーション問題切り分けマップのセキュリティの提供や、CA CEM 内のタブとデータの表示を制御するアクセス ポリシーの設定などができなくなります。 CA CEM でアプリケーション問題切り分けマップを提供し、アクセス ポリシーを使用する場合は、許可に CA EEM をデプロイする必要があります。

Introscope で、LDAP による認証とローカル許可を共に設定する場合は、このようなタイプのセキュリティおよび権限チェックについて事前に理解しておくと役に立ちます。

Introscope の LDAP による認証は、以下の v3 LDAP サーバおよびその他さまざまなサーバをサポートしています。

- IBM Directory Server （バージョン 5.1） -- この構成の例については、「IBM Directory Server 用の realms.xml 構文 (P. 67)」 を参照してください。
- Sun ONE Directory Server（バージョン 5.1）-- この構成の例については、「Sun ONE Directory Server 用の realms.xml 構文 (P. 68)」 を参照してください。
- Microsoft Active Directory（Windows 2000 および 2003）-- この構成の例については、「Microsoft Active Directory 用の realms.xml 構文 (P. 69)」 を参照してください。

Introscope のセキュリティの背景知識を理解したら、今度はセキュリティデプロイの計画に入ることができます。

これが、LDAP セキュリティの設定と維持のプロセスです。

1. LDAP サーバ上で CA APM ユーザおよびグループを設定します。
2. *realms.xml* で LDAP をセキュリティ領域として追加します。
3. ローカル許可を設定します。

LDAP による認証について

LDAP による認証の情報は*バインド*操作で提供されます。 この場合クライアントは、認証情報を含んでいる*バインド*操作をサーバに送ることにより、LDAP サーバとの接続を開始します。 *バインド*操作で提供される認証情報は、クライアントが選択する認証メカニズムによって異なります。

*バインド*を実行せずに、LDAP 要求を送信するクライアントは、匿名のクライアントとして扱われます。 *bindName* プロパティに値を入力しない場合は、認証メカニズムが適用されず、その他すべての認証環境プロパティが無視されることを意味します。 これを明示的に行うのは、設定されている可能性のある他の任意の認証プロパティが無視されるようにする場合だけにしてください。 いずれの場合も、クライアントは匿名のクライアントとして扱われます。 つまり、サーバはクライアントの身元がわからなくても、未認証のクライアントがアクセスできるように構成されている任意のデータにそのクライアントがアクセス（読み取りおよび更新）することを許可します。

realms.xml での LDAP による認証の構成

このトピックでは、認証方式として LDAP を構成する方法について説明します。

注: <*EM_Home*>/examples/authentication ディレクトリにあるサンプル構成ファイル realms.ldap.xml を利用できます。

realms.xml を構成するときは、以下のルールに従います。

重要: Enterprise Manager が起動するには、以下のルールすべてを満たす必要があります。

- descriptor= の値は大文字と小文字が区別されます。
  - たとえば、descriptor=LDAP Realm と descriptor=ldap realm とは異なります。
- LDAP 領域の場合、*descriptor=* の値は LDAP Realm である必要があります。
- 複数の領域がある場合、領域タグ内の id= の値は領域ごとに一意である必要があります。 例：

```
<realm descriptor="LDAP Realm" id="LDAP" active="true">
```

以下の手順に従います。

1. <*EM_Home*>/config ディレクトリの realms.xml ファイルを開きます。
2. 認証方式として LDAP が構成されるように、以下のプロパティを設定します。

   LDAP による認証の場合、Introscope ユーザは、正しいユーザ ID を入力すれば、空のパスワードを使用しても Workstation にログインできます。LDAP による認証では、パスワードが入力されていないことや、パスワードフィールドが無効であることがチェックされないので、ユーザは正常にログインできてしまいます。 この LDAP の認証動作は、Workstation クライアントまたは WebView にログインする場合も同様です。 セキュリティを確実に適用するために、disallowEmptyPassword プロパティを設定します。

   注: LDAP サーバは、各サイトで構成が異なります。 LDAP プロパティを構成するには、LDAP 管理者から LDAP 構成情報をあらかじめ入手しておきます。

url

リモート LDAP サーバの URL。

非 SSL 接続のデフォルト ポートは 389 です。SSL 接続のデフォルト ポートは 636 です。

SSL を使用する場合は、SSL 用 LDAP ポートをサーバ URL に含める必要があります。

たとえば、ldap://host:port となります。

useSSL

リモート LDAP サーバに接続するために SSL を使用するかどうか。

オプション： true、false

bindName

LDAP コンピュータにバインドするために使用する名前。未指定の場合、匿名バインドが使用されます。

たとえば、IntroscopeLDAPUser となります。

bindPassword

LDAP コンピュータにバインドするために使用するパスワード。

このプロパティはオプションです。

bindName フィールドが空白の場合（匿名バインドを使用）、bindPassword プロパティは無視されます。

plainTextPasswords

bindPassword がプレーン テキストであるか、暗号化されているかを示します。 このプロパティはオプションです。

このプロパティがない場合または True に設定されている場合、Enterprise Manager は *bindPassword* プロパティがプレーン テキストであると見なします。

デフォルトでは、この値は *True* に設定されます。つまり、パスワードはプレーン テキストであると見なされます。

Enterprise Manager は、realms.xml ファイルを読み取り、この値が *True* に設定されていることを認識すると、以下のアクションを実行します。

- bindPassword プロパティのプレーン テキスト パスワードを暗号化します。
- 暗号化したパスワードを使用して realms.xml を書き直します。
- realms.xml の plainTextPasswords プロパティを *False* に設定します。

  値が False に設定されている場合、パスワードは暗号化されています。

重要: Enterprise Manager が起動するには、realms.xml ファイルにこのプロパティが含まれている必要があります。

bindAuthentication

バインド時に使用する認証の種類。

オプション： none、simple、DIGEST-MD5

baseDN

すべてのユーザ オブジェクト クエリのベース識別名（DN）

オプション： cn=Users、dc=dev、dc=com

scopeDepth

ユーザ オブジェクトのクエリを実行するときの検索の深さ。

usernameAttribute

Introscope ユーザ名に一致する LDAP 属性の名前。

たとえば、userPrincipalName となります。

userObjectQuery

ユーザ オブジェクトのクエリに使用する LDAP 検索フィルタ。トークン「%u」は、クエリが実行される前に Introscope ユーザ名で置き換えられます。

たとえば、(&(userPrincipalName=%u)(objectclass=user)) となります。

serverCertificate

証明書ファイルの名前。サポートされる証明書は、仕様が X.509 でエンコード方式が BASE64 の証明書です。

指定しない場合、JVM のデフォルト認証局の証明書が使用されます（http://java.sun.com/j2se/1.5/docs/index.html を参照）。

groupNameAttribute

Introscope ユーザ名と一致するグループ属性の名前。

たとえば、*cn* となります。

groupObjectQuery

グループ オブジェクトのクエリに使用する LDAP 検索フィルタ。トークン「%u」は、クエリが実行される前に Introscope グループ名で置き換えられます。

たとえば、(&(objectClass=group)(cn={0})) となります。

groupMemberQuery

グループ メンバのクエリに使用する LDAP 検索フィルタ。 トークン「%u」は、クエリが実行される前に Introscope グループ メンバで置き換えられます。

たとえば、(&(objectClass=group)(member={0})) となります。

disallowEmptyPassword

ユーザが空のパスワードでログインできないことを要求します。

disableNestedGroupSearch

LDAP 認証中に、ユーザが属するグループ内のネストしたグループに対して、LDAP 再帰検索を無効にします。true に設定すると、LDAP 認証のパフォーマンスを向上させることができます。

このプロパティはオプションです。

オプション： true、false デフォルトは false です。

3. 変更を適用するために、realms.xml ファイルへの変更内容を保存し、Enterprise Manager を再起動します。

注: 以下の条件に該当する場合、アップグレード後の手動タスクとして絶対パスを更新します。

- アップグレード時に Introscope ディレクトリの名前を変更した場合。
- プロパティ ファイルで Introscope のディレクトリ内のファイルの参照に絶対パスを使用している場合。

この状況を避けるには、Introscope ルート ディレクトリ内部のファイルの参照に相対パスを使用します。

LDAP による認証が有効になった realms.xml 構文

以下は、LDAP が有効になったセキュリティ領域を構成するための *realms.xml* 構文の例です。

```
<?xml version="1.0" encoding="UTF-8"?>
<realms xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="0.1"
xsi:noNamespaceSchemaLocation="realms0.1.xsd">

    <realm active="true" descriptor="LDAP Realm" id="LDAP">
        <!-- Set the URL for the remote LDAP server.    -->
        <!-- The url has the format: ldap://server:port -->
        <property name="url">
            <value>ldap://myActiveDirectoryServer.mydomain.com:389</value>
        </property>
        <!-- Indicate whether SSL is used to connect to the remote LDAP server. -->
        <property name="useSSL">
            <value>false</value>
        </property>
        <!-- The bindName can be set to a name or an empty string;    -->
        <!-- or it can be commented out. If a name is specified,      -->
        <!-- it will be used to bind to the LDAP server. If the name  -->
        <!-- is unspecified (empty string) or the property itself     -->
        <!-- commented out, then an anonymous bind will occur.        -->
        <property name="bindName">
            <value>CN=Automatic Binding User,OU=Groups,DC=myDomain,DC=com</value>
        </property>
        <!-- If we are doing an anonymous bind, then the bindPassword -->
        <!-- property is ignored. Otherwise, this property sets       -->
        <!-- the password to use when binding to the LDAP server.     -->
        <property name="bindPassword">
            <value>secretPassword</value>
        </property>
```

```
        <!-- Set to true if the bindPassword is plain text -->
        <!-- If plainTextPasswords is set to true, the Enterprise Manager overwrites
this file, -->
        <!-- encrypting the password and setting plainTextPasswords to false -->
        <!-- This property is optional -->
        <!-- Default is true -->
        <property name="plainTextPasswords">
            <value>true</value>
        </property>
        <!-- Set the type of authentication to use when binding.   -->
        <!-- Valid values: none|simple|Digest-MD5                  -->
        <!-- Note than in Introscope 8.0 DIGEST-MD5 support has been -->
        <!-- replaced with Digest-MD5 support.                     -->
        <property name="bindAuthentication">
            <value>simple</value>
        </property>
        <!-- The nameSuffix can be set to a suffix or empty string;   -->
        <!-- or it can be commented out. If a suffix is defined,      -->
        <!-- then the value will be appended to the Introscope user   -->
        <!-- name when dealing with LDAP queries. If the suffix is    -->
        <!-- unspecified (empty string) or the property itself is     -->
        <!-- commented out, then the name suffix will not be appended -->
        <!-- to the user name.                                        -->
      <!--
        <property name="nameSuffix">
            <value>@dev.com</value>
        </property>
      -->
        <!-- Set the base DN for all user object queries. -->
        <property name="baseDN">
            <value>DC=myDomain,DC=com</value>
        </property>
        <!-- Set the search depth when querying for a user object. -->
        <!-- Valid values: onelevel|subtree                        -->
        <property name="scopeDepth">
            <value>subtree</value>
        </property>
        <!-- Set the name of the LDAP attribute      -->
        <!-- that will match an Introscope username. -->
        <property name="usernameAttribute">
            <value>cn</value>
        </property>
```

```
        <!-- Set the "LDAP search filter" that is used to query a user object.  -->
        <!-- The tokens "%u" and "{0}" (no quotes) will be filled in with the   -->
        <!-- Introscope username before the query executes.                     -->
        <!-- All XML special characters in the query must be escaped:           -->
        <!--   Use &amp; to indicate an ampersand, &                            -->
        <!--   Use &lt; to indicate a left angle ("less than") character        -->
        <!--   Use &gt; to indicate a right angle ("greater than") character    -->
        <!--   Use &quot; to indicate a quotation mark, "                       -->
        <!--   Use &apos; to indicate an apostrophe, '                          -->
        <property name="userObjectQuery">
            <value>(&amp;(objectClass=organizationalPerson)(cn={0}))</value>
        </property>
        <!-- Optionally set the name of the LDAP attribute  -->
        <!-- to use as the group name.                      -->
    <!--
        <property name="groupNameAttribute">
           <value>cn</value>
        </property>
    -->
        <!-- Optionally set a search filter to match LDAP groups for a member.  -->
        <!-- The tokens "%u" and "{0}" (no quotes) will be replaced by the      -->
        <!-- member's distinguished name.                                       -->
        <!-- All XML special characters in the query must be escaped. See       -->
        <!-- comments for userObjectQuery property above.                       -->
     <!--
        <property name="groupMemberQuery">

<value>(&amp;(objectClass=groupOfUniqueNames)(uniquemember=%u))</value>
        </property>
     -->
        <!-- Set the search filter used to match an LDAP group name.            -->
        <!-- The tokens "%g" and "{0}" (no quotes) will be replaced by the      -->
        <!-- group name before the query executes.                              -->
        <!-- All XML special characters in the query must be escaped. See       -->
        <!-- comments for userObjectQuery property above.                       -->
     <!--
        <property name="groupObjectQuery">
            <value>(&amp;(objectClass=groupOfUniqueNames)(cn=%g))</value>
        </property>
     -->
        <!-- When using SSL, specify the full path name of -->
        <!-- the LDAP Server Certificate (if available).   -->
     <!-- It is not necessary to escape backslashes.    -->
     <!--
        <property name="serverCertificate">
            <value>C:¥path¥to¥my¥cert¥cert.cer</value>
        </property>
```

```
      -->
         property name="disallowEmptyPassword">
             <value>true</value>
         </property>
      </realm>
</realms>
```

異なる証明書を使用する複数の LDAP サーバ用の realms.xml 構文

複数の LDAP サーバに互換性のない異なる証明書がある場合、realms.xml を設定して適切にバインドできます。

この例では、host1 という名前の単一の LDAP ホスト（SSL 用にポート 636 を使用）が LDAP 認証を実行します。 host1 には、host1.pem という証明書が realms.xml にあります。 同じポート 636 を使用する host2 という別のホストを追加します。 realms.xml 内の host2 の証明書は host2.pem で、host1.pem 証明書と互換性がありません。

serverCertificate 値を host1.pem として設定すると、バインド操作が host2 ではなく host1 で行われます。 serverCertificate の値を host2.pem に設定すると、バインド操作が host1 ではなく host2 に対して行われます。

この問題を回避するには、以下の例のように realms.xml を設定します。

```
<property name="url">
<value>ldap://host1.net:636 ldap://host2.net:636</value>
</property>

<property name="serverCertificate">
    <VALUE>CONFIG/host1.PEM</VALUE>
    <VALUE>CONFIG/host2.PEM</VALUE>
</property>
```

この設定では、バインド操作が host1 および host2 の両方に対して行われます。

IBM Directory Server 用の realms.xml 構文

以下に示す *realms.xml* は、SSL を有効にして IBM Directory Server を使用する場合の LDAP プロパティの構成例です。

注: 以下のコード サンプルは例にすぎないことに注意してください。各サイトの LDAP サーバは、それぞれ構成が異なります。

```
<?xml version="1.0" encoding="UTF-8"?>
<realms xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="0.1"
xsi:noNamespaceSchemaLocation="realms0.1.xsd">
<realm active="true" descriptor="LDAP Realm" id="LDAP">
<property name="url">
<value>ldap://machine01.co.com:123</value>
</property>
<property name="serverCertificate">
<value/>
</property>
<property name="bindPassword">
<value>jon</value>
</property>
<property name="useSSL">
<value>false</value>
</property>
<property name="userObjectQuery">
<value>(&amp;(objectClass=organizationalPerson)(cn={0})) </value>
</property>
<property name="groupNameAttribute">
           <value>cn</value>
        </property>
        <property name="groupObjectQuery">
           <value>(&amp;(objectClass=organizationalUnit)(cn={0}))</value>
        </property>
        <property name="groupMemberQuery">
           <value>(&amp;(objectClass=groupofNames)(member={0}))</value>
        </property>
<property name="bindAuthentication">
<value>simple</value>
</property>
<property name="bindName">
<value>cn=Jon Doe,ou=Groups,o=unitTest</value>
</property>
```

```
<property name="usernameAttribute">
<value>cn</value>
</property>
<property name="scopeDepth">
<value>subtree</value>
</property>
</realm>
</realms>
```

Sun ONE Directory Server 用の realms.xml 構文

以下に示す *realms.xml* は、SSL を有効にして Sun ONE Directory Server を使用する場合の LDAP プロパティの構成例です。

注: 以下のコード サンプルは例にすぎないことに注意してください。各サイトの LDAP サーバは、それぞれ構成が異なります。

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<realms xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="0.1"
xsi:noNamespaceSchemaLocation="realms0.1.xsd">
    <realm active="true" id="Introscope LDAP Realm" descriptor="LDAP Realm">
        <property name="bindName">
           <value>uid=User01,ou=Users,dc=co,dc=com</value>
        </property>
        <property name="scopeDepth">
           <value>subtree</value>
        </property>
        <property name="baseDN">
           <value>DC=co,DC=com</value>
        </property>
        <property name="bindPassword">
           <value>jim</value>
        </property>
        <property name="url">
           <value>ldap://123serv01.company.com:389</value>
        </property>
        <property name="usernameAttribute">
           <value>cn</value>
        </property>
        <property name="userObjectQuery">
           <value>(&amp;(objectClass=organizationalPerson)(cn={0}))</value>
        </property>
        <property name="groupNameAttribute">
           <value>cn</value>
        </property>
```

```
        <property name="groupObjectQuery">
           <value>(&amp;(objectClass=group)(cn={0}))</value>
        </property>
        <property name="groupMemberQuery">
           <value>(&amp;(objectClass=group)(member={0}))</value>
        </property>
        <property name="useSSL">
           <value>false</value>
        </property>
        <property name="bindAuthentication">
           <value>simple</value>
        </property>
        <property name="serverCertificate">
           <value/>
        </property>
    </realm>
</realms>
```

Microsoft Active Directory 用の realms.xml 構文

以下に示す *realms.xml* は、SSL を有効にして Microsoft Active Directory を使用する場合の LDAP プロパティの構成例です。

注: 以下のコード サンプルは例にすぎないことに注意してください。各サイトの LDAP サーバは、それぞれ構成が異なります。

```
<?xml version="1.0" encoding="UTF-8"?>
<realms xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="0.1"
xsi:noNamespaceSchemaLocation="realms0.1.xsd">

<realm active="true" descriptor="LDAP Realm" id="LDAP">
<property name="url">
<value>ldap://123serv01.company.com:389:389</value>
</property>
<property name="serverCertificate">
<value/>
</property>
<property name="bindPassword">
<value>Password4bindPassword</value>
</property>
<property name="useSSL">
<value>false</value>
</property>
<property name="userObjectQuery">
<value>(&amp;(objectClass=organizationalPerson)(cn={0})) </value>
</property>
```

```
<property name="baseDN">
<value>DC=ad-dev-02,DC=com</value>
</property>
<property name="bindAuthentication">
<value>simple</value>
</property>
<property name="bindName">
<value>CN=Jon Doe,cn=Users,DC=ad-dev-02,DC=com</value>
</property>
<property name="usernameAttribute">
<value>cn</value>
</property>
<property name="scopeDepth">
<value>subtree</value>
</property>
</realm>
</realms>
```

CA EEM による Introscope のセキュリティ保護

CA EEM は、一般的なアクセス ポリシーの管理、認証、および許可の各サービスを他のアプリケーションが共有できるようにする、エンタープライズ全体の CA Technologies ポリシー サーバです。 複数の Embedded Entitlements のクライアント アプリケーションをサポートする一元化された Embedded Entitlements サーバで構成されます。

詳細については、次の CA EEM ガイドを参照してください。これらは、CA サポートサイト(http://support.ca.com)からダウンロードされた CA EEM アプリケーションに付属しています。

- *CA Embedded Entitlements Manager Getting Started Guide*
- *CA Embedded Entitlements Manager Programming Guide*
- *CA Embedded Entitlements Manager Release Notes*

CA EEM のデプロイ オプション

Introscope のセキュリティは、CA EEM を使用して以下の複数の方法で設定できます。

- 認証と許可の両方に CA EEM をデプロイします。 詳細については、「realms.xml での CA EEM による認証の構成 (P. 76)」および「CA EEM による許可の構成 (P. 82)」を参照してください。
- CA EEM サーバを LDAP サーバに統合する設定を行った場合は、認証に LDAP、許可に CA EEM を使用できます。 詳細については、「LDAP を使用した CA EEM による認証の構成 (P. 80)」を参照してください。
- CA EEM サーバを SiteMinder に統合する設定を行った場合は、認証に SiteMinder、許可に CA EEM を使用できます。 詳細については、「CA SiteMinder による CA EEM による認証の構成」を参照してください。
- 認証専用に CA EEM をデプロイし、許可にローカルによるセキュリティを使用します。 詳細については、「ローカル許可を使用するための CA EEM の構成 (P. 125)」を参照してください。

注: CA APM は EEM 8.4 SP4 SDK を提供し、EEM サーバ バージョン 8.4 SP4 以降で認定されています。

重要: ローカルによるセキュリティを許可に使用すると、アプリケーション問題切り分けマップのセキュリティの提供や、CA CEM 内のタブとデータの表示を制御するアクセス ポリシーの設定などができなくなります。 CA CEM でアプリケーション問題切り分けマップを提供し、アクセス ポリシーを使用する場合は、許可に CA EEM をデプロイする必要があります。

CA EEM によるセキュリティを設定および維持するプロセス

Introscope のセキュリティの背景知識を理解したら、今度は Introscope の CA EEM によるセキュリティのデプロイ計画に進むことができます。 手順の概要は以下のとおりです。

以下の手順に従います。

1. CA EEM サーバをインストールします。 「CA EEM のインストール (P. 74)」を参照してください。
2. （オプション）。CA EEM ログ メッセージを提供するための *IntroscopeEnterpriseManager.properties* ファイルを構成します。 「CA EEM 関連メッセージのログ記録の構成 (P. 75)」を参照してください。

3. 各 Enterprise Manager で、CA EEM をセキュリティ領域として定義し、*<EM_Home>/config* ディレクトリにある *realms.xml* ファイルで認証と許可のプロパティを設定します。「realms.xml での CA EEM による認証の構成 (P. 76)」を参照してください。

   注: CA EEM サーバが LDAP サーバまたは CA SiteMinder Web Access Manager (SiteMinder) サーバのいずれかに統合されている場合は、ユーザ認証に LDAP または SiteMinder が使用されるように CA EEM を構成できます。

4. (オプション) CA EEM による認証で LDAP を構成します。「LDAP を使用した CA EEM による認証の構成 (P. 80)」を参照してください。

5. (オプション) CA EEM による認証で SiteMinder を構成します。「CA SiteMinder を使用した CA EEM による認証の構成 (P. 80)」を参照してください。

6. (オプション。ただし、推奨) *<EM_Home>/examples/authentication* ディレクトリにある *eem.register.app.xml* と *eem.add.global.identities.xml* のスクリプトをロードします。「CA EEM による許可の構成 (P. 82)」を参照してください。

   注: CA Technologies では、APM アプリケーションのデフォルトのユーザ、グループ、リソース、および権限を使用して APM アプリケーションを作成するサンプル スクリプトを用意しています。以下の手順 7 から手順 10 を実行するときは、これらのスクリプトを使用することをお勧めします。詳細については、「CA EEM による許可の構成 (P. 82)」を参照してください。

7. CA EEM 内で 1 つ以上の APM アプリケーションを作成します。「CA EEM での APM アプリケーションの登録 (P. 88)」を参照してください。

8. CA EEM 内で APM グループとユーザ、およびそれらの権限を作成します。「CA EEM での APM グループの作成と削除 (P. 93)」および「CA EEM での APM ユーザの作成と削除 (P. 98)」を参照してください。

9. CA EEM 内で APM リソース クラスおよびそれらの権限を作成します。「CA EEM での APM リソース クラスの作成と削除 (P. 102)」を参照してください。

10. CA EEM 内で APM ドメイン、サーバ、APM アプリケーション リソース、およびそれらの権限を作成します。「CA EEM APM ドメイン リソース アクセス ポリシーの作成と削除 (P. 111)」、「CA EEM APM サーバ リソース アクセス ポリシーの作成と削除 (P. 115)」、および「CA EEM APM フロントエンドおよびビジネス サービス リソース アクセス ポリシーの作成と削除 (P. 119)」を参照してください。

11. Enterprise Manager を再起動します。
12. CA EEM ベースのセキュリティを強化および維持するには、必要に応じて以下のタスクを実行します。
    - CA EEM のアクティビティとエラーをレポートするログ メッセージを構成する。「CA EEM 関連メッセージのログ記録の構成 (P. 75)」を参照してください。
    - CA EEM による認証で CA EEM サーバを LDAP または SiteMinder に統合する構成を行う。 「LDAP を使用した CA EEM による認証の構成 (P. 80)」または「CA SiteMinder を使用した CA EEM による認証の構成 (P. 80)」を参照してください。
    - 複数の領域を定義する。 たとえば、認証に CA EEM、許可にローカルを定義します。「ローカル許可を使用するための CA EEM の構成 (P. 125)」を参照してください。
    - CA APM スクリプトを変更するか、または独自のスクリプトを作成する。 「CA EEM による許可の構成 (P. 82)」を参照してください。
    - APM アプリケーションを追加または削除する。「CA EEM での APM アプリケーションの登録 (P. 88)」を参照してください。
    - APM グループおよびそれらの権限を追加、編集、または削除する。「CA EEM での APM グループの作成と削除 (P. 93)」を参照してください。
    - APM ユーザおよびそれらの権限を追加、編集、または削除する。「CA EEM での APM ユーザの作成と削除 (P. 98)」を参照してください。
    - APM リソース クラスおよびそれらの権限を追加、編集、または削除する。「CA EEM での APM リソース クラスの作成と削除 (P. 102)」を参照してください。
    - APM ドメイン リソースおよびそれらの権限を追加、編集、または削除する。
      - CA EEM 内の場合。 「CA EEM APM ドメイン リソース アクセス ポリシーの作成と削除 (P. 111)」を参照してください。
      - ローカル許可の場合は、*domains.xml* 内で更新。 「domains.xml での Introscope ドメイン権限の構成 (P. 50)」を参照してください。

- Enterprise Manager サーバ リソースおよびそれらの権限を追加、編集、または削除する。
  - CA EEM 内の場合。「CA EEM APM サーバ リソース アクセス ポリシーの作成と削除 (P. 115)」を参照してください。
  - ローカル許可の場合は、*server.xml* 内で更新。「Enterprise Manager サーバ権限の構成 (P. 54)」を参照してください。
- Enterprise Manager アプリケーション リソースおよびそれらの権限を追加、編集、または削除する。「CA EEM APM フロントエンドおよびビジネス サービス リソース アクセス ポリシーの作成と削除 (P. 119)」を参照してください。

CA EEM のインストール

CA EEM は、Enterprise Manager と同じコンピュータにインストールできるスタンドアロン サーバ コンポーネントです。 CA EEM の要件については、「*CA Embedded Entitlements Manager Release Notes*」を参照してください。

CA EEM のインストールについては、「CA APM インストールおよびアップグレード ガイド」を参照してください。 CA EEM のインストールに関する追加情報については、以下の CA EEM ガイドを参照してください。これらは、CA EEM 製品インストール ファイルに付属しています。

- CA Embedded Entitlements Manager Getting Started Guide
- CA Embedded Entitlements Manager Release Notes

重要: CA EEM データ ストアおよびサーバ フェールオーバを処理するために CA EEM を構成できます。 詳細については、「*CA Embedded Entitlements Manager Getting Started Guide*」を参照してください。

CA EEM サーバには、APM アプリケーション、ユーザ、およびグループのデータを CA EEM にインポートできる Safex ユーティリティが付属しています。 詳細については、「CA EEM による許可の構成 (P. 82)」を参照してください。

（オプション）CA EEM 関連メッセージのログ記録の構成

IntroscopeEntrerpriseManager.properties ファイルを更新して、詳細な CA EEM ログ メッセージを提供できます。このログ メッセージは、CA EEM エラーのトラブルシューティングに役立ちます。たとえば、ユーザが CA EEM へのログインに失敗する場合や、そのユーザに対して権限が設定されていない場合などです。

以下の手順に従います。

1. <EM_Home>/config ディレクトリに移動します。
2. IntroscopeEntrerpriseManager.properties ファイルを開きます。
3. 以下のプロパティを、IntroscopeEntrerpriseManager.properties ファイルに追加します。

   ```
   log4j.logger.Manager.EemRealm=DEBUG
   log4j.logger.additivity.Manager.EemRealm=false
   ```

4. IntroscopeEntrerpriseManager.properties ファイルを保存して閉じます。

   <EM_Home>/logs/IntroscopeEnterpriseManager.log ファイル内のログ メッセージの CA EEM 接続情報、およびデバッグ メッセージを確認できます。 ログ メッセージには、Enterprise Manager が CA EEM 内で接続しているアプリケーションと、CA EEM サーバの場所が表示されます。ユーザとグループを取得するために SiteMinder または外部ディレクトリ（LDAP 領域）が使用されるように CA EEM サーバを構成している場合は、それらの情報もログに記録されます。

   例：

   ```
   8/05/09 04:15:59 PM PDT [INFO] [Manager.EemRealm] EEM realm attached to
   application "APM" in EEM server at <EEM_Machine_Name> using SiteMinder
   ```

realms.xml での CA EEM による認証の構成

realms.xml ファイルで CA EEM をセキュリティ領域として構成すると、Introscope は認証に CA EEM を使用します。

CA EEM サーバは各組織でそれぞれ独自の方法で構成されるので、*realms.xml* の CA EEM プロパティを構成する前に、CA EEM 構成情報を取得する必要があります。 CA EEM をインストールしなかった場合は、この情報について組織の CA EEM 管理者に問い合わせてください。 また、認証対象の CA APM ユーザの権限が CA EEM サーバで定義されていることを確認する必要があります。 CA EEM サーバでの CA APM ユーザの設定については、「CA EEM での APM ユーザの作成と削除 (P. 98)」を参照してください。

realms.xml を構成するときは、以下のルールに従います。

重要: これらのルールのいずれかに従わなかった場合、Enterprise Manager は起動しません。

- *descriptor=* の値は大文字と小文字が区別されます。
  - たとえば、*descriptor=EEM Realm* と *descriptor=eem realm* とは異なります。
- EEM 領域の場合、*descriptor=* の値は *EEM Realm* である必要があります。
- 複数の領域がある場合、領域タグ内の *id=* の値は領域ごとに一意である必要があります。 例：
  - *<realm descriptor="EEM Realm" id="EEM Server 1" active="true">*
  - *<realm descriptor="EEM Realm" id="EEM Server 2" active="true">*

場合によっては複数の領域を設定することがありますが、たとえば、ユーザに基本的な権限を与えるデフォルト領域と、別の権限を与える第 2 の領域が必要な場合です。また、2 台の LDAP サーバがあり、その両方のセキュリティをテストすることもあります。 あるいは、これまでローカルによるセキュリティを使用していて、CA EEM に移行する際にローカルによるセキュリティを維持したい場合もあると思います。

realms.xml が間違って構成されていると、Enterprise Manager はエラー メッセージを表示します。 たとえば、以下のようになります。

```
4/13/10 03:06:32.960 PM PDT [ERROR] [main] [Manager] The EM failed to start. Invalid
realm descriptor in the EEM realm descriptor: eem realm
```

以下の手順に従います。

注: *APM* という名前のアプリケーションに基づいたサンプルの EEM 領域については、*<EM_Home>/examples/authentication* ディレクトリにあるサンプルの *realms.eem.xml* 構成ファイルを参照してください。

1. *<EM_Home>/config* ディレクトリの *realms.xml* ファイルを開きます。
2. 以下のプロパティを適宜設定します。

   注: 認証と許可の両方に CA EEM サーバを使用するには、*enableAuthorization* プロパティの値をデフォルトのまま（*true*）にします。 この値を *false* に設定した場合、CA EEM は認証だけを実行し、許可にはローカルによるセキュリティ領域を使用します。 たとえば、LDAP または SiteMinder で構成された CA EEM を認証に使用すると同時に、権限をローカル領域に維持する場合は、ローカル許可を使用することもできます。

   host

   CA EEM サーバのホスト名。 このプロパティはオプションです。

   appname

   Enterprise Manager が CA EEM 内で接続する APM アプリケーションの名前。 このプロパティは必須です。

   username

   CA EEM サーバに接続するユーザの名前。 このプロパティはオプションです。

   CA EEM のデフォルト値は *EiamAdmin* です。

   password

   CA EEM サーバへの接続に使用するパスワード。 このプロパティは必須です。

   CA EEM のデフォルト値は *EiamAdmin* です。

plainTextPasswords

パスワードがプレーン テキストで保存されているか、暗号化して保存されているかを示します。 このプロパティは必須です。

Enterprise Manager は、*realms.xml* ファイルを読み取って、この値が *True* に設定されていることを認識すると、以下の操作を行います。

- プレーン テキスト パスワードを暗号化します。
- 暗号化したパスワードを使用して *realms.xml* を書き直します。
- *realms.xml plainTextPasswords* プロパティを *False* に設定します。

値が *False* に設定されると、パスワードは暗号化されていると見なされます。

重要: このプロパティが *realms.xml* ファイル内に含まれていない場合は、Enterprise Manager は起動せず、エラー メッセージが表示されます。

EnableAuthorization

CA EEM による許可を有効化します。 このプロパティはオプションです。

デフォルトでは、この値は *True* に設定されます。つまり、CA EEM は認証と許可に使用されます。

この値を *False* に設定した場合、CA EEM は認証だけに使用され、ローカル許可が使用されます。

3. *realms.xml* ファイルを保存します。
4. Enterprise Manager を再起動して *realms.xml* への変更を適用します。

CA EEM による認証が有効になった realms.xml 構文の例

以下は、*realms.xml* で CA EEM 対応のセキュリティ領域を構成するための構文の例です。

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<realms xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="0.1"
xsi:noNamespaceSchemaLocation="realms0.1.xsd">
    <realm descriptor="EEM Realm" id="EEM" active="true">
        <!-- Set the hostname of the EEM server -->
        <!-- This property is optional -->
        <!-- Default is localhost -->
            <value>localhost</value>
        </property>
```

```
        <!-- Set the name of the EEM application to attach to -->
        <!-- This property is required -->
        <!--
        <property name="appname">
            <value>MyIntroscopeApp</value>
        </property>
        -->
        <!-- Set the user name to connect to the EEM server -->
        <!-- This property is optional -->
        <!-- Default is EiamAdmin -->
        <property name="username">
            <value>EiamAdmin</value>
        </property>
        <!-- Set the password to connect to the EEM server -->
        <!-- This property is required -->
        <property name="password">
            <value>EiamAdmin</value>
        </property>
        <!-- Set to true if the password is plain text -->
        <!-- If plainTextPasswords is set to true, the Enterprise Manager overwrites
this file, -->
        <!-- encrypting the password and setting plainTextPasswords to false -->
        <!-- This property is required -->
        <property name="plainTextPasswords">
            <value>true</value>
        </property>
        <!-- Enable authorization in the EEM server -->
        <!-- If set to false, the EEM server is used for authentication only -->
        <!-- This property is optional -->
        <!-- Default is true -->
        <property name="enableAuthorization">
            <value>true</value>
        </property>
    </realm>
</realms>
```

LDAP を使用した CA EEM による認証の構成

お使いの CA EEM サーバが、CA EEM がサポートする LDAP サーバに統合されている場合は、認証に LDAP サーバが使用されるように CA EEM を構成できます。 この場合、ユーザとグループは LDAP に属します。 認証の目的で CA EEM サーバが LDAP サーバに統合される場合、Introscope での追加構成は一切必要ありません。 Introscope がサポートする LDAP サーバの詳細については、「LDAP による Introscope のセキュリティ保護 (P. 57)」を参照してください。

注: CA EEM を複数の外部ディレクトリ（LDAP と SiteMinder など）に同時に統合されるように構成することはできません。

LDAP を使用して CA EEM による認証を構成するとき、許可には CA EEM をデプロイします。 詳細については、「CA EEM による許可の構成 (P. 82)」を参照してください。

以下の手順に従います。

1. CA EEM 対応の LDAP サーバ（SUN ONE LDAP サーバなど）を設定および構成します。
2. LDAP ユーザ ディレクトリにユーザとグループを追加します。

   注: CA EEM サーバを LDAP などの外部ユーザ ディレクトリに接続すると、CA EEM 内でグローバル ユーザを作成または追加することができなくなります。
3. CA EEM の［設定］タブで、LDAP サーバまたは Active Directory サーバに接続するように CA EEM を構成します。

   詳細については、「*CA Embedded Entitlements Manager Getting Started Guide*」および「*CA Embedded Entitlements Manager Programming Guide*」で、LDAP 関連のトピックを参照してください。

CA SiteMinder を使用した CA EEM による認証の構成

SiteMinder は一元化された Web アクセス管理システムで、以下の機能を持ちます。

- ユーザ認証およびシングル サインオン
- 認証管理
- ポリシー ベースでの許可

- アイデンティティ フェデレーション
- Web アプリケーションおよびポータルへのアクセス監査

認証に SiteMinder が使用されるように CA EEM を構成できます。 この場合、ユーザとグループは SiteMinder に属します。 認証の目的で CA EEM サーバが SiteMinder に統合される場合、Introscope での追加構成は一切必要ありません。

CA EEM で SiteMinder を使用して認証を行うように構成する場合は、CA EEM をデプロイして許可を行います。 詳細については、「CA EEM による許可の構成 (P. 82)」を参照してください。

注: CA EEM を複数の外部ディレクトリ（LDAP と SiteMinder など）に同時に統合するように構成することはできません。

以下の手順に従います。

1. SiteMinder ユーザ ディレクトリにユーザとグループを追加します。

   注: CA EEM サーバを SiteMinder などの外部ユーザ ディレクトリに接続すると、CA EEM 内でグローバル ユーザを作成または追加することができません。

2. CA EEM の［設定］タブで、SiteMinder に接続するように CA EEM を構成します。

   注: CA EEM の SiteMinder への統合の詳細については、以下のガイドの関連するトピックを参照してください。

   - *CA Embedded Entitlements Manager Getting Started Guide*
   - CA Embedded Entitlements Manager Release Notes

   注: サンプルのデプロイについては、ナレッジ ベース（KB）の記事 TEC534187 「CA Wily APM security example: CA SiteMinder for authentication with CA EEM for authorization」を参照してください。

CA EEM による許可の構成

許可領域として CA EEM を使用する場合は、APM アプリケーションおよび APM のユーザ、グループおよび権限で CA EEM サーバを構成する必要があります。 これには、以下のいずれかの方法を使用できます。

- CA EEM Safex ユーティリティ

  Safex は、CA EEM に付属するコマンド ライン インターフェース（CLI）ユーティリティです。 Safex は、XML スクリプトを実行して CA EEM にアプリケーションを登録し、ユーザとグループを作成します。

  CA APM では、デフォルトの APM グローバル ユーザ、リソース、および権限を使用して APM アプリケーションを作成する Safex のサンプル スクリプトを用意しています。
  また、Safex スクリプトを使用して CA EEM から XML ファイルにデータをエクスポートすることもできます。詳細については、「*CA Embedded Entitlements Manager Programming Guide*」を参照してください。

- CA EEM インターフェース

  CA EEM インターフェースの使用については、「*CA Embedded Entitlements Manager Getting Started Guide*」および「*CA Embedded Entitlements Manager Online Help*」を参照してください。

  サンプルのデプロイについては、ナレッジ ベース（KB）の記事 TEC534188 「CA Wily APM security example: Setting up CA Wily APM users, groups, and resources in CA EEM」を参照してください。

CA EEM インターフェースにアクセスする方法

アクセス権がある場合は、CA EEM にログインして APM アプリケーションおよび APM のユーザ、グループおよび権限を設定することができます。

- CA EEM 内の APM アプリケーションにログインします。

  a. CA EEM ログイン ページで、APM または登録済みアプリケーションの名前を［アプリケーション］ドロップダウン リストでクリックします。

  b. ログイン名とパスワードを入力します。

  APM アプリケーションのデフォルト ログイン名は *EiamAdmin* です。

非 FIPS モードで APM-CA EEM 統合を設定する方法

注: EEM のインストール場所にある igateway.conf ファイルで <FIPSMode>OFF</FIPSMode> を使用して FIPS モードを OFF に設定して、非 FIPS モードで EEM サーバを設定します。 このファイルのデフォルトのインストール場所は、C:¥ProgramFiles¥CA¥SharedComponents¥iTechnology です。

1. eiam.config ファイルと eiam.log4j.config ファイルを設定します。
   - <EM install>¥config ディレクトリ内の eiam.config および eiam.log4j.config ファイルを開きます。
   - FIPS モードが OFF に設定され、<FIPSMode>OFF</FIPSMode> と表示されていることを確認します。 デフォルトのモードは OFF です。
2. ダイジェスト アルゴリズムを以下のいずれかのアルゴリズムに設定します。
   - MD5 （デフォルト）
   - SHA1
   - SHA256
   - SHA384
   - SHA512

   APM-EEM 統合が非 FIPS モードで設定されます。

FIPS モードで APM-CA EEM 統合を設定する方法

注: EEM のインストール場所にある igateway.conf ファイルで <FIPSMode>ON</FIPSMode> を使用して FIPS モードを ON に設定して、FIPS モードで EEM サーバを設定します。 このファイルのデフォルトのインストール場所は、C:¥Program Files¥CA¥SharedComponents¥iTechnology です。

1. eiam.config ファイルと eiam.log4j.config ファイルを設定します。
   - <EM install>¥config ディレクトリ内の eiam.config および eiam.log4j.config ファイルを開きます。
   - <FIPSMode>OFF</FIPSMode> を <FIPSMode>ON</FIPSMode> に変更することにより、FIPS モードを ON に設定します。
2. ダイジェスト アルゴリズムを以下のいずれかのアルゴリズムに設定します。
   - SHA1
   - SHA256
   - SHA384
   - SHA512

   APM-EEM 統合が FIPS モードで設定されます。

CA EEM による許可を構成する方法

重要: CA EEM を許可に使用する場合、Enterprise Manager は CA EEM 内の 1 つ以上のアプリケーションに接続する必要があります。 CA EEM では、権限を定義するアクセス ポリシーおよびリソース クラスを格納するためにアプリケーションを使用しています。

重要: CA EEM サーバを LDAP または SiteMinder などの外部ユーザ ディレクトリに接続すると、CA EEM 内でグローバル ユーザを作成または追加することができません。認証のために、CA EEM サーバが LDAP サーバまたは SiteMinder サーバに統合されている場合は、CA EEM ではなく LDAP または SiteMinder 内でユーザとグループを設定します。あるいは、LDAP または SiteMinder 内でユーザとグループの CA EEM アクセス ポリシーを変更します。

重要: *eem.register.app.xml* スクリプトには、認証のために LDAP または SiteMinder を使用して構成された CA EEM を設定するためのサンプル コードが含まれません。

以下の手順に従います。

1. CA EEM による許可のための *realms.xml* ファイルを構成します。
   a. *<EM_Home>/config* ディレクトリの *realms.xml* ファイルを開きます。
   b. *appname* プロパティが、Enterprise Manager が CA EEM 内で接続している APM アプリケーションの名前に設定されていることを確認します。 たとえば、*APM* となります。

      以下の手順 2a で CA EEM サーバを構成するときに使用するものと同じアプリケーション名を使用します。
   c. *enableAuthorization* プロパティが *True* に設定されていることを確認します。
   d. *realms.xml* ファイルを保存します。
   e. Enterprise Manager を再起動して *realms.xml* への変更を適用します。
2. 1 つ以上の Safex スクリプトを作成、実行して、APM アプリケーション、グループ、ユーザ、リソース クラス、およびドメインとサーバのリソースをロードします。

   CA Technologies では、*<EM_Home>/examples/authentication* ディレクトリに、これらの Safex サンプル スクリプトを用意しています。

   eem.register.app.xml

   デフォルトの APM アプリケーションを登録します。

   eem.unregister.app.xml

   デフォルトの APM アプリケーションを登録解除します。

   eem.add.global.identities.xml

   デフォルトの APM グローバル ユーザを追加します。

   eem.remove.global.identities.xml

   デフォルトの APM ユーザを削除します。

   注: CA EEM による許可のデプロイを設定するためのベース スクリプトとして使用する *eem.register.app.xml* および *eem.add.global.identities.xml* に変更を加えることをお勧めします。これらのスクリプトを実行すると、CA EEM による許可を設定するための要件が満たされます。

a. Safex スクリプト内でこれらの CA EEM によるセキュリティのエレメントを構成します。

- アプリケーション。「CA EEM でのアプリケーションの登録 (P. 88)」を参照してください。
- グループ。「CA EEM での APM グループの作成と削除 (P. 93)」を参照してください。
- ユーザ。「CA EEM での APM ユーザの作成と削除 (P. 98)」を参照してください。

注: CA EEM は空のパスワードをサポートしません。したがって、CA EEM でユーザを作成するたびに、パスワードを指定する必要があります。

- リソース クラス。「CA EEM での APM リソース クラスの作成と削除 (P. 102)」を参照してください。
- ドメイン リソース権限。「CA EEM での APM リソース クラスの作成と削除 (P. 102)」を参照してください。
- サーバ リソース権限。「CA EEM APM サーバ リソース アクセス ポリシーの作成と削除 (P. 115)」を参照してください。

b. オプション： CA EEM 構成スクリプトのベースとして *eem.register.app.xml* ファイルを使用しない場合は、 CA EEM インターフェースを使用して、これらの条件が満たされるように CA EEM サーバを構成します。

- *ドメイン リソース クラス*と*サーバ リソース クラス*の 2 つのリソース クラスを作成します。

  リソース クラスには、Introscope で利用可能な権限と一致するアクションのリストが含まれている必要があります。 たとえば、サーバ権限の場合、Introscope のアクションは、*shutdown*、*publish_mib*、および *full* です。 詳細については、「CA EEM APM ドメイン リソース アクセス ポリシーの作成と削除 (P. 111)」および「CA EEM APM サーバ リソース アクセス ポリシーの作成と削除 (P. 115)」を参照してください。

- ポリシー セットを作成します。ポリシーによって、リソース クラス、1 つ以上のアクション、1 つ以上の ID、およびゼロまたは 1 つ以上のリソースが定義されます。
  - リソースは特定のリソースの名前です（*スーパードメイン*など）。リソースが指定されない場合、ポリシーはそのリソース クラスのすべてのインスタンスに適用されます。 *サーバ リソース クラス*はシングルトンなので、そのポリシーにリソースが含まれていてはいけません。
  - *ID* はグループの名前です。
- アプリケーション固有のユーザ グループを指定するには、プレフィックス *ug:* を使用します。また、組織のデプロイ環境に応じて、グローバル ユーザ グループを指定するには、*gug:* を使用します。

3. *<EEM_Server>* ディレクトリに移動します。このディレクトリは通常、以下の場所にあります。

   ```
   C:¥Program Files¥CA¥SharedComponents¥iTechnology
   ```

4. コマンド プロンプトで、以下のコマンドを実行します。

   ```
   C:¥Program Files¥CA¥SharedComponents¥iTechnology¥safex.exe -h hostname -u
   username -p password -f <Safex スクリプト名>.xml
   ```

   たとえば、以下のようになります。

   ```
   C:¥Program Files¥CA¥SharedComponents¥iTechnology¥safex.exe -h hostname -u
   username -p password -f eem.register.app.xml
   ```

   スクリプトが実行され、定義した構成値が CA EEM にロードされます。

5. CA EEM にログインし、APM アプリケーション、グループ、ユーザ、リソース クラス、ドメインとサーバのリソース、および関連する権限を表示します。
   a. APM アプリケーションのリストを表示するには、［設定］タブをクリックします。
   b. APM グループおよびユーザを表示するには、［ID の管理］タブをクリックします。
   c. APM リソース クラスおよびドメインとサーバのリソースを表示するには、［アクセス ポリシーの管理］タブをクリックします。

CA EEM での APM アプリケーションの登録

Introscope のセキュリティに使用するアプリケーションを CA EEM で 1 つ以上登録します。 CA EEM でアプリケーションを登録すると、ユーザの詳細情報とアクセス ポリシーを格納するアプリケーション インスタンスが作成されます。 ユーザとアプリケーションの操作の詳細については、以下の CA EEM のドキュメントを参照してください。

- *CA Embedded Entitlements Manager Getting Started Guide*
- *CA Embedded Entitlements Manager Online Help*
- *CA Embedded Entitlements Manager Programming Guide*

CA APM では、CA EEM アプリケーションを *APM* の名前で登録するデフォルトの Safex スクリプトを用意しています。

重要: CA EEM でアプリケーションを登録するには、Safex スクリプトを使用します。 CA EEM ユーザ インターフェースを使用してアプリケーションを登録することはできません。

注: *APM* という名前のアプリケーションを作成する Safex スクリプト コードについては、*<EM_Home>/examples/authentication* ディレクトリにある *eem.register.app.xml* サンプル ファイルを参照してください。

非 FIPS モードの CA EEM で APM アプリケーションを登録する方法

1. *<EEM_Server>* ディレクトリ内に Safex XML ファイルを作成します。このディレクトリは通常、*C:¥Program Files¥CA¥SharedComponents¥iTechnology* にあります。

   たとえば、以下のようになります。

   ```
   C:¥Program Files¥CA¥SharedComponents¥iTechnology ¥Register_APM.xml.
   ```

2. Safex XML ファイルに以下のコードをカット アンド ペーストし、引用符内の変数を各自の変数に置き換えます。

   ```
   <Safex>
      <!-- Attach as global user -->
      <Attach/>
      <!-- register "APM" application -->
      <Register certfile="APM.p12" password="Enter Your Password">
         <ApplicationInstance name="APM" label="APM">
         </ApplicationInstance>
      </Register>
      <Detach/>
   </Safex>
   ```

3. コマンドプロンプトを開き、*<EEM_Server>* ディレクトリに移動します。通常は、*C:¥Program Files¥CA¥SharedComponents¥iTechnology* です。

4. Safex スクリプトを実行するには、以下のコマンドを実行します。

   ```
   >safex.exe -h localhost -u EiamAdmin -p <パスワード> -f <ファイル名>.xml
   ```

   たとえば、以下のようになります。

   ```
   >safex.exe -h localhost -u EiamAdmin -p <パスワード> -f Register_APM.xml
   ```

5. CA EEM 内の APM アプリケーションを表示します。

   a. スクリプトに入力した管理者名とパスワードを使用して、CA EEM にログインします。

      たとえば、ユーザ名に *EiamAdmin*、パスワードに *<パスワード>* を使用します。

      注: CA EEM では、デフォルトのグローバル権限を持つ管理者名ユーザ名として *EiamAdmin* を使用できます。

   b. APM アプリケーションのリストを表示するには、［設定］タブをクリックします。

   c. そのアプリケーションに関する情報を表示または編集するには、アプリケーション名（APM など）をクリックします。

FIPS モードの CA EEM で APM アプリケーションを登録する方法

重要: CA EEM でアプリケーションを登録するには、Safex スクリプトを使用します。CA EEM ユーザ インターフェースを使用してアプリケーションを登録することはできません。

注: APM という名前のアプリケーションを作成する Safex スクリプト コードについては、<EM_Home>/examples/authentication ディレクトリにある eem.register.app.xml サンプル ファイルを参照してください。

1. <EEM_Server> ディレクトリ内に Safex XML ファイルを作成します。このディレクトリは通常、C:¥Program Files¥CA¥SharedComponents¥iTechnology にあります。

   たとえば、以下のようになります。

   ```
   C:¥Program Files¥CA¥SharedComponents¥iTechnology ¥Register_APM.xml.
   ```

2. Safex XML ファイルに以下のコードをカット アンド ペーストし、引用符内の変数を各自の変数に置き換えます。

   ```
   <Safex>
   <!-- Attach as global user -->
   <Attach/>
   <!-- register "APM" application -->
   <Register certtype="pem" certfile="APM.pem" keyfile="APM.key">
   <ApplicationInstancxxle name="APM" label="APM">
   ```

```
</ApplicationInstance>
</Register>
<Detach/>
</Safex>
```

3. コマンドプロンプトを開き、<EEM_Server> ディレクトリに移動します。通常は、C:¥Program Files¥CA¥SharedComponents¥iTechnology です。
4. Safex スクリプトを実行するには、以下のコマンドを実行します。

   ```
   >safex.exe -h localhost -u EiamAdmin -p <パスワード> -f <ファイル名>.xml -fips
   ```

   たとえば、以下のようになります。

   ```
   >safex.exe -h localhost -u EiamAdmin -p <パスワード> -f Register_APM.xml -fips
   ```

5. CA EEM 内の APM アプリケーションを表示します。
   - スクリプトに入力した管理者名とパスワードを使用して、CA EEM にログインします。

     たとえば、ユーザ名に EiamAdmin、パスワードに <パスワード> を使用します。

     注: CA EEM では、デフォルトのグローバル権限を持つ管理者ユーザ名として EiamAdmin を使用できます。
   - APM アプリケーションのリストを表示するには、［設定］タブをクリックします。
   - そのアプリケーションに関する情報を表示または編集するには、アプリケーション名をクリックします。 たとえば、APM となります。

CA EEM での APM アプリケーションの登録解除

CA EEM でアプリケーションを登録解除するときは、アプリケーションおよびすべての関連するユーザとグループを CA EEM サーバから削除します。

注: CA EEM インターフェースを使用してこれらのタスクを実行することもできます。詳細については、「*CA Embedded Entitlements Manager Getting Started Guide*」、「*CA Embedded Entitlements Manager Online Help*」、および「*CA Embedded Entitlements Manager Programming Guide*」を参照してください。

以下の手順に従います。

注: APM という名前のアプリケーションおよびそのユーザとグループを登録解除する Safex スクリプト コードについては、*<EM_Home>/examples/authentication* ディレクトリにある *eem.unregister.app.xml* サンプル ファイルを参照してください。

1. *<EEM_Server>* ディレクトリ内に Safex XML ファイルを作成します。このディレクトリは通常、*C:¥Program Files¥CA¥SharedComponents¥iTechnology* にあります。

   たとえば、*C:¥Program Files¥CA¥SharedComponents¥iTechnology¥Unregister_APM.xml* となります。

2. Safex XML ファイルに以下のコードをカット アンド ペーストし、引用符内の変数を各自の変数に置き換えます。

```
<Safex>
   <!-- Attach as global user -->
   <Attach/>

   <!-- unregister "APM" application -->
<UnRegister>
     <ApplicationInstance name="APM" label="APM"/>
  </UnRegister>
</Safex>
```

3. コマンド プロンプトを開き、*<EEM_Server>* ディレクトリに移動します。通常は、*C:¥Program Files¥CA¥SharedComponents¥iTechnology* です。

4. 以下のコマンドを実行して Safex スクリプトを実行します。

   ```
   >safex.exe -h localhost -u EiamAdmin -p <パスワード> -f <ファイル名>.xml
   ```

   たとえば、以下のようになります。

   ```
   >safex.exe -h localhost -u EiamAdmin -p <パスワード> -f Unregister_APM.xml
   ```

   FIPS モードの CA EEM で APM アプリケーションの登録を解除する場合は、以下のコマンドを実行して Safex スクリプトを実行します。

   ```
   >safex.exe -h localhost -u EiamAdmin -p <パスワード> -f <ファイル名>.xml -fips
   ```

   たとえば、以下のようになります。

   ```
   >safex.exe -h localhost -u EiamAdmin -p <パスワード> -f Unregister_APM.xml -fips
   ```

5. CA EEM 内の APM アプリケーションを表示します。

   a. CA EEM にログインします。

   b. APM アプリケーションのリストを表示するには、［設定］タブをクリックします。

   登録解除した APM アプリケーションが削除され、表示されなくなります。 関連するユーザとグループもすべて削除されます。

CA EEM での APM グループの作成と削除

CA EEM には以下の 2 つのレベルのユーザ グループがあります。

- アプリケーション固有のグループ : アクセスを許可されているアプリケーションに固有の権限が与えられます。 アプリケーション固有のグループは他のアプリケーションと権限を共有しません。

  注: デフォルトである、CA APM の CA EEM によるセキュリティはアプリケーション固有のグループを使用してデプロイされます。

- グローバル ユーザ グループ : CA EEM に登録されているすべてのアプリケーションへのアクセス権を持っているので、すべての権限が与えられます。

注: CA EEM サーバを LDAP や SiteMinder などの外部ユーザ ディレクトリに接続すると、CA EEM 内でグローバル グループを作成または追加することができなくなります。 認証用の CA EEM サーバが LDAP サーバまたは SiteMinder サーバに統合されている場合は、CA EEM 内ではなく LDAP または SiteMinder 内でグループを設定します。

CA EEM は、子グループがその親グループから権限を継承する、ネストされたグループをサポートしています。 したがって、子グループに権限を割り当てる必要はありません。 ただし、子グループについて追加の権限を定義することはできます。

CA APM ユーザが CEM コンソールを表示するには、許可が成功するように 1 つ以上の CEM リソースについてアクセス ポリシーが定義されている必要があります。 また、Investigator ツリーおよびコンソールを表示するには、1 つ以上のドメインに対して読み取り権限を持っている必要があります。 CA APM ユーザが CEM コンソールおよび Investigator ツリーとコンソールの両方を表示する場合は、これらの要件が両方とも満たされなければなりません。

注: デフォルトの APM ユーザを追加する Safex スクリプト コードについては、*<EM_Home>/examples/authentication* ディレクトリにある *eem.add.global.identities.xml* サンプル ファイルを参照してください。

注: 認証に LDAP または SiteMinder が使用されるように CA EEM を構成し、LDAP または SiteMinder サーバ上でユーザとグループを作成した場合、CA EEM に APM グループを追加する必要はありません。Safex スクリプトを使用して APM アプリケーションを登録するだけです。「CA EEM での APM アプリケーションの登録 (P. 88)」を参照してください。

注: CA EEM インターフェースを使用してこれらのタスクを実行することもできます。詳細については、「*CA Embedded Entitlements Manager Getting Started Guide*」、「*CA Embedded Entitlements Manager Online Help*」、および「*CA Embedded Entitlements Manager Programming Guide*」を参照してください。

Safex ユーティリティを使用して APM グループを作成する方法

1. *<EEM_Server>* ディレクトリ内に Safex XML ファイルを作成します。このディレクトリは通常、*C:¥Program Files¥CA¥SharedComponents¥iTechnology* にあります。

   たとえば、*C:¥Program Files¥CA¥SharedComponents¥iTechnology¥Add_Groups.xml* となります。

2. Safex XML ファイルに以下のコードをカット アンド ペーストし、引用符内の変数を各自の変数に置き換えて、他の適切な値を構成します。

   注: アプリケーション固有のユーザ グループを指定するには、プレフィックス *ug:* を使用します。また、デプロイについて適切な場合、グローバル ユーザ グループを指定するには、*gug:* を使用します。

```
<Safex>
   <!-- Attach as global user -->
   <Attach/>
   <!-- add user group -->
   <Add>
         <Folder name="/APM" />

         <UserGroup name="Admin" folder="/">
              <Description>Administrator Group</Description>
         </UserGroup>

         <UserGroup name="Guest" folder="/">
              <Description>Guest Group</Description>
         </UserGroup>
      </Add>
      <Detach/>
</Safex>
```

3. コマンド プロンプトを開き、*<EEM_Server>* ディレクトリに移動します。通常は、*C:¥Program Files¥CA¥SharedComponents¥iTechnology* です。

4. 以下のコマンドを実行して Safex スクリプトを実行します。

   ```
   >safex.exe -h localhost -u EiamAdmin -p <パスワード> -f <ファイル名>.xml
   ```

   たとえば、以下のようになります。

   ```
   >safex.exe -h localhost -u EiamAdmin -p <パスワード> -f
   eem.add.global.identities.xml
   ```

   FIPS モードで CA EEM に統合されている APM アプリケーションに対してグループを作成する場合は、以下のコマンドを実行して Safex スクリプトを実行します。

   ```
   >safex.exe -h localhost -u EiamAdmin -p <パスワード> -f <ファイル名>.xml -fips
   ```

   たとえば、以下のようになります。

   ```
   >safex.exe -h localhost -u EiamAdmin -p <パスワード> -f
   eem.add.global.identities.xml -fips
   ```

5. CA EEM 内のグループを表示します。

   a. CA EEM にログインします。

   b. ［ID の管理］タブをクリックします。

   c. ［グループ］リンクをクリックします。

   d. ［グループの検索］ウィンドウで、［アプリケーション グループを表示］チェック ボックスをオンにして、［実行］をクリックします。

      CA EEM の［ユーザ グループ］ウィンドウに APM グループのリストが表示されます。

   e. グループ名のリンクをクリックすると、そのグループに関する詳細情報が［ユーザ グループ］ウィンドウに表示されます。

Safex ユーティリティを使用して APM グループを削除する方法

注: グループを削除する前に、グループ内のユーザを削除します。削除対象のグループを別のグループが参照している場合は、参照を削除します。

1. *<EEM_Server>* ディレクトリ内に Safex XML ファイルを作成します。このディレクトリは通常、*C:¥Program Files¥CA¥SharedComponents¥iTechnology* にあります。

   たとえば、*C:¥Program Files¥CA¥SharedComponents¥iTechnology¥Remove_Group.xml* となります。

2. Safex XML ファイルに以下のコードをカット アンド ペーストし、引用符内の変数を各自の変数に置き換えて、他の適切な値を構成します。

   注: アプリケーション固有のユーザ グループを指定するには、プレフィックス *ug:* を使用します。また、デプロイについて適切な場合、グローバル ユーザ グループを指定するには、*gug:* を使用します。

```
<Safex>
   <!-- Attach as global user -->
   <Attach/>
<!-- remove global users and groups -->
   <Remove>
            <GlobalUserGroup name="Admin" folder="/"/>
            <GlobalUserGroup name="Guest" folder="/"/>
            <GlobalFolder name="/APM" />
   </Remove>
   <Detach/>
</Safex>
```

3. コマンド プロンプトを開き、*<EEM_Server>* ディレクトリに移動します。通常は、*C:¥Program Files¥CA¥SharedComponents¥iTechnology* です。

4. 以下のコマンドを実行して Safex スクリプトを実行します。

```
>safex.exe -h localhost -u EiamAdmin -p <パスワード> -f <ファイル名>.xml
```

   たとえば、以下のようになります。

```
>safex.exe -h localhost -u EiamAdmin -p 1234567 -f Remove_Group.xml
```

   FIPS モードで CA EEM に統合されている APM アプリケーションに対してグループを削除する場合は、以下のコマンドを実行して Safex スクリプトを実行します。

```
>safex.exe -h localhost -u EiamAdmin -p <パスワード> -f <ファイル名>.xml -fips
```

   たとえば、以下のようになります。

```
>safex.exe -h localhost -u EiamAdmin -p 1234567 -f Remove_Group.xml -fips
```

5. CA EEM 内の APM グループを表示します。

   a. CA EEM にログインします。

   b. ［ID の管理］タブをクリックします。

   c. ［グループ］リンクをクリックします。

   d. ［グループの検索］ウィンドウで、［アプリケーション グループを表示］チェック ボックスをオンにして、［実行］をクリックします。

   CA EEM の［ユーザ グループ］ウィンドウに APM グループのリストが表示されます。 削除した APM グループは表示されません。

CA EEM での APM ユーザの作成と削除

CA EEM には以下の 2 つのタイプのユーザがあります。

- アプリケーション固有のユーザ： アクセスを許可されているアプリケーションに固有の権限が与えられます。
- グローバル ユーザ： CA EEM に登録されているすべてのアプリケーションへのアクセス権を持っています。 アプリケーション固有のユーザ グループにグローバル ユーザを割り当てると、そのグローバル ユーザはアプリケーション固有のユーザになります。

CA APM の Safex スクリプトを使用して CA EEM に追加される APM グローバル ユーザとアプリケーション固有のユーザは、CA EEM 内でアプリケーション固有のグループのメンバとして設定されます。 CA EEM による許可が成功するために、APM ユーザが CA EEM 内のグループのメンバである必要はありません。 ただし、CA EEM 内のグループのメンバでない APM ユーザがドメインやサーバなどのリソースを編集できるようになるには、アクセス ポリシーが定義されている必要があります。

注: 認証に LDAP または SiteMinder が使用されるように CA EEM を構成し、LDAP または SiteMinder サーバ上でユーザとグループを作成した場合、CA EEM に APM ユーザを追加する必要はありません。Safex スクリプトを使用して APM アプリケーションを登録するだけです。 「CA EEM での APM アプリケーションの登録 (P. 88)」を参照してください。

注: CA EEM サーバを LDAP や SiteMinder などの外部ユーザ ディレクトリに接続すると、CA EEM 内でグローバル ユーザを作成または追加することができなくなります。 ただし、外部（LDAP または SiteMinder）ユーザ ディレクトリ内のユーザについてアプリケーション固有の詳細を追加することができるようになります。 認証用の CA EEM サーバが LDAP サーバまたは SiteMinder サーバに統合されている場合は、CA EEM 内ではなく LDAP または SiteMinder 内でユーザを設定します。

注: デフォルトの APM グローバル ユーザを追加する Safex スクリプト コードについては、*eem.add.global.identities.xml* サンプル ファイルを参照してください。 APM アプリケーション固有のグループに APM グローバル ユーザを追加する Safex スクリプト コードについては、*eem.register.app.xml* サンプル ファイルを参照してください。 どちらのファイルも *<EM_Home>/examples/authentication* ディレクトリにあります。

注: CA EEM インターフェースを使用してこれらのタスクを実行することもできます。詳細については、「*CA Embedded Entitlements Manager Getting Started Guide*」、「*CA Embedded Entitlements Manager Online Help*」、および「*CA Embedded Entitlements Manager Programming Guide*」を参照してください。

重要: CA EEM は空のパスワードをサポートしません。したがって、CA EEM でユーザを作成するたびに、パスワードを指定する必要があります。

Safex ユーティリティを使用して APM ユーザを作成する方法

1. *<EEM_Server>* ディレクトリ内に Safex XML ファイルを作成します。このディレクトリは通常、*C:¥Program Files¥CA¥SharedComponents¥iTechnology* にあります。

   たとえば、*C:¥Program Files¥CA¥SharedComponents¥iTechnology¥Add_Users.xml* となります。

2. Safex XML ファイルに以下のコードをカット アンド ペーストし、引用符内の変数を各自の変数に置き換えて、他の適切な値を構成します。

```
<Safex>
   <!-- Attach as global user -->
   <Attach/>

   <!-- add global users -->
   <Add>
         <GlobalUser name="admin" folder="/APM">
               <UserName>admin</UserName>
               <DisplayName>Admin</DisplayName>
               <!-- blank passwords not allowed -->
               <Password>admin</Password>
               <FirstName>APM</FirstName>
               <LastName>Admin</LastName>
               <WorkPhoneNumber>1-888-888-8888</WorkPhoneNumber>
               <EmailAddress>support@yourcompany.com</EmailAddress>
               <GroupMembership>Admin</GroupMembership>
         </GlobalUser>

         <GlobalUser name="guest" folder="/APM">
               <UserName>guest</UserName>
               <DisplayName>Guest</DisplayName>
               <Password>guest12</Password>
               <FirstName>APM</FirstName>
               <LastName>Guest</LastName>
               <WorkPhoneNumber>1-888-888-8888</WorkPhoneNumber>
```

```
                <EmailAddress>support@yourcompany.com</EmailAddress>
                <GroupMembership>Guest</GroupMembership>
            </GlobalUser>

        <!-- add users to groups -->
        <User folder="/APM" name="guest">
        <GroupMembership>Guest</GroupMembership>
        </User>
        <User folder="/APM" name="admin">
        <GroupMembership>Admin</GroupMembership>
        </User>

        </Add>
        <Detach/>
</Safex>
```

3. コマンドプロンプトを開き、*<EEM_Server>* ディレクトリに移動します。通常は、*C:¥Program Files¥CA¥SharedComponents¥iTechnology* です。
4. 以下のコマンドを実行して Safex スクリプトを実行します。

   ```
   >safex.exe -h localhost -u EiamAdmin -p <パスワード> -f <ファイル名>.xml
   ```

   たとえば、以下のようになります。

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Add_Users.xml
   ```

   FIPS モードで CA EEM に統合されているアプリケーションに対して APM ユーザを作成する場合は、以下のコマンドを実行して Safex スクリプトを実行します。

   ```
   >safex.exe -h localhost -u EiamAdmin -p <パスワード> -f <ファイル名>.xml -fips
   ```

   たとえば、以下のようになります。

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Add_Users.xml -fips
   ```

5. CA EEM 内の APM ユーザを表示します。
   a. CA EEM にログインします。
   b. ［ID の管理］タブをクリックします。
   c. ［ユーザ］リンクをクリックします。
   d. ［ユーザの検索］ウィンドウで、［属性］、［オペレータ］、または［値］の検索用語を設定し、［実行］をクリックします。

      CA EEM の［ユーザ］ウィンドウに APM ユーザのリストが表示されます。

   e. APM ユーザ名のリンクをクリックすると、そのユーザに関する詳細情報が［ユーザの詳細］ウィンドウに表示されます。

Safex ユーティリティを使用して APM ユーザを削除する方法

注: デフォルトの APM グローバル ユーザを削除する Safex スクリプト コードについては、*eem.remove.global.identities.xml* サンプル ファイルを参照してください。 アプリケーション固有のユーザを含めて APM アプリケーションを削除する Safex スクリプト コードについては、*eem.unregister.app.xml* サンプル ファイルを参照してください。 どちらのファイルも *<EM_Home>/examples/authentication* ディレクトリにあります。

1. *<EEM_Server>* ディレクトリ内に Safex XML ファイルを作成します。このディレクトリは通常、*C:¥Program Files¥CA¥SharedComponents¥iTechnology* にあります。

   たとえば、*C:¥Program Files¥CA¥SharedComponents¥iTechnology¥Remove_User.xml* となります。

2. Safex XML ファイルに以下のコードをカット アンド ペーストし、引用符内の変数を各自の変数に置き換えて、他の適切な値を構成します。

```
<Safex>
   <!-- Attach as global user -->
   <Attach/>
<!-- remove global users and groups -->
  <Remove>
         <GlobalUser name="admin" folder="/APM"/>
         <GlobalUser name="guest" folder="/APM"/>
         <GlobalFolder name="/APM" />
   </Remove>
   <Detach/>
</Safex>
```

3. コマンド プロンプトを開き、*<EEM_Server>* ディレクトリに移動します。通常は、*C:¥Program Files¥CA¥SharedComponents¥iTechnology* です。

4. 以下のコマンドを実行して Safex スクリプトを実行します。

   ```
   >safex.exe -h localhost -u EiamAdmin -p <パスワード> -f <ファイル名>.xml
   ```

   たとえば、以下のようになります。

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Remove_User.xml
   ```

   FIPS モードで CA EEM に統合されているアプリケーションに対して APM ユーザを削除する場合は、以下のコマンドを実行して Safex スクリプトを実行します。

   ```
   >safex.exe -h localhost -u EiamAdmin -p <パスワード> -f <ファイル名>.xml -fips
   ```

   たとえば、以下のようになります。

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Remove_User.xml -fips
   ```

5. CA EEM 内の APM ユーザを表示します。

   a. CA EEM にログインします。

   b. ［ID の管理］タブをクリックします。

   c. ［ユーザ］リンクをクリックします。

   d. ［ユーザの検索］ウィンドウで、［属性］、［オペレータ］、または［値］の検索用語を設定し、［実行］をクリックします。

   CA EEM の［ユーザ］ウィンドウに APM ユーザのリストが表示されます。 削除した APM ユーザは表示されません。

CA EEM での APM リソース クラスの作成と削除

新しいアプリケーションを登録するごとに、APM リソース クラスを定義しなければならない場合があります。 Introscope では、少なくともドメインとサーバのリソース クラスが必要です。 CA CEM を使用する場合、CA CEM 固有のリソース クラスを定義する必要があります。 CA CEM の CA EEM によるセキュリティの詳細については、「CA CEM の CA EEM による認証および許可 (P. 146)」を参照してください。

重要: CA APM のセキュリティでは、修正済みの APM リソース クラスおよび権限名を使用する必要があります。

APM リソース クラスごとに関連する権限を指定する必要があります。CA EEM ではこの権限のことを *アクション*と呼びます。

注: デフォルトのリソース クラスを含む *APM* という名前のアプリケーションを作成する Safex スクリプト コードについては、*<EM_Home>/examples/authentication* ディレクトリにある *eem.register.app.xml* サンプル ファイルを参照してください。

注: CA EEM インターフェースを使用してこれらのタスクを実行することもできます。詳細については、「*CA Embedded Entitlements Manager Getting Started Guide*」、「*CA Embedded Entitlements Manager Online Help*」、および「*CA Embedded Entitlements Manager Programming Guide*」を参照してください。

Safex ユーティリティを使用して APM リソース クラスを作成する方法

1. *<EEM_Server>* ディレクトリ内に Safex XML ファイルを作成します。このディレクトリは通常、*C:¥Program Files¥CA¥SharedComponents¥iTechnology* にあります。

   たとえば、*C:¥Program Files¥CA¥SharedComponents¥iTechnology¥Add_resource_classes.xml* となります。

2. ドメイン リソース クラスの権限を決定します。

   read

   ユーザまたはグループは、ドメイン内のすべてのエージェントとビジネス ロジックを表示できます。

   この権限で実行できるタスクには以下のものがあります。

   - Investigator ツリーの表示 (ユーザがアクセス権を持つドメイン内のエージェントが表示されます)
   - Workstation コンソールでのダッシュボードの表示
   - Investigator のプレビュー ペインでのメトリック データとエレメント データの表示 (Investigator ツリー内の特定リソースのデフォルト ビューである、上位 N 件を示すフィルタされたビューの表示を含みます)
   - 管理モジュール、エージェント、またはエレメントの設定の表示
   - アラート メッセージの参照
   - 履歴 Data Viewer での履歴データの更新および拡大/縮小表示
   - 履歴 Data Viewer の履歴データの範囲に関するオプションの変更

- グラフでのメトリックの表示/非表示の切り替え
- Data Viewer でのメトリックの前面/背面移動
- グループとユーザの基本設定の変更 (ホーム ダッシュボードの設定や、管理モジュール名をダッシュボード名と共に表示するかどうかなど)

注: read 権限を持つユーザまたはグループは、Workstation のすべてのコマンドを参照できます。 ただし、アクセス権を持たないコマンドは無効になります。

write

write 権限を持つユーザまたはグループは、read 権限を持つユーザまたはグループが実行可能な操作をすべて実行できますが、以下のタスクも行うことができます。

- ドメイン内のすべてのエージェントとビジネス ロジックの表示
- ダッシュボードの作成および編集
- ドメイン内のすべてのモニタリング ロジックの編集

run_tracer

ユーザまたはグループは、エージェントについてトランザクション追跡セッションを開始できます。

注: この権限には、read 権限も割り当てる必要があります。

historical_agent_control

ユーザまたはグループはエージェント（複数可）をマウントおよびマウント解除できます。

注: この権限には、read 権限も割り当てる必要があります。

live_agent_control

ユーザまたはグループは、ドメイン内のメトリック、リソース、およびエージェントの報告をシャットオフできます。

注: この権限には、read 権限も割り当てる必要があります。

dynamic_instrumentation

ユーザまたはグループは動的インスツルメンテーションを実行できます。

動的インスツルメンテーションについては、「CA APM Java エージェント実装ガイド」または「CA APM .NET エージェント実装ガイド」を参照してください。

thread_dump

ユーザまたはグループは［スレッド ダンプ］タブを参照および使用できます。

スレッド ダンプの使用および設定については、「CA APM Workstation ユーザ ガイド」および「CA APM Java エージェント実装ガイド」を参照してください。

full

ユーザまたはグループは、ドメインに対するすべての権限を持ちます。

APM ドメインの構成については、「Introscope のセキュリティおよび権限の概要 (P. 37)」を参照してください。

3. サーバ リソース クラスの権限を決定します。

shutdown

ユーザまたはグループは Enterprise Manager をシャットダウンできます。

publish_mib

ユーザまたはグループは SNMP コレクション データを MIB に発行できます。

MIB を発行するには、SNMP コレクションを作成する必要があります。このタスクを行うには、SNMP コレクションの保存先のドメインに対する書き込みアクセス権が必要です。

apm_status_console_control

ユーザまたはグループは、APM ステータス アラート アイコンの表示、APM ステータス コンソールの使用、APM ステータス コンソール CLW コマンドの実行を行えます。

注: メトリック ブラウザ ツリーでアクティブなクランプのメトリック情報を表示するには、domains.xml のスーパードメイン権限 (P. 50)を持っている必要があります。

full

ユーザまたはグループは Enterprise Manager サーバに対するすべての権限を持ちます。

4. アプリケーション問題切り分けマップのセキュリティを提供するビジネス サービス リソース クラスの権限を決定します。

書き込み、読み取り、および機密データの読み取り

Introscope ユーザおよびグループは、アプリケーション問題切り分けマップにビジネス サービスを表示できます。

注: アプリケーション問題切り分けマップにビジネス サービスを表示するには、任意の CA EEM 権限を使用できます。 この場合、これらの 3 つの権限はデフォルトで使用できます。

注: ビジネス サービスを表示するためのユーザ権限を変更する場合、そのような変更は、ユーザが Workstation からいったんログアウトし再度ログインするまで、アプリケーション問題切り分けマップに反映されません。

5. フロントエンドに対してアプリケーション問題切り分けマップのセキュリティを提供するビジネス アプリケーション リソース クラスの権限を決定します。

書き込み

Introscope ユーザおよびグループは、アプリケーション問題切り分けマップにフロントエンドを表示できます。

注: スーパードメインのセキュリティは、アプリケーション問題切り分けマップのセキュリティに優先します。 詳細については、「スーパードメインのセキュリティは、アプリケーション問題切り分けマップのセキュリティに優先する (P. 131)」を参照してください。

注: CA APM の CA EEM によるセキュリティは、ビジネス アプリケーション リソース クラスを使用して、マップのフロントエンドに対するセキュリティを提供します。

注: マップにフロントエンドを表示するには、任意の CA EEM 権限を使用できます。 この場合、書き込み権限だけがデフォルトで使用できます。

注: マップのフロントエンドを表示するためのユーザ権限を変更する場合、そのような変更は、ユーザが Workstation からいったんログアウトし再度ログインするまで、アプリケーション問題切り分けマップに反映されません。

6. <ResourceClass> で始まり
</ResourceClass> で終わるコードを Safex XML ファイルにカット アンド ペーストし、リソース クラスと権限を各自の変数に置き換えて、他の適切な値を構成します。

   注: CA EEM では、権限はアクションと呼ばれます。

```
<Safex>
   <!-- Attach as global user -->
   <Attach/>
   <!-- register "APM" application  -->
   <Register certfile="APM.p12" password="EiamAdmin">
      <ApplicationInstance name="APM" label="APM">
             <Brand>Introscope</Brand>
             <MajorVersion>1</MajorVersion>
             <MinorVersion>0</MinorVersion>
             <Description>APM Application</Description>
             <ResourceClass>
                <Name>Domain</Name>
                <Action>read</Action>
                <Action>write</Action>
                <Action>run_tracer</Action>
                <Action>historical_agent_control</Action>
                <Action>dynamic_instrumentation</Action>
                <Action>live_agent_control</Action>
                <Action>Thread_Dump</Action>
                <Action>full</Action>
            </ResourceClass>
            <ResourceClass>
                <Name>Server</Name>
                <Action>shutdown</Action>
                <Action>publish_mib</Action>
                <Action>apm_status_console_control</Action>
                <Action>full</Action>
            </ResourceClass>
            <ResourceClass>
                <Name>Business Service</Name>
                <Action>write</Action>
                <Action>read</Action>
                <Action>read sensitive data</Action>
            </ResourceClass>
            <ResourceClass>
                <Name>Business Application</Name>
                <Action>write</Action>
            </ResourceClass>

      </ApplicationInstance>
```

```
    </Register>
    <Detach/>
</Safex>
```

注: *ビジネス サービス*および*ビジネス アプリケーション*リソース クラスは、アプリケーション問題切り分けマップのユーザ権限を設定するために必要です。 権限を設定しない場合は、すべてのユーザがすべてのフロントエンドを表示できます。 ビジネス アプリケーション リソース クラスは、特定のフロントエンドを表示するための権限を提供します。

7. コマンド プロンプトを開き、*<EEM_Server>* ディレクトリに移動します。通常は、*C:¥Program Files¥CA¥SharedComponents¥iTechnology* です。
8. 以下のコマンドを実行して Safex スクリプトを実行します。

   ```
   >safex.exe -h localhost -u EiamAdmin -p <パスワード> -f <ファイル名>.xml
   ```

   たとえば、以下のようになります。

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Add_resource_classes.xml
   ```

   FIPS モードで CA EEM に統合されているアプリケーションに対して APM リソース クラスを作成する場合は、以下のコマンドを実行して Safex スクリプトを実行します。

   ```
   >safex.exe -h localhost -u EiamAdmin -p <パスワード> -f <ファイル名>.xml -fips
   ```

   たとえば、以下のようになります。

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Add_resource_classes.xml -fips
   ```

9. CA EEM 内の APM リソースを表示します。
   a. CA EEM にログインします。
   b. ［アクセス ポリシーの管理］タブをクリックします。
   c. ［ポリシー］リンクをクリックします。

   CA EEM にリソース クラスのポリシーが表示されます。

Safex ユーティリティを使用して APM リソース クラスを削除する方法

1. *<EEM_Server>* ディレクトリ内に Safex XML ファイルを作成します。このディレクトリは通常、*C:¥Program Files¥CA¥SharedComponents¥iTechnology* にあります。

   たとえば、*C:¥Program Files¥CA¥SharedComponents¥iTechnology¥Remove_Resource_class.xml* となります。

2. Safex XML ファイルに以下のコードをカット アンド ペーストし、引用符内の変数を各自の変数に置き換えて、他の適切な値を構成します。

```
<Safex>
   <!-- Attach as global user -->
   <Attach/>

<!-- remove resource class -->
      <ApplicationInstance name="APM" label="APM">
      <Remove>
                <ResourceClass>
                   <Name>Business Service</Name>
                   <Action>write</Action>
                   <Action>read</Action>
                   <Action>read sensitive data</Action>
             </ResourceClass>
     </Remove>
   </ApplicationInstance>
   <Detach/>
</Safex>
```

3. コマンド プロンプトを開き、*<EEM_Server>* ディレクトリに移動します。通常は、*C:¥Program Files¥CA¥SharedComponents¥iTechnology* です。

4. 以下のコマンドを実行して Safex スクリプトを実行します。

   ```
   >safex.exe -h localhost -u EiamAdmin -p <パスワード> -f <ファイル名>.xml
   ```

   たとえば、以下のようになります。

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Remove_Resource_class.xml
   ```

   FIPS モードで CA EEM に統合されているアプリケーションに対して APM リソース クラスを削除する場合は、以下のコマンドを実行して Safex スクリプトを実行します。

   ```
   >safex.exe -h localhost -u EiamAdmin -p <パスワード> -f <ファイル名>.xml -fips
   ```

   たとえば、以下のようになります。

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Remove_Resource_class.xml
   -fips
   ```

5. CA EEM 内の APM リソースを表示します。
   a. CA EEM にログインします。
   b. ［アクセス ポリシーの管理］タブをクリックします。
   c. ［ポリシー］リンクをクリックします。

   削除したリソース クラスは表示されません。

CA EEM のアクセス ポリシーについて

CA EEM のアクセス ポリシーは、ドメイン、サーバ、フロントエンド、ビジネス サービスなどの特定のリソースに対して特定のアクションを実行するためにグループに与えられる権限を反映しています。 つまり、ビジネス サービスとフロントエンド（CA EEM ではビジネス アプリケーションと呼びます）のアクセス ポリシーを提供するビジネス セキュリティは、エージェントではなく、アプリケーション問題切り分けマップに影響します。 ただし、ドメイン セキュリティは、アプリケーション問題切り分けマップではなく、エージェントに影響します。

グローバル ユーザがアプリケーション固有のユーザ グループに追加されると、そのユーザはグループに与えられるリソース権限を取得します。

例として、グローバル ユーザ Admin をアプリケーション固有の CEM System Administrator ユーザ グループのメンバにする CA APM Safex スクリプトのコード断片を示します。

```
<User folder="/APM" name="cemadmin"><GroupMembership>CEM System
Administrator</GroupMembership><GroupMembership>Admin</GroupMembership>
</User>
```

CA APM Safex スクリプトの後半には、CA EEM アプリケーション リソース アクセス ポリシーを設定する以下のスニペットがあります。

```
        <Policy name="Business Application write" folder="/Policies">
        <Description>CEM System Administrator Group and CEM Configuration
Administrator Group have write permission for all Business
Applications.</Description>
        <ResourceClassName>Business Application</ResourceClassName>
        <Action>write</Action>
        <Identity>ug:CEM Configuration Administrator</Identity>
```

```
 <Identity>ug:CEM System Administrator</Identity>
</Policy>
```

ポリシー定義内の以下の行は、CEM System Administrator ユーザ グループに対し、アプリケーション リソースにアクセスするための権限を付与します。

```
ug:CEM System Administrator
```

Admin は CEM System Administrator ユーザ グループのメンバであるので、Admin には、アプリケーション問題切り分けマップにフロントエンドを表示する権限も与えられます。

フロントエンドに対するセキュリティは、問題切り分けマップ ツリーに適用されます。 つまり、権限を持っていないユーザの問題切り分けマップ ツリーには、フロントエンド ノードが表示されません。 ただし、マップ セキュリティはメトリック ブラウザ ツリーには適用されません。 このツリーでは、ユーザはフロントエンドとメトリックをすべて表示できます。

CA EEM APM ドメイン リソース アクセス ポリシーの作成と削除

このトピックでは、CA EEM で CA APM ドメインのセキュリティを保護する方法について説明します。 たとえば、スーパードメインやユーザ定義のドメインがこれに該当します。 ドメイン セキュリティを提供するには、*スーパードメイン*およびユーザ定義ドメインの CA EEM アクセス ポリシーを、ドメイン権限を設定するための CA EEM ドメイン リソースとして追加する必要があります。

注: ローカルによるセキュリティの場合、ドメイン権限は *domains.xml* ファイルで構成します。詳細については、「domains.xml での Introscope ドメイン権限の構成 (P. 50)」を参照してください。 CA EEM によるセキュリティの場合、*domains.xml* 内のドメイン権限は無視され、CA EEM 内で代わりに設定されます。

注: ドメイン リソースのデフォルトのアクセス ポリシーを含む *APM* という名前のアプリケーションを作成する Safex スクリプト コードについては、*<EM_Home>/examples/authentication* ディレクトリにある *eem.register.app.xml* サンプル ファイルを参照してください。

注: CA EEM インターフェースを使用してこれらのタスクを実行することもできます。詳細については、「*CA Embedded Entitlements Manager Getting Started Guide*」、「*CA Embedded Entitlements Manager Online Help*」、および「*CA Embedded Entitlements Manager Programming Guide*」を参照してください。

Safex ユーティリティを使用して、CA EEM APM ドメイン リソース アクセス ポリシーを作成する方法

1. *<EEM_Server>* ディレクトリ内に Safex XML ファイルを作成します。このディレクトリは通常、*C:¥Program Files¥CA¥SharedComponents¥iTechnology* にあります。

   たとえば、*C:¥Program Files¥CA¥SharedComponents¥iTechnology¥Add_domains.xml* となります。

2. Safex XML ファイルに以下のコードをカット アンド ペーストし、引用符内の変数を各自の変数に置き換えて、ID、リソース クラス、および権限の値を構成します。ドメイン権限については、「CA EEM での APM リソース クラスの作成と削除 (P. 102)」の手順 2 （「各リソース クラスについて許可する権限を決定します」） を参照してください。

   注: CA EEM では、権限はアクションと呼ばれます。

```
<Safex>
   <Attach label="APM"/>
   <!-- add policies -->
   <Add>
        <Policy name="Domain Admin" folder="/Policies">
        <Description>Admin group has full permission for all
domains</Description>
        <Identity>gug:Admin</Identity>
        <Action>full</Action>
        <ResourceClassName>Domain</ResourceClassName>
        <Resource>SuperDomain</Resource>
        </Policy>
     </Add>
     <Detach/>
</Safex>
```

3. コマンド プロンプトを開き、*<EEM_Server>* ディレクトリに移動します。通常は、*C:¥Program Files¥CA¥SharedComponents¥iTechnology* です。

4. 以下のコマンドを実行して Safex スクリプトを実行します。

   ```
   >safex.exe -h localhost -u EiamAdmin -p <パスワード> -f <ファイル名>.xml
   ```

   たとえば、以下のようになります。

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Add_domains.xml
   ```

   FIPS モードで CA EEM に統合されているアプリケーションに対して Safex ユーティリティを使用して CA EEM APM ドメイン リソース アクセス ポリシーを作成する場合は、以下のコマンドを実行して Safex スクリプトを実行します。

   ```
   >safex.exe -h localhost -u EiamAdmin -p <パスワード> -f <ファイル名>.xml -fips
   ```

   たとえば、以下のようになります。

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Add_domains.xml- fips
   ```

5. CA EEM 内の APM ドメインを表示します。

   a. CA EEM にログインします。

   b. ［アクセス ポリシーの管理］タブをクリックします。

   c. ［ポリシー］リンクをクリックします。

   d. ［ポリシーの検索］ウィンドウで、［リソースに一致するポリシーを表示］をクリックします。次に、［リソース クラス名］ドロップダウン リストから［ドメイン］を選択し、［実行］をクリックします。

   CA EEM の［ポリシー テーブル］ウィンドウに APM ドメイン リソース アクセス ポリシーのリストが表示されます。

Safex ユーティリティを使用して、CA EEM APM ドメイン リソース アクセス ポリシーを削除する方法

1. *<EEM_Server>* ディレクトリ内に Safex XML ファイルを作成します。このディレクトリは通常、*C:¥Program Files¥CA¥SharedComponents¥iTechnology* にあります。

   たとえば、*C:¥Program Files¥CA¥SharedComponents¥iTechnology¥Remove_domain.xml* となります。

2. Safex XML ファイルに以下のコードをカット アンド ペーストし、引用符内の変数を各自の変数に置き換えて、ID、リソース クラス、および権限の値を構成します。ドメイン権限については、「CA EEM での APM リソース クラスの作成と削除 (P. 102)」の手順 2 （「各リソース クラスについて許可する権限を決定します」） を参照してください。

   注: CA EEM では、権限はアクションと呼ばれます。

   ```
   <Safex>
      <Attach label="APM"/>
      <Remove>
           <Policy name="Domain Guest" folder="/Policies"/>
      </Remove>
      <Detach/>
   </Safex>
   ```

3. コマンド プロンプトを開き、*<EEM_Server>* ディレクトリに移動します。通常は、*C:¥Program Files¥CA¥SharedComponents¥iTechnology* です。

4. 以下のコマンドを実行して Safex スクリプトを実行します。

   ```
   >safex.exe -h localhost -u EiamAdmin -p <パスワード> -f <ファイル名>.xml
   ```

   たとえば、以下のようになります。

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Remove_domain.xml
   ```

   FIPS モードで CA EEM に統合されているアプリケーションに対して Safex ユーティリティを使用して CA EEM APM ドメイン リソース アクセス ポリシーを削除する場合は、以下のコマンドを実行して Safex スクリプトを実行します。

   ```
   >safex.exe -h localhost -u EiamAdmin -p <パスワード> -f <ファイル名>.xml -fips
   ```

   たとえば、以下のようになります。

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Remove_domain.xml -fips
   ```

5. CA EEM 内の APM ドメインを表示します。
   a. CA EEM にログインします。
   b. ［アクセス ポリシーの管理］タブをクリックします。
   c. ［ポリシー］リンクをクリックします。
   d. ［ポリシーの検索］ウィンドウで、［リソースに一致するポリシーを表示］をクリックします。次に、［リソース クラス名］ドロップダウン リストから［ドメイン］を選択し、［実行］をクリックします。

   CA EEM の［ポリシー テーブル］ウィンドウに APM ドメイン リソース アクセス ポリシーのリストが表示されます。 削除した APM ドメイン リソース アクセス ポリシーは表示されません。

CA EEM APM サーバ リソース アクセス ポリシーの作成と削除

サーバ権限を設定するには、CA EEM APM サーバ リソースのアクセス ポリシーを追加する必要があります。

注: サーバ リソースのデフォルトのアクセス ポリシーを含む APM という名前のアプリケーションを作成する Safex スクリプト コードについては、*<EM_Home>/examples/authentication* ディレクトリにある *eem.register.app.xml* サンプル ファイルを参照してください。

注: CA EEM インターフェースを使用してこれらのタスクを実行することもできます。詳細については、「*CA Embedded Entitlements Manager Getting Started Guide*」、「*CA Embedded Entitlements Manager Online Help*」、および「*CA Embedded Entitlements Manager Programming Guide*」を参照してください。

Safex ユーティリティを使用して CA EEM APM サーバ リソース アクセス ポリシーを作成する方法

1. *<EEM_Server>* ディレクトリ内に Safex XML ファイルを作成します。このディレクトリは通常、*C:¥Program Files¥CA¥SharedComponents¥iTechnology* にあります。

   たとえば、*C:¥Program Files¥CA¥SharedComponents¥iTechnology¥Add_server.xml* となります。

2. Safex XML ファイルに以下のコードをカット アンド ペーストし、引用符内の変数を各自の変数に置き換えて、ID、リソース クラス、および権限の値を構成します。サーバ権限については、「CA EEM での APM リソース クラスの作成と削除 (P. 102)」の手順 2 （「各リソース クラスについて許可する権限を決定します」）を参照してください。

   注: CA EEM では、権限はアクションと呼ばれます。

```
<Safex>
   <Attach label="APM"/>
   <!-- add policies -->

   <Add>
        <Policy name="Server Admin" folder="/Policies">
        <Description>Admin group has full permission for the
server</Description>

        <Identity>gug:Admin</Identity>

        <Action>full</Action>

        <ResourceClassName>Server</ResourceClassName>
        </Policy>
     </Add>

     <Detach/>
</Safex>
```

3. コマンド プロンプトを開き、*<EEM_Server>* ディレクトリに移動します。通常は、*C:¥Program Files¥CA¥SharedComponents¥iTechnology* です。

4. 以下のコマンドを実行して Safex スクリプトを実行します。

   ```
   >safex.exe -h localhost -u EiamAdmin -p <パスワード> -f <ファイル名>.xml
   ```

   たとえば、以下のようになります。

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Add_server.xml
   ```

   FIPS モードで CA EEM に統合されているアプリケーションに対して Safex ユーティリティを使用して CA EEM APM サーバ リソース アクセス ポリシーを作成する場合は、以下のコマンドを実行して Safex スクリプトを実行します。

   ```
   >safex.exe -h localhost -u EiamAdmin -p <パスワード> -f <ファイル名>.xml -fips
   ```

   たとえば、以下のようになります。

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Add_server.xml -fips
   ```

5. CA EEM 内の APM サーバ リソースを表示します。

   a. CA EEM にログインします。

   b. ［アクセス ポリシーの管理］タブをクリックします。

   c. ［ポリシー］リンクをクリックします。

   d. ［ポリシーの検索］ウィンドウで、［リソースに一致するポリシーを表示］をクリックします。次に、［リソース クラス名］ドロップダウン リストから［サーバ］を選択し、［実行］をクリックします。

      CA EEM の［ポリシー テーブル］ウィンドウに APM サーバ リソース アクセス ポリシーのリストが表示されます。

   e. サーバ アクセス ポリシー名のリンクをクリックすると、APM サーバ リソースに関する詳細情報がポリシー詳細のウィンドウに表示されます。

Safex ユーティリティを使用して、CA EEM APM サーバ リソース アクセス ポリシーを削除方法

1. *<EEM_Server>* ディレクトリ内に Safex XML ファイルを作成します。このディレクトリは通常、*C:¥Program Files¥CA¥SharedComponents¥iTechnology* にあります。

   たとえば、*C:¥Program Files¥CA¥SharedComponents¥iTechnology¥Remove_server.xml* となります。

2. Safex XML ファイルに以下のコードをカット アンド ペーストし、引用符内の変数を各自の変数に置き換えて、ID、リソース クラス、および権限の値を構成します。サーバ権限については、「CA EEM での APM リソース クラスの作成と削除 (P. 102)」の手順 2 （「各リソース クラスについて許可する権限を決定します」）を参照してください。

   注: CA EEM では、権限はアクションと呼ばれます。

```
<Safex>
   <Attach label="APM"/>
   <Remove>
        <Policy name="Server Admin" folder="/Policies">
        <Description>Admin group has full permission for the
server</Description>
        <Identity>gug:Admin</Identity>
        <Action>full</Action>
        <ResourceClassName>Server</ResourceClassName>
        </Policy>
     </Remove>
     <Detach/>
</Safex>
```

3. コマンド プロンプトを開き、*<EEM_Server>* ディレクトリに移動します。通常は、*C:¥Program Files¥CA¥SharedComponents¥iTechnology* です。

4. 以下のコマンドを実行して Safex スクリプトを実行します。

   ```
   >safex.exe -h localhost -u EiamAdmin -p <パスワード> -f <ファイル名>.xml
   ```

   たとえば、以下のようになります。

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Remove_server.xml
   ```

   FIPS モードで CA EEM に統合されているアプリケーションに対して Safex ユーティリティを使用して CA EEM APM サーバ リソース アクセス ポリシーを削除する場合は、以下のコマンドを実行して Safex スクリプトを実行します。

   ```
   >safex.exe -h localhost -u EiamAdmin -p <パスワード> -f <ファイル名>.xml -fips
   ```

   たとえば、以下のようになります。

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Remove_server.xml -fips
   ```

5. CA EEM 内の APM サーバ リソースを表示します。

   a. CA EEM にログインします。

   b. ［アクセス ポリシーの管理］タブをクリックします。

   c. ［ポリシー］リンクをクリックします。

   d. ［ポリシーの検索］ウィンドウで、［リソースに一致するポリシーを表示］をクリックします。次に、［リソース クラス名］ドロップダウン リストから［サーバ］を選択し、［実行］をクリックします。

   CA EEM の［ポリシー テーブル］ウィンドウに APM サーバ リソース アクセス ポリシーのリストが表示されます。 削除した APM サーバ リソース アクセス ポリシーは表示されません。

CA EEM APM フロントエンドおよびビジネス サービス リソース アクセス ポリシーの作成と削除

アプリケーション問題切り分けマップ権限を設定するには、フロントエンド（CA EEM ではビジネス アプリケーションと呼びます）とビジネス サービスのアクセス ポリシーを CA EEM APM アプリケーション リソースとして追加する必要があります。

注: CA EEM インターフェースを使用してこれらのタスクを実行することもできます。詳細については、「*CA Embedded Entitlements Manager Getting Started Guide*」、「*CA Embedded Entitlements Manager Online Help*」、および「*CA Embedded Entitlements Manager Programming Guide*」を参照してください。

Safex ユーティリティを使用して CA EEM APM フロントエンドまたはビジネス サービス リソース アクセス ポリシーを作成する方法

1. *<EEM_Server>* ディレクトリ内に Safex XML ファイルを作成します。このディレクトリは通常、*C:¥Program Files¥CA¥SharedComponents¥iTechnology* にあります。

   たとえば、*C:¥Program Files¥CA¥SharedComponents¥iTechnolog¥Add_application_policy.xml* となります。

2. Safex XML ファイルに以下のコードをカット アンド ペーストし、引用符内の変数を各自の変数に置き換えて、ID、リソース、および権限の値を構成します。 アプリケーション権限については、「CA EEM での APM リソース クラスの作成と削除 (P. 102)」の手順 2 （「各リソース クラスについて許可する権限を決定します」）を参照してください。

   注: CA EEM では、権限はアクションと呼ばれます。

   注: 以下のサンプル コードは、アプリケーション問題切り分けマップに Banking Application という名前のアプリケーションを表示する権限を Guest ユーザに付与します。

```
<Safex>
   <Attach label="APM"/>
   <!-- add policies -->

   <Add>
        <Policy name="Business Application Write to a banking application"
folder="/Policies">
        <Description>Guest Group has write permission for a Banking
Application.</Description>

        <ResourceClassName>Business Application</ResourceClassName>

        <Resource>Banking Application</Resource>

        <Action>write</Action>

        <Identity>ug:Guest</Identity>
        </Policy>
     </Add>
     <Detach/>
</Safex>
```

3. コマンド プロンプトを開き、*<EEM_Server>* ディレクトリに移動します。通常は、*C:¥Program Files¥CA¥SharedComponents¥iTechnology* です。

4. 以下のコマンドを実行して Safex スクリプトを実行します。

   ```
   >safex.exe -h localhost -u EiamAdmin -p <パスワード> -f <ファイル名>.xml
   ```

   たとえば、以下のようになります。

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Add_application_policy.xml
   ```

   FIPS モードで CA EEM に統合されているアプリケーションに対して Safex ユーティリティを使用して CA EEM APM フロントエンドまたはビジネス サービス リソース アクセス ポリシーを作成する場合は、以下のコマンドを実行して Safex スクリプトを実行します。

   ```
   >safex.exe -h localhost -u EiamAdmin -p <パスワード> -f <ファイル名>.xml -fips
   ```

   たとえば、以下のようになります。

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Add_application_policy.xml
   -fips
   ```

5. CA EEM 内の APM アプリケーション リソース ポリシーを表示します。

   a. CA EEM にログインします。

   b. ［アクセス ポリシーの管理］タブをクリックします。

   c. ［ポリシー］リンクをクリックします。

   d. ［ポリシーの検索］ウィンドウで、［リソースに一致するポリシーを表示］をクリックします。次に、［リソース クラス名］ドロップダウン リストからアプリケーション ポリシー名を選択し、［実行］をクリックします。

      CA EEM の［ポリシー テーブル］ウィンドウに APM アプリケーション リソース アクセス ポリシーのリストが表示されます。

   e. アプリケーション リソース アクセス ポリシー名のリンクをクリックすると、APM アプリケーション リソースに関する詳細情報がポリシー詳細のウィンドウに表示されます。

Safex ユーティリティを使用して CA EEM APM フロントエンドまたはビジネス サービス リソース アクセス ポリシーを削除する方法

1. *<EEM_Server>* ディレクトリ内に Safex XML ファイルを作成します。このディレクトリは通常、*C:¥Program Files¥CA¥SharedComponents¥iTechnology* にあります。

   たとえば、*C:¥Program Files¥CA¥SharedComponents¥iTechnology¥Remove_application_policy.xml* となります。

2. Safex XML ファイルに以下のコードをカット アンド ペーストし、引用符内の変数を各自の変数に置き換えて、ID、リソース、および権限の値を構成します。 アプリケーション権限については、「CA EEM での APM リソース クラスの作成と削除 (P. 102)」の手順 2 （「各リソース クラスについて許可する権限を決定します」）を参照してください。

   注: CA EEM では、権限はアクションと呼ばれます。

```
<Safex>
   <Attach label="APM"/>
       <Remove>
        <Policy name="Business Application Write to a banking application"
folder="/Policies">
        <Description>Guest Group has write permission for a Banking
Application.</Description>

        <ResourceClassName>Business Application</ResourceClassName>

        <Resource>Banking Application</Resource>

        <Action>write</Action>

        <Identity>ug:Guest</Identity>
        </Policy>
       </Remove>
     <Detach/>
</Safex>
```

3. コマンド プロンプトを開き、*<EEM_Server>* ディレクトリに移動します。通常は、*C:¥Program Files¥CA¥SharedComponents¥iTechnology* です。

4. 以下のコマンドを実行して Safex スクリプトを実行します。

   ```
   >safex.exe -h localhost -u EiamAdmin -p <パスワード> -f <ファイル名>.xml
   ```

   たとえば、以下のようになります。

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Remove_application_policy.xml
   ```

   FIPS モードで CA EEM に統合されているアプリケーションに対して Safex ユーティリティを使用して CA EEM APM フロントエンドまたはビジネス サービス リソース アクセス ポリシーを削除する場合は、以下のコマンドを実行して Safex スクリプトを実行します。

   ```
   >safex.exe -h localhost -u EiamAdmin -p <パスワード> -f <ファイル名>.xml -fips
   ```

   たとえば、以下のようになります。

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Remove_application_policy.xml
   -fips
   ```

5. CA EEM 内の APM アプリケーション リソースを表示します。

   a. CA EEM にログインします。

   b. ［アクセス ポリシーの管理］タブをクリックします。

   c. ［ポリシー］リンクをクリックします。

   d. ［ポリシーの検索］ウィンドウで、［リソースに一致するポリシーを表示］をクリックします。次に、［リソース クラス名］ドロップダウン リストからアプリケーション ポリシー名を選択し、［実行］をクリックします。

   CA EEM の［ポリシー テーブル］ウィンドウに APM アプリケーション リソース アクセス ポリシーのリストが表示されます。 削除した APM アプリケーション アクセス ポリシーは表示されません。

クラスタ内での CA EEM の設定

クラスタ内で CA EEM によるセキュリティを提供するには、すべての Enterprise Manager が CA EEM 内の同じアプリケーションに接続するように *realms.xml* ファイルを構成します。また、クラスタに新しいコレクタを追加してエージェントまたは TIM の数を増やすときは、以下の手順に従います。

以下の手順に従います。

重要: CA EEM を許可に使用する場合、Enterprise Manager は CA EEM 内の 1 つ以上のアプリケーションに接続する必要があります。 その理由は、CA EEM では、権限を定義するアクセス ポリシーおよびリソース クラスを格納するためにアプリケーションを使用するからです。

1. Enterprise Manager （コレクタ、MOM、または CDV）で、CA EEM による許可のための *realms.xml* ファイルを構成します。
   a. *<EM_Home>/config* ディレクトリの *realms.xml* ファイルを開きます。
   b. *appname* プロパティを、Enterprise Manager が CA EEM 内で接続するアプリケーションの名前に設定します。 たとえば、*APM* となります。

      この名前は、CA EEM サーバを構成するときに使用するのと同じ APM アプリケーション名です。
   c. *enableAuthorization* プロパティを *True* に設定します。
   d. *realms.xml* ファイルを保存します。
   e. Enterprise Manager を再起動して *realms.xml* への変更を適用します。
2. クラスタ内の各 Enterprise Manager について上記の手順 1 を繰り返します。

   クラスタ内のすべての Enterprise Manager が CA EEM 内の同じアプリケーションに接続すると、CA EEM によるセキュリティがクラスタ全体で有効になります。

ローカルによるセキュリティから CA EEM によるセキュリティへの移行

これまでローカルによる認証および許可を使用して Introscope を実行していて、これから CA EEM ベースの認証および許可をデプロイする場合は、以下の手順に従います。

- CA EEM のインストール
- 認証用の CA EEM の構成
- 許可用の CA EEM の構成

また、CA EEM ベースの認証と、ローカル許可をデプロイすることもできます。 詳細については、「ローカル許可を使用するための CA EEM の構成 (P. 125)」を参照してください。

CA EEM によるセキュリティ デプロイについて十分に理解するには、「CA EEM による Introscope のセキュリティ保護 (P. 70)」のトピックを最初からお読みください。

LDAP から CA EEM によるセキュリティへの移行

これまで LDAP による認証およびローカル許可を使用して Introscope を実行していて、これから CA EEM ベースの認証および許可をデプロイする場合は、以下の手順に従います。

- CA EEM のインストール
- 認証用の CA EEM の構成
- 許可用の CA EEM の構成

CA EEM によるセキュリティ デプロイについて十分に理解するには、「CA EEM による Introscope のセキュリティ保護 (P. 70)」のトピックを最初からお読みください。

ローカル許可を使用するための CA EEM の構成

CA APM ユーザの認証が EEM によるセキュリティの領域で行われる場合、デフォルトでは、その CA APM ユーザの許可も EEM 領域で行われます。ただし、*realms.xml* 内の *enableAuthorization* フラグが *false* に設定されている場合、CA APM ユーザに対しては CA EEM で認証が行われた後、CA EEM による許可ではなくローカル許可が使用されます。 この場合、許可のアクセス ポリシーは、CA EEM によるセキュリティのユーザ グループのメンバであるこの CA APM ユーザのローカル領域に基づきます。 たとえば、LDAP または SiteMinder で構成された CA EEM を認証に使用すると同時に、権限をローカル領域に維持する場合は、ローカル許可を使用することもできます。

Introscope の場合、ローカル領域の権限は *domains.xml* および *server.xml* ファイルで定義します。

CA CEM の場合、ローカル領域のアクセス ポリシーはセキュリティ ユーザ グループのメンバシップに基づきます。

CA APM が CA EEM による認証の後にローカル許可を実行するには、CA EEM 内で APM のセキュリティ ユーザ グループにユーザを割り当てる必要があります。 ただし、この場合、CA EEM 内でアクセス ポリシーを作成する必要はありません。

許可にローカルによるセキュリティを使用することは、以下を意味します。

- *realms.xml* 内の *enableAuthorization* フラグが *false* に設定されます。
- Introscope の場合、CA EEM 内にユーザとグループを作成し、*domains.xml* ファイルで権限を割り当てる必要があります。
- CA CEM の場合、CA EEM 内でユーザおよび 4 つのデフォルト セキュリティ グループすべてを作成する必要があります。たとえば、CA EEM 内で *cemadmin* ユーザと *CEM システム管理者*セキュリティ グループを作成します。次に、*CEM システム管理者*セキュリティ グループのメンバとして *cemadmin* を割り当てます。これによって、*cemadmin* に *CEM システム管理者*セキュリティ グループの権限を付与します。 CA CEM の 4 つのデフォルト セキュリティ グループについては、「デフォルトの CA CEM のセキュリティ ユーザ グループに関連付けられるメニュー項目と権限 (P. 143)」を参照してください。

以下の手順に従います。

1. *<EM_Home>/config* ディレクトリの *realms.xml* ファイルを開きます。
2. *enableAuthorization* プロパティを *false* に設定します。

   この値を *false* に設定した場合、CA EEM は認証だけを実行し、許可にはローカルによるセキュリティ領域を使用します。 詳細については、「realms.xml での CA EEM による認証の構成 (P. 76)」を参照してください。 ローカル許可の詳細については、「ローカルによるセキュリティを使用した Introscope のセキュリティ保護 (P. 41)」を参照してください。
3. *realms.xml* ファイルを保存します。
4. ドメイン権限を構成します。「domains.xml での Introscope ドメイン権限の構成 (P. 50)」を参照してください。
5. Enterprise Manager サーバ権限を構成します。「Enterprise Manager サーバ権限の構成 (P. 54)」を参照してください。

Introscope シングル サインオン（SSO）について

シングル サインオン（SSO）は、本来であれば個別のログインが必要とされる複数のアプリケーションへのアクセスを 1 回のログインで済ませることのできる方法です。

ユーザが Introscope にログインするとき、使用しているブラウザが Cookie を受け入れる場合は、SSO が自動的に動作します。 それから後は、CA APM Web アプリケーション間を移動でき、各アプリケーションへのログインおよび再認証の必要はありません。 ユーザのブラウザが Cookie を受け入れない場合、SSO は動作しないため、CA APM の各アプリケーションには別々にログインする必要があります。

以下の Introscope Web アプリケーションが SSO をサポートしています。

- Web Start Workstation
- WebView
- CEM コンソール

Introscope Workstation（シック クライアント）は SSO をサポートしていません。

SiteMinder SSO および Introscope のセキュリティについて

CA EEM を使用して Introscope のセキュリティをデプロイしており、認証用の CA EEM サーバが CA SiteMinder に統合されている場合、Introscope Web アプリケーションは SiteMinder の SSO 機能を利用できます。 認証に SiteMinder を使用する CA EEM のデプロイについては、「CA SiteMinder を使用した CA EEM による認証の構成 (P. 80)」を参照してください。

Web アプリケーションが Introscope と SiteMinder SSO の両方のクレデンシャルを検出した場合、Web アプリケーションは最初に Introscope のクレデンシャルを使用して認証を試みます。 最初の認証が失敗した場合は、次に SiteMinder のクレデンシャルを使用して認証を試みます。

SiteMinder SSO の詳細については、「*CA APM for CA SiteMinder Web Access Manager ガイド*」を参照してください。

アプリケーション問題切り分けマップのセキュリティ保護

Introscope で CA EEM による許可をデプロイしている場合、アプリケーション問題切り分けマップにフロントエンドとビジネス サービスを表示するためのユーザ権限を設定できます。 権限を設定するには、Safex スクリプトを実行するか、CA EEM 内で、ビジネス アプリケーション（フロントエンド）およびビジネス サービス リソースに対して任意の権限（書き込み、読み取り、または機密データの読み取り）を指定します。

セキュリティに CA EEM を使用しない場合、ユーザは、アプリケーション問題切り分けマップにすべてのビジネス アプリケーションとビジネス サービスを表示できます。セキュリティに CA EEM をデプロイするが、関連するアクセス ポリシーで CA EEM ビジネス アプリケーションおよびビジネス サービス リソースとして特定のフロントエンドやビジネス サービスを追加 *しない* 場合も同様です。 CA EEM ビジネス アプリケーションおよびビジネス サービス リソースの詳細については、「CA EEM での APM リソース クラスの作成と削除 (P. 102)」を参照してください。 アプリケーション問題切り分けマップの使用時にユーザが表示できる内容の詳細については、「*CA APM Workstation ユーザ ガイド*」を参照してください。

ドメイン セキュリティはフロントエンドおよびビジネス サービス マップ セキュリティに加えて、アプリケーション問題切り分けマップに適用されます。 また、スーパードメイン セキュリティは、すべてのフロントエンドおよびビジネス サービス セキュリティに優先します。 ドメイン セキュリティによって、ユーザとグループが表示を許可されるエージェント データが制限されます。 詳細については、「スーパードメインのセキュリティは、アプリケーション問題切り分けマップのセキュリティに優先する (P. 131)」を参照してください。

eem.register.app.xml スクリプトを実行してデフォルトの CA APM アプリケーションを設定する場合は、以下に説明するビジネス サービスおよびビジネス アプリケーション（フロントエンド）のリソース クラスとアクションが提供されます。 詳細については、「CA EEM による許可の構成 (P. 82)」を参照してください。

アプリケーション問題切り分けマップのセキュリティをデプロイするには、CA EEM 内で以下の高レベルの手順を実行します。

1. ユーザ グループとユーザを定義します。

   APM グループ (P. 93)および APM ユーザ (P. 98)のサンプル スクリプトを使用できます。

2. ユーザ、グループ、および権限（CA EEM 内のアクション）に基づいてアクセス ポリシーを作成します。

   サンプル スクリプトについては、「CA EEM のアクセス ポリシーについて (P. 110)」を参照してください。

3. 各アクセス ポリシーをリソース クラスに関連付けます。 その後で、特定のリソースをアクセス ポリシーに追加して、ポリシーをさらに制限できます。

4. 個々のビジネス サービスとビジネス アプリケーション、およびビジネス サービスとビジネス アプリケーションのリソース クラスをポリシーに追加します。

   注: 個々のビジネス サービスおよびビジネス アプリケーションを、それぞれに対応するビジネス クラスのメンバとして定義する必要はありません。

詳細については、「CA EEM での APM リソース クラスの作成と削除 (P. 102)」の以下の手順を参照してください。

- アプリケーション問題切り分けマップのセキュリティを提供するビジネス サービス リソース クラスの権限を決定します。
- フロントエンドに対してアプリケーション問題切り分けマップのセキュリティを提供するビジネス アプリケーション リソース クラスの権限を決定します。

注: ビジネス サービスおよびビジネス アプリケーション（フロントエンド）の場合、ユーザは付与される権限によって、アプリケーション問題切り分けマップを表示するためのアクセス権が提供されます。

注: ビジネス サービスまたはビジネス アプリケーションを表示するためのユーザ権限を変更する場合、そのような変更は、ユーザが Workstation からいったんログアウトし再度ログインするまで、アプリケーション問題切り分けマップに反映されません。

注: リソースが指定されていないビジネス サービスまたはビジネス アプリケーション ポリシーは、そのビジネス サービスまたはビジネス アプリケーション リソース クラス内のすべてのリソースに適用されます。

フロントエンドを CA EEM ビジネス アプリケーション リソースとして追加し、そのフロントエンドをアプリケーション問題切り分けマップに表示する権限を、関連するビジネス アプリケーション リソース クラスのユーザまたはグループに与えないとします。その場合、ユーザまたはグループの問題切り分けマップ ツリーにフロントエンドは表示されません。 これは、ビジネス サービスにも当てはまります。ビジネス サービスも、ユーザが権限を与えられない限り、ツリーに表示されません。 ただし、ユーザが権限を与えられていないフロントエンドが、ビジネス サービスによって呼び出される場合、あるいはユーザまたはグループが表示を許可されている別のフロントエンドによって呼び出される場合、そのフロントエンドはマップに表示されます。しかし、以下の制約があります。

- 無効の状態で表示される
- 選択できない
- 依存関係またはメトリック データが表示されない

ただし、ユーザとグループは、このフロントエンドに関する個々のエージェント データをメトリック ブラウザ ツリーで表示できます。

重要: スーパードメイン権限を持っているユーザは、アプリケーション問題切り分けマップにフロントエンドと BusinessService を表示することを許可されます。詳細については、「スーパードメインのセキュリティは、アプリケーション問題切り分けマップのセキュリティに優先する (P. 131)」を参照してください。

Safex スクリプトを使用してアプリケーション問題切り分けマップの権限を設定する手順については、以下を参照してください。

- CA EEM での APM リソース クラスの作成と削除 (P. 102)
- 「CA EEM APM フロントエンドおよびビジネス サービス リソース アクセス ポリシーの作成と削除 (P. 119)」を参照してください。

注: アプリケーション問題切り分けマップのセキュリティが有効になっているときに Workstation でビジネス アプリケーションおよびビジネス サービスがどのように表示されるかについては、「CA APM Workstation ユーザ ガイド」を参照してください。

スーパードメインのセキュリティによるアプリケーション問題切り分けマップのセキュリティの上書き

ドメイン セキュリティはフロントエンドおよびビジネス サービス マップ セキュリティに加えて、アプリケーション問題切り分けマップに適用されます。 ドメイン セキュリティによって、ユーザとグループが表示を許可されるエージェント データが制限されます。 ドメイン セキュリティの詳細については、「Introscope ドメインの定義と構成 (P. 25)」および「domains.xml での Introscope ドメイン権限の構成 (P. 50)」を参照してください。

［問題切り分けマップ］タブでは、ドメイン セキュリティによって、ユーザとグループが以下で表示するエージェントが制限されます。

- アプリケーション問題切り分けマップの下の、物理的な位置のリスト内にあるエージェントのリスト
- 表示される任意のメトリックの下の、物理的な位置のリスト内にあるエージェントのリスト これらは、問題切り分けマップ ツリーのサブノードが選択されているときに表示されます。たとえば、［稼働状況］ノードや個々のメトリック ノードです。

*スーパードメイン*のセキュリティは、アプリケーション問題切り分けマップのセキュリティに優先します。 つまり、任意の領域（ローカルまたは EEM）で*スーパードメイン*のアクセス権を与えられているユーザは、ビジネス サービスとビジネス アプリケーションの読み取り権限が付与されていなくても、アプリケーション問題切り分けマップにフロントエンドとビジネス サービスをすべて表示できます。

たとえば、Introscope が 3 つのフロントエンド A、B、および C を監視しているとします。 Tai という名前の Introscope ユーザにフロントエンド A だけを表示する権限を付与します。 Tai は*スーパードメイン*のドメイン権限も持っており、すべてのエージェントの表示を許可されています。 この場合、Tai は、アプリケーション問題切り分けマップおよび Investigator ツリーの両方で 3 つのフロントエンドをすべて表示できます。

Introscope のセキュリティのトラブルシューティング

以下に、Introscope のセキュリティに関する問題をトラブルシューティングするときに役に立つヒントを示します。

症状:

CA APM グループ、ユーザ、およびリソース クラスをロードするために Safex スクリプトを実行すると、エラー メッセージが表示される。

エラー メッセージの例

```
"1375 [0x00000458] ERROR PozFactory null - PozFactory::attachPoz - Error invoking iPoz::ClientAttach on host localhost 1375 [0x00000458] ERROR PozFactory null - PozFactory::attachPoz Error: Bad signature: incompatible signature digest type in the request from host [192.168.200.1.ca.com:1331]. Server is running in [Fips_Mode_On] and request signature digest type is [ITECH_DIGEST_MD5]. FIPS does not support ITECH_DIGEST_MD5 digest type"
```

解決方法:

CA EEM サーバが FIPS 専用モードになっている。

CA EEM サーバの設定を非 FIPS モードに変更します。

症状:

Introscope ユーザが Introscope にログインするとき、エラー メッセージが表示される。

Introscope ユーザがログインできない。

解決方法:

ユーザ名とパスワードが正しく入力されていることを確認します。

症状:

Enterprise Manager が CA EEM APM アプリケーション インスタンスに接続しているかどうかを確認できない。

Introscope が CA EEM に接続しているかどうかがわからない。

解決方法:

<EM_Home>/logs/IntroscopeEnterpriseManager.log ファイル内のログ メッセージを参照してください。

ログ メッセージには以下の情報が表示されます。

- Enterprise Manager が CA EEM 内で接続しているアプリケーション
- CA EEM サーバの場所
- CA EEM サーバがユーザとグループを取得するために CA EEM と外部ディレクトリ（LDAP または SiteMinder）のどちらを使用しているか

例：

```
8/05/09 04:15:59 PM PDT [INFO] [Manager.EemRealm] EEM realm attached to application "APM" in EEM server at <EEM_Machine_Name> using SiteMinder
```

症状:

Enterprise Manager と CA EEM 間のインタラクションに問題がある。

Introscope CA EEM 接続をデバッグする。

解決方法:

CA EEM デバッグ プロパティを設定して、CA EEM に関するログ メッセージを表示します。 詳細については、「CA EEM 関連メッセージのログ記録の構成 (P. 75)」を参照してください。

Introscope のセキュリティ メカニズム

セキュリティ ニーズに応じて、以下の表に示す適切な Introscope のセキュリティ メカニズムを有効にします。

実現するセキュリティ メカニズム	この保護を実現する方法
Workstation、WebView、Web Start Workstation、または CEM コンソールから Enterprise Manager へログインする際のパスワードを変更し、セキュリティ保護する。	このセキュリティ上のベスト プラクティスは強く推奨されます。 Workstation、WebView、および Web Start のパスワードの詳細については、「CA APM Workstation ユーザ ガイド」を参照してください。 CEM コンソール パスワードの詳細については、「CA CEM (139P.)パスワードの管理」を参照してください。

実現するセキュリティ メカニズム	この保護を実現する方法
Enterprise Manager がインストールされている Windows または Linux マシン上のファイル システム セキュリティを設定し、使用する。	許可されたユーザだけが *users.xml* ファイルにアクセスして、ローカルによるセキュリティ用の APM ドメインをセットアップできるようにします。
コレクタと MOM 間の暗号鍵構成を設定し、使用する。	許可されたユーザだけがコレクタにアクセスできるようにします。 詳細については、「セキュリティ保護された認証のための公開鍵および秘密鍵の構成 (P. 35)」を参照してください。
APM データベースのパスワードを変更し、セキュリティ保護する。	許可されたユーザだけが APM データベースにアクセスできるようにします。 詳細については、「CA APM インストールおよびアップグレード ガイド」を参照してください。
データベース管理者の訓練	APM データベースの全般的な稼働状況を維持するため。
IntroscopeAgent.profile ファイル内の SSL 通信プロパティを構成して、SSL 上でのエージェント - Enterprise Manager 間通信を可能にする。	エージェントと Enterprise Manager 間の通信をセキュリティ保護します。 詳細については、「*CA APM Java Agent 実装ガイド*」または「*CA APM .NET Agent 実装ガイド*」を参照してください。
Enterprise Manager とブラウザ間の SSL 暗号化通信	Enterprise Manager とブラウザ間の通信をセキュリティ保護します。 詳細については、「HTTPS のみによる Enterprise Manager アクセスの制限 (P. 175)」を参照してください。
Introscope 認証	許可されたユーザだけが Introscope と CA APM にログインできるようにします。
Introscope の許可	許可されたユーザだけが Introscope ドメインにアクセスできるようにします。
アプリケーション問題切り分けマップのセキュリティ	許可されたユーザだけが、アプリケーション問題切り分けマップに特定のビジネス サービスおよびフロントエンドを表示できるようにします。 詳細については、「アプリケーション問題切り分けマップのセキュリティ保護 (P. 128)」を参照してください。

第 4 章: CA CEM のセキュリティ保護

CA CEM をアップグレードする場合は、「CA APM インストールおよびアップグレード ガイド」でセキュリティ関連のアップグレードのトピックを参照してください。

CA CEM のセキュリティについて必要な情報を以下に示します。

1. CA CEM のセキュリティについて理解する (P. 136)。
2. CA CEM のユーザおよびセキュリティ ユーザ グループについて理解する (P. 142)。
3. CA CEM パスワードの管理について理解する (P. 139)。
4. セキュリティに CA Embedded Entitlements Manager （CA EEM）をデプロイする場合は、以下について理解する。
   - CA CEM の EEM によるセキュリティ (P. 146)
   - 必要な CA CEM ユーザおよびセキュリティ ユーザ グループの管理 (P. 147)
   - リソース クラス (P. 149)
   - リソース (P. 150)
   - アクセス ポリシー (P. 151)
5. ローカルによるセキュリティをデプロイする場合は、以下について理解する。
   - CA CEM のローカルによるセキュリティ (P. 157)
   - 必要な CA CEM ユーザの管理 (P. 157)
6. プライベート パラメータを定義する (P. 160)。
7. セキュリティに関係のある HTTP 応答および要求コンテンツについて理解する (P. 162)。
8. （オプション）FIPS 140-2 暗号化を適用する (P. 170)。
9. （オプション）HTTPS を介した TIM 通信を構成する (P. 174)。
10. （オプション）ブラウザと Enterprise Manager 間の通信を HTTPS に限定する (P. 175)。

CA CEM のセキュリティ メカニズム

セキュリティ ニーズに応じて、以下の表に示す適切な CA CEM のセキュリティ メカニズムを有効にします。

実現するセキュリティ メカニズム	この保護を実現する方法
データ センターの保護エリア内で CA CEM を実行し、Introscope のセキュリティを設定する。	Enterprise Manager マシンへのアクセス権によって、Enterprise Manager ファイル システムへの不正アクセスを防止します。
データベース管理者の訓練	APM データベースの全般的な稼働状況を維持するため。
APM データベースのパスワードを変更し、セキュリティ保護する。	許可されたユーザだけが APM データベースにアクセスできるようにします。 詳細については、「CA APM インストールおよびアップグレード ガイド」を参照してください。
各 TIM マシンの Linux root アカウントのデフォルト パスワードを変更する。	TIM データ セキュリティ 詳細については、「CA APM インストールおよびアップグレード ガイド」を参照してください。
Workstation、WebView、Web Start Workstation、または CEM コンソールから Enterprise Manager へログインする際のパスワードを変更し、セキュリティ保護する。	Workstation、WebView、および Web Start のパスワードの詳細については、「CA APM Workstation ユーザ ガイド」を参照してください。 CEM コンソール パスワードの詳細については、「CA CEM (139P.)パスワードの管理」を参照してください。
Enterprise Manager と TIM 間の SSL 暗号化通信	Enterprise Manager と TIM 間の通信をセキュリティ保護します。 詳細については、「HTTPS を介した TIM 通信の構成 (P. 174)」を参照してください。
Enterprise Manager とブラウザ間の SSL 暗号化通信	Enterprise Manager とブラウザ間の通信をセキュリティ保護します。 詳細については、「HTTPS のみによる Enterprise Manager アクセスの制限 (P. 175)」を参照してください。

実現するセキュリティ メカニズム	この保護を実現する方法
FIPS 準拠のセキュリティ	Federal Information Processing Standards（連邦情報処理標準）による、より高いレベルのセキュリティ。 詳細については、「FIPS 140-2 準拠の暗号化 (P. 170)」を参照してください。
CA CEM の認証	許可されたユーザだけが CA CEM にログインできるようにします。
CA CEM の許可	特定のユーザが表示できる CEM コンソールのタブと、ユーザが操作できる特定のデータを決定するアクセス ポリシー
［Configure TIM Web Protect］オプション	クロスサイト リクエスト フォージェリから TIM Web ページを保護します。 詳細については、「TIM 用の Web 保護を設定する方法」を参照してください。

注: CA APM のセキュリティの基本事項を理解するには、「CA APM のセキュリティの概要 (P. 11)」および「Introscope がセキュリティをチェックする仕組み (P. 40)」を参照してください。

CA APM のセキュリティを設定する際、単一または混合のどちらのセキュリティ領域をデプロイするかを決める必要があります。 CA APM ユーザが CA CEM にアクセスするためには、ローカル、CA EEM、または LDAP のいずれかの領域をデプロイする必要があります。

TIM 用の Web 保護を設定する方法

［Configure TIM Web Protect］オプションを設定して、クロスサイト リクエスト フォージェリから TIM Web ページを保護します

以下の手順に従います。

1. TIM 設定ページにアクセスします。

   TIM 設定ページにアクセスする方法については、「*APM 設定および管理ガイド*」の「CEM コンソールおよびセットアップ ページへのアクセス」を参照してください。

2. ［Configure TIM Web Protect］オプションをクリックします。
3. 以下のいずれかのオプションを選択して、アプリケーションの要件に基づいてページを保護します。
   - システムの状態を変更するページ。
   - システム情報を表示するページ。
4. ［保存］をクリックします。

   TIM 保護が設定されます。

重要: TIM の Web 保護オプションを有効にしたページは、直接アクセスするためにブックマークすることはできません。

CA CEM 認証について

ローカル領域を使用して CA CEM ユーザを認証するデプロイの場合、*<EM_Home>/config* ディレクトリ ファイルの *users.xml* ファイルが CA CEM に対する CA CEM ユーザ クレデンシャルになります。

注: Wily CEM 4.5 からアップグレードして、ローカルによるセキュリティを使用する場合、Wily CEM 4.5 ユーザは *usersCEM45.xml* ファイルに登録されている可能性があります。 詳細については、「CA APM インストールおよびアップグレード ガイド」を参照してください。

CA EEM 領域の CA APM ユーザを認証するデプロイの場合、CA EEM サーバが CA CEM に対する CA CEM ユーザ クレデンシャルを提供します。

注: CA EEM サーバを SiteMinder と連携して動作するように構成している場合、SiteMinder をデプロイして CA EEM ユーザを認証できます。

CA CEM パスワードの管理

CA APM ユーザ パスワードは、EEM 領域とローカル領域の両方で暗号化されます。 パスワードがローカルによるセキュリティでどのように暗号化されるかについては、「users.xml での CA APM ユーザおよびグループの構成 (P. 46)」を参照してください。

ローカルによるセキュリティの場合、CA CEM で用意されている 2 つの CA CEM ユーザ *admin* および *cemadmin* をそのまま使用できます。 どちらのユーザも、管理者および CEM システム管理者という CA CEM のセキュリティ ユーザ グループに属します。 *admin* のデフォルト パスワードについては、「*CA APM インストールおよびアップグレード ガイド*」を参照してください。ローカルによるセキュリティでの CA CEM ユーザ パスワードの更新については、「users.xml での CA APM ユーザおよびグループの構成 (P. 46)」を参照してください。

CA EEM の CA APM 管理者は、CA CEM ユーザのパスワードを更新できます。CA CEM ユーザは、CA EEM の自己管理機能を使用して自分のパスワードを変更できます。

CA EEM 内で CA CEM ユーザのパスワードをリセットする方法

CA EEM の CA APM 管理者は、CA EEM 内で CA CEM ユーザのパスワードを更新できます。

1. CA EEM 内の APM アプリケーションにログインします。
   a. CA EEM ログイン ページで、［アプリケーション］ドロップダウン リストから［APM］を選択します。
   b. ログイン名とパスワードを入力します。

   APM アプリケーションのデフォルト ログインは *EiamAdmin* です。
2. ［ID の管理］タブに移動します。
3. ［ユーザの検索］ボックスで、［アプリケーション ユーザの詳細］を選択し、［実行］をクリックします。
4. ［ユーザ］ボックス ツリーで APM ユーザ名をクリックします。

5. ユーザ情報が表示されたら、［認証］ボックスで以下のどちらかを実行します。
   - ［次のログイン時にパスワードを変更］チェック ボックスをオンにします。
   - ［パスワードをリセット］チェック ボックスをオンにし、新しいパスワードを入力および確認します。 新しいパスワードをユーザに通知します。
6. ［保存］をクリックします。

   詳細については、「*CA Embedded Entitlements Manager Online Help*」を参照してください。

自己管理機能によって CA EEM パスワードをリセットする方法

CA CEM ユーザは、自己管理手順を使用して、CA EEM 内で自分のパスワードを変更できます。

1. CA EEM 内の APM アプリケーションにログインします。
   a. CA EEM ログイン ページで、［アプリケーション］ドロップダウン リストから［グローバル］を選択します。
   b. ログイン名とパスワードを入力します。
2. ［ホーム］タブに移動します
3. ［自己管理］ボックスで［パスワードを変更］リンクをクリックします。

   詳細については、「*CA Embedded Entitlements Manager Online Help*」を参照してください。

CA CEM の許可について

CA CEM ユーザがローカルで許可されると、各ユーザが属する CA CEM のセキュリティ ユーザ グループに基づいて、特定のユーザが表示できる CEM コンソールのタブと、そのユーザが操作できる特定のデータが決まります。アクセス ポリシーは、CA CEM のセキュリティ ユーザ グループに基づいて割り当てられます。

ローカル領域を使用して CA APM ユーザを許可するデプロイの場合、標準的な CA CEM のセキュリティ ユーザ グループによる CEM コンソールの表示は、*users.xml* （Wily CEM 4.5 からアップグレードした場合は *usersCEM45.xml*）によって許可されます。これについては、「デフォルトの CA CEM のセキュリティ ユーザ グループに関連付けられるメニュー項目と権限 (P. 143)」で説明しています。詳細については、「ローカルのユーザとグループおよび CA CEM (P. 157)」を参照してください。

CA CEM ユーザが CA EEM 内で許可されると、アクセス ポリシーによって、特定のユーザが表示できる CEM コンソール タブと、そのユーザが操作できる特定のデータが決まります。

CA EEM で CA APM ユーザを許可するデプロイの場合、CA EEM 内でアクセス ポリシーを設定するには、Safex スクリプトの *eem.register.app.xml* を実行するか（推奨）、手動で行います。

<EM_Home>/examples/authentication ディレクトリにある Safex スクリプトの *eem.register.app.xml* を実行してアクセス ポリシーを設定する場合、標準的な CA CEM ユーザ グループによる CEM コンソールの表示は CA EEM によって許可されます。これについては、「デフォルトの CA CEM のセキュリティ ユーザ グループに関連付けられるメニュー項目と権限 (P. 143)」で説明しています。

詳細については、「CA CEM の CA EEM による認証および許可 (P. 146)」および「CA EEM のアクセス ポリシーについて (P. 110)」を参照してください。

CA CEM のセキュリティ ユーザ グループについて

CA CEM にはデフォルトで 4 つのセキュリティ ユーザ グループがあります。旧バージョンの CA CEM からアップグレードしている場合、CA CEM のロールという概念はよく理解されています。 CA APM のセキュリティを統一化するため、現在、CA CEM のロールは CA CEM セキュリティ ユーザ グループと呼ばれています。

デフォルトの CA CEM のセキュリティ ユーザ グループは以下のとおりです。

- 管理者 -- Introscope と CA CEM へのアクセス権を持ち、Introscope 管理者と CEM システム管理者の権限が付与されます。
- CEM システム管理者 -- CA CEM のシステム機能をすべて管理します。
- CEM 構成管理者 -- 一般的な CA CEM 構成を管理します。
- CEM アナリスト -- CA CEM のレポートとビューのみへのアクセス権を持ちます。
- CEM インシデント アナリスト -- 障害に関する HTTP 情報を含む、CA CEM のレポートとビューへのアクセス権を持ちます。

CA CEM システムのセキュリティを保護するため、管理者グループに割り当てるユーザの数をできる限り少なくすることをお勧めします。

デフォルトの CA CEM のセキュリティ ユーザ グループのメンバが表示できる CA CEM タブについては、「デフォルトの CA CEM のセキュリティ ユーザ グループに関連付けられるメニュー項目と権限 (P. 143)」を参照してください。

ローカルによるセキュリティをデプロイする場合、CA CEM ではこれらのデフォルト グループを *users.xml* ファイルで指定します。

重要: ローカル許可をデプロイする場合、デフォルトの CA CEM のセキュリティ ユーザ グループにセキュリティ ユーザ グループを追加したり、これらのグループに関連付けられたアクセス ポリシーを変更したりすることはできません。 詳細については、「ローカルのユーザとグループおよび CA CEM (P. 157)」を参照してください。

セキュリティに CA EEM をデプロイする場合、CA CEM のセキュリティ ユーザ グループとアクセス ポリシーの設定は CA EEM サーバで行います。具体的には、Safex スクリプトを実行するか、CA EEM 内で操作します。 詳細については、「CA EEM での APM グループの作成と削除 (P. 93)」を参照してください。CA CEM のセキュリティ ユーザ グループは、必要に応じて、追加、変更、または削除できます。

重要: アクセス ポリシーを設定して CA CEM ユーザが表示できる内容を制限する場合は、CA EEM による許可をデプロイする必要があります。

その他の CA CEM の認証および許可のソリューション

CA CEM 認証には LDAP を構成できます。

CA APM 認証のための LDAP の構成については、「LDAP による Introscope のセキュリティ保護 (P. 57)」を参照してください。

重要: 認証に LDAP を使用する場合は、CA APM ユーザ グループを手動で構成する必要があります。 LDAP グループ名が CA CEM グループ名に完全に一致していることを確認してください。

また、ローカルによるセキュリティを使用して CA CEM を許可するように CA EEM を構成することもできます。 それには、許可にローカル領域が使用されるように CA EEM を構成します。 詳細については、「ローカル許可を使用するための CA EEM の構成 (P. 125)」を参照してください。

デフォルトの CA CEM のセキュリティ ユーザ グループに関連付けられるメニュー項目と権限

以下の表に、デフォルトの CA CEM のセキュリティ ユーザ グループに関連付けられるメニュー項目と権限を示します。

メニュー 機能	CEM システム管理者	CEM 構成管理者	CEM アナリスト	CEM インシデント アナリスト
パッチ： 電子メール設定 イベント	○	×	×	×

メニュー 機能	CEM システム管理者	CEM 構成管理者	CEM アナリスト	CEM インシデント アナリスト
セキュリティ： プライベート パラメータ FIPS 設定 アクセス ポリシー（CA EEM のみ）	○	×	×	×
設定 ドメイン 監視 サービス Web サーバ フィルタ インシデントの設定 HTTPS 設定 プラグイン Introscope 設定	○	○	×	×
管理 概要 ビジネス アプリケーション ビジネス サービス 規格 ユーザ グループ 相関 SLA 記録セッション トランザクション検出	○	○	×	×
ツール スクリプト レコーダ	○	○	×	×

メニュー 機能	CEM システム管理者	CEM 構成管理者	CEM アナリスト	CEM インシデント アナリスト
CEM サービス レベル管理 インシデント管理 » 注を参照 パフォーマンス レポート 品質レポート 分析グラフ マイ レポート	はい -- すべてのページ	はい -- ［CEM］ - ［インシデント管理］ - ［障害詳細］ページの［HTTP 情報］セクションの表示を除く	はい -- ［CEM］ - ［インシデント管理］ - ［障害詳細］ページの［HTTP 情報］セクションの表示を除く	はい -- すべてのページ

注: ［CEM］ - ［インシデント管理］ - ［障害詳細］ページの［HTTP 情報］セクションでは、Query パラメータ、Post パラメータ、および要求と応答の本文に関する追加データを表示できます。 この情報は、［包括的な障害詳細をキャプチャ］チェック ボックス（［設定］ - ［ドメイン］ページ）がオンになっている場合、TIM によって収集されます。

この追加データを表示するには、ユーザは、障害に関してビジネス サービスに対する*機密データの読み取り*アクセス権が付与されるグループのメンバである必要があります。 たとえば、CEM インシデント アナリスト グループにはこのアクセス権があります。

詳細については、「障害時の HTTP 要求および応答の保護 (P. 162)」を参照してください。

CA CEM の CA EEM による認証および許可

CA EEM の基本事項を理解するには、「CA EEM による Introscope のセキュリティ保護」を参照してください。

CA CEM のセキュリティに CA EEM をデプロイする場合、認証と許可は CA EEM サーバで行われます。CA EEM による許可は、セキュリティ ユーザ グループのメンバシップではなく、アクセス ポリシーに基づいています。CA EEM 内では、アクセス ポリシーは、リソース クラス、リソース、および権限（読み取りや書き込みなど）の 3 つの要素で構成されます。詳細については、「CA EEM のアクセス ポリシーについて (P. 110)」を参照してください。

注: CA EEM では、権限はアクションと呼ばれます。

以下のトピックでは、CA CEM 固有のデフォルト リソース クラス、リソース、およびアクセス ポリシーについて説明します。CA APM には、デフォルトの CA APM アプリケーションを登録し、CA CEM のグローバル ユーザ、アプリケーション固有のユーザ、セキュリティ ユーザ グループ、リソース クラス、およびリソース クラスのアクセス ポリシーを作成する、CA EEM Safex スクリプトが用意されています。

CA EEM での CA CEM ユーザおよびグループの管理

CA CEM のセキュリティは CA EEM アクセス ポリシーに基づいています。このポリシーは、特定のユーザおよびアプリケーション固有のユーザ グループに適用されます。

標準的な CA CEM ユーザおよびグループを提供する APM アプリケーションを設定するには、Safex スクリプトの *eem.register.app.xml* および *eem.add.global.identities.xml* を実行することをお勧めします。 これらの Safex スクリプトによって、グローバル ユーザ、グローバル ユーザ グループ、および APM アプリケーション固有のユーザ グループが作成されます。

CA EEM 内で CA CEM ユーザは CA CEM の 4 つのデフォルト セキュリティ グループ（CEM システム管理者、CEM 構成管理者、CEM アナリスト、または CEM インシデント アナリスト）のいずれかに属することができますが、強制ではありません。 CA CEM ユーザは、HR 管理者グループなど、定義した新しいグループに属することができます。デフォルトの CA CEM のセキュリティ ユーザ グループの詳細については、「デフォルトの CA CEM のセキュリティ ユーザ グループに関連付けられるメニュー項目と権限 (P. 143)」を参照してください。

CA CEM ユーザおよびグループは、作成、追加、変更、または削除できます。 また、CA CEM ユーザを有効または無効にすることもできます。

重要: CEM コンソールを使用している CA APM ユーザが Introscope Investigator データを表示するには、そのユーザが APM のセキュリティ ユーザ グループ 1 つと、CA CEM のセキュリティ ユーザ グループ 1 つの両方に含まれている必要があります。 たとえば、APM ゲスト グループと CEM アナリスト グループといった組み合わせがあります。 詳細については、「CA EEM Introscope ユーザに対する CEM コンソール アクセス権の付与 (P. 156)」または「ローカル Introscope ユーザに対する CEM コンソール アクセス権の付与 (P. 158)」を参照してください。

CA CEM ユーザを追加、変更、または削除する方法

- CA CEM ユーザを追加、変更、または削除するには、「CA EEM での APM ユーザの作成と削除 (P. 98)」で説明している方法のいずれかを使用します。

CA CEM のセキュリティ ユーザ グループを追加、変更、または削除する方法

- CA CEM のセキュリティ ユーザ グループを追加、変更、または削除する方法は、「CA EEM での APM グループの作成と削除 (P. 93)」で説明しています。

CA CEM ユーザを有効または無効にする方法

1. CA EEM 内の APM アプリケーションにログインします。
   a. CA EEM ログイン ページで、［アプリケーション］ドロップダウン リストから［APM］を選択します。
   b. ログイン名とパスワードを入力します。

   CA APM アプリケーションのデフォルト ログインは *EiamAdmin* です。
2. ［ID の管理］タブに移動します。
3. ［ユーザの検索］ボックスで、［アプリケーション ユーザの詳細］を選択し、［実行］をクリックします。
4. ［ユーザ］ボックス ツリーで APM ユーザ名をクリックします。
5. ユーザ情報が表示されたら、［認証］ボックスで以下のどちらかを実行します。
   - ［再開日］の右側にあるカレンダをクリックします。
   - ［停止日］の右側にあるカレンダをクリックします。
6. 有効化または無効化のアクションが行われる日付と時刻を選択し、［OK］をクリックします。
7. ［保存］をクリックします。

   詳細については、「*CA Embedded Entitlements Manager Online Help*」を参照してください。

CA EEM 内の CA CEM リソース クラスについて

CA CEM の許可に CA EEM を使用する場合は、CA CEM のセキュリティ ユーザ グループが表示できる CEM コンソールのタブを決めるためのアクセス ポリシーを設定します。 リソース クラスはアクセス ポリシーの必須要素です。 各リソース クラスには権限が関連付けられます。CA EEM では権限のことをアクションと呼びます。

以下の表に、CA CEM のデフォルト リソース クラスに関連付けられるアクションを示します。

CA CEM リソース クラス	デフォルト アクション
ビジネス アプリケーション	書き込み
ビジネス サービス	書き込み 読み取り 機密データの読み取り
インシデント	書き込み
レポート	書き込み
サーバ	書き込み
システム管理設定	書き込み
システム セキュリティ設定	書き込み
ユーザ グループ	書き込み
Web サービス	許可
アクセス ポリシー	書き込み

リソース クラスに［書き込み］アクションが関連付けられているとき、そのリソース クラスへのアクセス権を与えられた CA CEM ユーザまたはグループの CEM コンソール メニューには、関連するタブが表示されます。たとえば、ビジネス アプリケーション リソース クラスによって、CA CEM ユーザの CEM コンソールには、［管理］ -［ビジネス アプリケーション］が表示されます。

ビジネス サービス リソース クラスには、*読み取り*および*機密データの読み取り*の 2 つだけの追加アクションも関連付けられています。 ビジネス サービスに対する*機密データの読み取り*権限を持っている CA CEM ユーザは、その特定のビジネス サービスの障害に加えられた HTTP ヘッダ情報を表示できます。 詳細については、「CA APM 設定および管理ガイド」を参照してください。

ビジネス サービス リソース クラスは、CA CEM ユーザが TIM およびエージェント記録へのアクセス権を持っているかどうかも決定します（[管理] - ［記録セッション］）。 1 つ以上のビジネス サービスに対する書き込み権限を持っているユーザは、［記録セッション］タブにアクセスできます。

Introscope 固有のリソース クラスについて

デフォルトの CA APM アプリケーションは、CA CEM リソース クラスに加え、Introscope 固有の 2 つのリソース クラスを備えています。

- ドメイン： Introscope ユーザに対し、Introscope 固有のドメイン（スーパードメインなど）を表示する権限を与えます。

  注: これは［CEM］-［設定］-［ドメイン］の機能とは関係ありません。

- サーバ： Introscope ユーザに対し、Enterprise Manager を起動および停止する権限を与えます。

これらのリソース クラスを編集または削除しないでください。

CA EEM 内の CA CEM リソースについて

デフォルトの CA APM アプリケーションは CA CEM リソースを必要としません。CA EEM 内では、リソース クラスは関連するリソースを持たないか、1 つ以上持つことができます。

ただし、CA CEM には、ビジネス サービス リソース クラスのリソースを作成する機能があります。 作成するビジネス サービス リソースは、組織に固有のものになります。 ビジネス サービス リソースを作成するときは、各ビジネス サービスに 1 つ以上のアクセス ポリシーを関連付けます。 CA EEM 内の CA CEM リソースを編集することもできます。

CEM コンソールまたは CA EEM 内では、ビジネス サービスを設定できます。ビジネス サービスのデフォルト アクセス ポリシーの詳細については、「デフォルトの CA EEM CEM アクセス ポリシー (P. 151)」を参照してください。 新しいビジネス サービスの作成については、「*CA APM トランザクション定義ガイド*」を参照してください。

また、固有のアクセス ポリシーを持つ CA EEM 内で CA CEM リソースを作成しなければならない場合もあります。 特定のビジネス サービス リソースの権限を、特定の CA CEM ユーザおよびセキュリティ ユーザ グループに制限したい場合などは、そのようにすることがあります。

重要: CA EEM 内で新しい CA CEM リソースを作成する場合は、CA EEM 内で定義されている既存の CA CEM リソース クラスおよびアクセス ポリシーを使用する必要があります。

新しいリソースを定義するには、「デフォルトの CA EEM CEM アクセス ポリシー (P. 151)」で説明しているとおり、新しいアクセス ポリシーを定義します。

デフォルトの CA EEM CEM アクセス ポリシー

CA EEM 内では、アクセス ポリシーは、アプリケーション固有のリソース クラスおよびリソースのアクセス ルールを定義します。

警告： Introscope 管理者でない限り、CA EEM 内に表示されるドメインとサーバのアクセス ポリシーを変更または削除しないでください。 これらは Introscope 専用のアクセス ポリシーです。

CA EEM 内では、アクセス ポリシーは、リソース クラス、リソース、およびアクションの 3 つの要素で構成されます。

デフォルトの CA CEM アクセス ポリシーは、標準的な CA CEM のセキュリティ ユーザ グループに対し、CEM コンソールのメニューと権限を提供します。詳細については、「デフォルトの CA CEM のセキュリティ ユーザ グループに関連付けられるメニュー項目と権限 (P. 143)」を参照してください。

<EM_Home>/examples/authentication ディレクトリにある Safex スクリプト ファイルの *eem.register.app.xml* を実行することをお勧めします。 Safex スクリプトを実行して APM アプリケーションを設定するときのために、CA Technologies では、以下に示すとおり、APM アプリケーション用のデフォルトの CA CEM アクセス ポリシーを用意しています。

CA CEM アクセス ポリシー	説明	リソース クラス/アクション	付与されるセキュリティ ユーザ グループ
Web サービス - 許可	CEM システム管理者グループは、Web サービスに関する情報を表示できます	Web サービス/許可	CEM システム管理者
ユーザ グループ - 書き込み	CEM システム管理者グループおよび CEM システム構成管理者グループは、［管理］-［ユーザ グループ］タブ上で実行できるすべてのアクティビティ用の書き込み権限を持ちます	ユーザ グループ/書き込み	CEM システム管理者 CEM 構成管理者
システム セキュリティ設定	CEM システム管理者グループは、［システム セキュリティ設定］下のすべてのリソースに対する書き込み権限を持ちます	システム セキュリティ設定/書き込み	CEM システム管理者
システム構成設定 - 書き込み	CEM システム管理者グループおよび CEM 構成管理者グループは、［システム構成設定］下のすべてのリソースに対する書き込み権限を持ちます。	システム構成設定/書き込み	CEM システム管理者 CEM 構成管理者
システム構成設定 - 包括的な障害詳細をキャプチャ	CEM システム管理者グループは、［包括的な障害詳細をキャプチャ］チェック ボックスに対する書き込み権限を持ちます。	システム構成設定/包括的な障害詳細をキャプチャ	CEM システム管理者

CA CEM アクセス ポリシー	説明	リソース クラス/アクション	付与されるセキュリティ ユーザ グループ
システム管理設定 - 書き込み	CEM システム管理者グループは、［システム管理設定］下のすべてのリソースに対する書き込み権限を持ちます。	システム管理設定/書き込み	CEM システム管理者
レポート - 書き込み	すべての CEM グループは、すべてのレポートに対する書き込み権限を持ちます。	レポート/書き込み	CEM システム管理者 CEM 構成管理者 CEM アナリスト CEM インシデント アナリスト
インシデント - 書き込み	すべての CEM グループは、すべてのインシデントに対する書き込み権限を持ちます。	インシデント/書き込み	CEM システム管理者 CEM 構成管理者 CEM アナリスト CEM インシデント アナリスト
ビジネス サービス - 機密データの読み取り	CEM インシデント アナリスト グループは、すべてのビジネス サービスに対する機密データの読み取り権限を持ちます。	ビジネス サービス/機密データの読み取り	CEM インシデント アナリスト
ビジネス サービス - 読み取り	CEM アナリスト グループおよびインシデント アナリスト グループは、すべてのビジネス サービスに対する読み取り権限を持ちます。	ビジネス サービス/読み取り	CEM アナリスト CEM インシデント アナリスト
ビジネス サービス - 読み取り/書き込み	CEM 構成管理者グループは、すべてのビジネス サービスに対する読み取りおよび書き込み権限を持ちます。	ビジネス サービス/ 書き込み ビジネス サービス/読み取り	CEM 構成管理者

CA CEM アクセス ポリシー	説明	リソース クラス/アクション	付与されるセキュリティ ユーザ グループ
ビジネス サービス - すべての権限	CEM システム管理者グループは、すべてのビジネス サービス機能に対するすべての権限を持ちます。	ビジネス サービス/書き込み ビジネス サービス/読み取り ビジネス サービス/機密データの読み取り	CEM システム管理者
ビジネス アプリケーション - 書き込み	CEM システム管理者グループおよび CEM 構成管理者グループは、すべてのビジネス アプリケーションに対する書き込み権限を持ちます。	ビジネス アプリケーション/書き込み	CEM システム管理者 CEM 構成管理者
アクセス ポリシー - すべての権限	CEM システム管理者グループおよび CEM 構成管理者グループは、すべてのアクセス ポリシーに対するすべての権限を持ちます。	アクセス ポリシー/書き込み アクセス ポリシー/読み取り	CEM システム管理者 CEM 構成管理者

CA CEM ビジネス サービスのデフォルトのアクセス ポリシーについて

CA CEM の許可に CA EEM をデプロイした場合、CA EEM 内でアクセス ポリシーを作成および変更できます。また、CEM コンソールの［アクセス ポリシー］タブを使用して、ビジネス サービスに関連付けられた CA CEM アクセス ポリシーを追加、変更、または削除できます。

CA CEM の［アクセス ポリシー］タブを使用して CA CEM アクセス ポリシーを追加または変更する場合は、以下のことが該当します。

- *アクセス ポリシー* リソース クラスへの書き込み権限が必要です。
- CEM コンソールを使用してアクセス ポリシーを管理することによって、個々の APM ユーザではなく、APM アプリケーション セキュリティ ユーザ グループに限定して、権限の付与または取り消しが可能になります。 詳細については、「CA APM 設定および管理ガイド」を参照してください。

- 「CA EEM での CA CEM アクセス ポリシーの更新 (P. 155)」で説明しているとおり、アクセス ポリシーを直接変更することもできます。
- CA CEM は、アクセス ポリシーの変更を CA EEM に直接送信して格納します。

デフォルトのビジネス サービス アクセス ポリシーを作成または編集するか、新しいビジネス サービスに関連付ける場合は、「CA APM トランザクション定義ガイド」を参照してください。

CA EEM での CA CEM アクセス ポリシーの更新

CA EEM 内でデフォルトの CA CEM アクセス ポリシーを変更すると、以下のことが可能になります。

- CA CEM ユーザまたはセキュリティ ユーザ グループが CA CEM のタブを表示することを許可する。
- CA CEM ユーザまたはセキュリティ ユーザ グループが CA CEM のタブを表示することを制限する。

以下の手順に従います。

1. CA EEM 内の APM アプリケーションにログインします。
   a. CA EEM ログイン ページで、［アプリケーション］ドロップダウン リストから［APM］を選択します。
   b. ログイン名とパスワードを入力します。

   CA APM アプリケーションのデフォルト ログインは *EiamAdmin* です。
2. ［アクセス ポリシーの管理］ - ［アクセス ポリシー］に移動します。
3. ［アクセス ポリシー］ツリー内のアクセス ポリシー、たとえば、［レポート］をクリックします。
4. ［ポリシー テーブル］セクションで、アクセス ポリシー名のリンク、たとえば、［レポート - 書き込み］をクリックします。

5. ［ID］セクションで、ポリシーに関連付ける CA CEM ユーザまたはセキュリティ ユーザ グループを追加または更新します。

   たとえば、CEM インシデント アナリスト グループのレポート書き込みアクセス ポリシーへの関連付けを解除したい場合は、［CEM アナリスト］グループを強調表示し、［選択された ID］ボックスの右側にあるゴミ箱アイコンをクリックします。

6. ［保存］をクリックします。

CA EEM での新しい CA CEM アクセス ポリシーの追加

CA EEM 内では、新しい CA CEM アクセス ポリシーを追加できます。 その場合は、APM のデフォルトのリソース クラスと権限セットを使用する必要があります。

以下の手順に従います。

- Safex スクリプトを実行して、既存のリソース クラスに関連付ける新しいポリシーを追加します。 「CA EEM APM フロントエンドおよびビジネス サービス リソース アクセス ポリシーの作成と削除 (P. 119)」を参照してください。

CA EEM Introscope ユーザに対する CEM コンソール アクセス権の付与

Introscope ユーザが CEM コンソールを表示するには、許可が成功するように 1 つ以上の CA CEM リソース クラスについてアクセス ポリシーが定義されている必要があります。Introscope ユーザに CEM コンソールへのアクセス権を与えるため、そのユーザに対して 1 つ以上の CA CEM リソース クラスのアクセス ポリシーを定義します。

以下の手順に従います。

1. CA EEM 内の APM アプリケーションにログインします。

   a. CA EEM ログイン ページで、［アプリケーション］ドロップダウン リストから［APM］を選択します。

   b. ログイン名とパスワードを入力します。

   CA APM アプリケーションのデフォルト ログインは *EiamAdmin* です。

2. ［アクセス ポリシーの管理］ - ［アクセス ポリシー］に移動します。
3. ［アクセス ポリシー］ツリー内のアクセス ポリシー、たとえば、［システム管理設定］をクリックします。
4. ［ポリシー テーブル］セクションで、アクセス ポリシー名のリンク、たとえば、［システム管理設定 - 書き込み］をクリックします。
5. ［ID］セクションで、アクセス ポリシーに Introscope ユーザを追加します。
6. ［保存］をクリックします。

CA CEM のローカルによる認証および許可

CA CEM にローカルによるセキュリティをデプロイする場合、CA APM では認証と許可に *users.xml* ファイルを使用します。 ローカルによるセキュリティの背景情報については、「ローカルによるセキュリティを使用した Introscope のセキュリティ保護 (P. 41)」を参照してください。

注: Wily CEM 4.5 からアップグレードして、ローカルによるセキュリティを使用する場合、Wily CEM 4.5 ユーザは *usersCEM45.xml* ファイルに登録されている可能性があります。 詳細については、「CA APM インストールおよびアップグレード ガイド」を参照してください。

ローカルのユーザとグループおよび CA CEM

ローカルによるセキュリティをデプロイする場合、CA CEM ではデフォルトのセキュリティ ユーザ グループを *users.xml* ファイル（Wily CEM 4.5 からアップグレードした場合は *usersCEM45.xml*）で指定します。

ローカル CA CEM ユーザ、つまり *users.xml* ファイル（Wily CEM 4.5 からアップグレードした場合は *usersCEM45.xml*）に定義されたユーザが CEM コンソールにアクセスするには、CA CEM の 4 つの標準的なセキュリティ ユーザ グループのうちのいずれか 1 つのメンバである必要があります。

警告： ローカル許可をデプロイする場合、デフォルトの CA CEM グループにセキュリティ ユーザ グループを追加したり、これらのグループに関連付けられたアクセス ポリシーを変更したりすることはできません。 CA CEM のローカルによるセキュリティはこれらのグループにのみ基づきます。 どのような変更も、CA CEM のセキュリティ デプロイに関する問題を引き起こす場合があります。

users.xml （Wily CEM 4.5 からアップグレードした場合は *usersCEM45.xml*）内の CA CEM ユーザを許可するデプロイの場合、CA CEM アクセス ポリシーは固定され、変更できません。 これは、以下のことを意味します。

- 標準的な CA CEM のセキュリティ ユーザ グループの新しい名前を追加したり、グループの名前を変更したりすることはできません。
- CA CEM のセキュリティ ユーザ グループにはユーザを追加できます。
- 各ユーザは標準的な CA CEM のセキュリティ ユーザ グループ（CEM システム管理者、CEM 構成管理者、CEM アナリスト、または CEM インシデント アナリスト）のいずれか 1 つに属する必要があります。ユーザがメンバとなっているグループに基づいて、そのユーザのアクセス ポリシーが決まります。標準的な CA CEM のセキュリティ ユーザ グループが CEM コンソールで表示する内容については、「デフォルトの CA CEM のセキュリティ ユーザ グループに関連付けられるメニュー項目と権限 (P. 143)」を参照してください。

CA CEM ユーザは追加、変更、または削除できます。

以下の手順に従います。

- *users.xml* で CA CEM ユーザを追加、変更、または削除します。 詳細については、「users.xml での CA APM ユーザおよびグループの構成 (P. 46)」を参照してください。

ローカル Introscope ユーザに対する CEM コンソール アクセス権の付与

ローカルの Introscope ユーザが CEM コンソールを表示するには、APM のセキュリティ ユーザ グループ 1 つと、CA CEM のセキュリティ ユーザ グループ 1 つの両方に含まれている必要があります。 たとえば、APM ゲスト グループと CA CEM アナリスト グループといった組み合わせがあります。

以下の手順に従います。

- *users.xml* で、CA CEM ユーザ グループに Introscope ユーザを追加します。「users.xml での CA APM ユーザおよびグループの構成 (P. 46)」を参照してください。

たとえば、Introscope の認証および許可のために *users.xml* に登録されている Tandav Gupta という名前のユーザを、CEM システム管理者グループに追加します。

CA CEM のその他のセキュリティ タスク

CA EEM CEM およびローカルによるセキュリティを使用した認証と許可の設定タスクに加えて、CA CEM のセキュリティ リンクについて学習し、以下に示す CA CEM のその他のセキュリティ タスクを実行できます。

- CA CEM の［セキュリティ］リンク（P. 159）
- 新しいビジネス サービスのデフォルト アクセス ポリシーの設定（「*CA APM 設定および管理ガイド*」を参照）
- プライベート パラメータの定義（P. 160）
- 障害時の HTTP 要求および応答の保護（P. 162）
- FIPS 140-2 準拠の暗号化（P. 170）
- HTTPS を介した TIM 通信の構成（P. 174）
- HTTPS のみによる Enterprise Manager アクセスの制限（P. 175）
- CA CEM レポートのビジネス サービス データを参照できるユーザを制限する場合は、CA EEM を使用して、EEM が CA APM の唯一のセキュリティ領域になるように設定する必要があります。 詳細については、「セキュリティ領域について（P. 15）」のトピック、および「CA APM 設定および管理ガイド」の CA CEM のレポート機能に関する箇所を参照してください。

CA CEM の［セキュリティ］リンク

［セキュリティ］リンク上に表示されるタブは、Introscope または CA APM をインストール済みであるかどうか、および CA EEM を使用しているかどうかによって異なります。

たとえば、セキュリティ ソリューションにかかわらず、プライベート パラメータは常に非表示にすることができます。 ただし、認証と許可に CA EEM を使用する場合は、ビジネス サービスへのアクセスしか制限できません。以下の表に、実装したセキュリティ ソリューションに基づいて CEM コンソールに表示される内容を示します。

この CA CEM タブは表示されるか?	Introscope のみ（CA EEM あり）	Introscope のみ（CA EEM なし）	CA APM（CA EEM あり）	CA APM（CA EEM なし）
プライベート パラメータ	○	○	○	○

この CA CEM タブは表示されるか?	Introscope のみ（CA EEM あり）	Introscope のみ（CA EEM なし）	CA APM（CA EEM あり）	CA APM（CA EEM なし）
アクセス ポリシー	○	×	○	×
FIPS 設定	×	×	○	○

プライベート パラメータの定義

HTTP パラメータは HTTP で使用される名前と値のペアです。一般的なタイプの HTTP パラメータは、Cookie、Query、および Post です。CA CEM の HTTP パラメータの詳細については、「CA APM トランザクション定義ガイド」を参照してください。

CA CEM は、トランザクション記録および認識プロセスの一環として HTTP パラメータを記録します。 通常、すべての HTTP パラメータは、記録されるすべてのトランザクションについて表示されます。

CA CEM のプライベート パラメータでは、プライベートのままにする必要のある HTTP ヘッダ情報を指定できます。 CA CEM のプライベート パラメータ値は、システム管理者、構成管理者、またはすべての CA CEM ユーザに表示されません。 エンドユーザのみがパラメータの値を把握しています。

ヒント： すべてのプライベート パラメータ名が明らかにされるとは限りません（password と pin および field1 と field2 など）。 ライブ トランザクションを表示する前に、テスト トランザクションで HTTP パラメータを確認して、すべてのプライベート パラメータのセキュリティが保護されるようにすることをお勧めします。

パラメータをプライベートとして指定すると、その値は TIM ログおよび CEM コンソールにアスタリスクで表示されます。

ワイルドカード文字「*」を使用すると、一致のパターンを一般化できます。 以下のワイルドカード文字列を使用できます。

- abc* -- 前方一致
- * xyz -- 後方一致

- abc*xyz -- 前方および後方一致
- * -- アスタリスクのみのパラメータ名パターンを作成する場合は、すべてのパラメータがプライベートになります。

たとえば、「pin」をより一般化する場合は、その前にアスタリスクを追加することによって、「userpin」や「login_pin」などの他のエントリがプライベート パラメータとして認識されるようにすることができます。

注: 1 つのプライベート パラメータについて使用できる「*」ワイルドカード文字は 1 つだけです。 正規表現（regex）は使用できません。

CA CEM のデフォルト プライベート パラメータは以下のとおりです。

- *access_id
- pass
- *passcode
- pin
- *password
- pw
- *ssn

プライベート パラメータの変更

既存の CA CEM プライベート パラメータを更新するには、以下の手順に従います。

以下の手順に従います。

1. ［セキュリティ］ -［プライベート パラメータ］を選択します。
2. パラメータ名をクリックします（*password など）。アスタリスクは、password の語の前に任意の数の文字を表示できることを意味します。
3. パスワード コレクションに別のパラメータを入力します。 たとえば、HTTP トラフィック内での password の語の表示で、語の前に常に文字がない状態であることがわかっている場合は、*password パラメータを password に変更します。
4. ［保存］をクリックして、新しいプライベート パラメータ保存します。

プライベート パラメータの追加

新しい CA CEM プライベート パラメータを作成するには、以下の手順に従います。

以下の手順に従います。

1. ［セキュリティ］ - ［プライベート パラメータ］を選択します。
2. ［新規］をクリックして、新しいプライベート パラメータを作成します。
3. 必要なプライベート パラメータを入力します。
4. ［保存］をクリックして、新しいプライベート パラメータ保存します。

障害時の HTTP 要求および応答の保護

機密データの読み取り権限を持つ CA CEM ユーザとしてログインしているときに障害が発生した場合、ブラウザによって送信および生成された内容を正確に確認できます。また、権限があれば、Query および Post パラメータと、HTTP 要求および応答本文の情報を表示できます。

デフォルトでは、CEM システム管理者または CEM インシデント アナリスト グループに属する CA CEM ユーザは、機密データの読み取り権限を持ちます。

障害情報の表示

［障害詳細］ページには、ユーザ、トランザクション、Web サーバに関する情報など、障害に関するさまざまなカテゴリの情報が表示されます。障害についてキャプチャされた特定の HTTP パラメータ情報を表示する方法を以下に説明します。

以下の手順に従います。

1. ［インシデント管理］ - ［障害］を選択します。
2. 表示する障害の日付と時刻をクリックします。

   ［HTTP 情報］領域に、以下を含む、障害発生時にユーザが体験した具体的な内容に関する情報が表示されます。

   - ホスト、URL パス、TCP ポート
   - Cookie

- HTTP ヘッダ（Cookie 以外）

権限が与えられている場合は、この HTTP 情報を［障害詳細］ページで表示することもできます。

- Query および Post パラメータ
- 応答本文（先頭の 1,024 バイト）：この値を変更する方法については、「キャプチャされる応答本文の最大サイズの変更 (P. 169)」を参照してください。
- 要求本文（先頭の 1,024 バイト）：詳細については、「要求本文情報の表示について (P. 164)」を参照してください。

この HTTP 情報の表示の詳細については、「包括的な障害詳細をキャプチャ (P. 166)」を参照してください。

3. 障害発生時にユーザが表示していたのと同じページを表示するために、RequestHeader の［参照者］の内容をブラウザにカット アンド ペーストできます。

要求本文情報の表示について

要求本文情報を表示することは、障害を理解するうえで役立ちます。POST 要求には要求本文があります（空の場合もあります）。 GET 要求には要求本文がありません。

要求本文情報を表示するために知っておかなければならないことが 2 つあります。

- 整形式の XML/HTML だけが表示できます。整形式でない XML/HTML を表示する方法については、「非整形式の XML/HTML の表示 (P. 164)」を参照してください。
- デフォルトでは、障害について要求本文情報の先頭の 1,024 バイトを表示できます。 ただし、この値は変更できます。「表示される要求本文の最大サイズの変更 (P. 165)」を参照してください。

非整形式の XML/HTML の表示

障害に関連付けられた XML/HTML が整形式でない場合、HTTP 要求本文を表示するためのリンクをクリックすると、空のまたは不完全な要求が表示されます。

非整形式の XML/HTML を表示するための対応策はあります。

注: *任意*の要求本文情報（整形式であるとないとにかかわらず）を表示するには、［包括的な障害詳細をキャプチャ］チェック ボックスをオンにすると同時に、機密データの読み取り権限を持っている必要があります。詳細については、「包括的な障害詳細をキャプチャ (P. 166)」を参照してください。

以下の手順に従います。

1. ［インシデント管理］ -［障害］を選択します。
2. 表示する障害の日付と時刻をクリックします。
3. ［要求本文］リンクを右クリックし、ファイルを保存します。
4. テキスト エディタまたは HTML エディタを使用して、要求本文の全コンテンツを表示します。

表示される要求本文情報の最大サイズの変更

デフォルトでは、障害について要求本文情報の先頭の 1,024 バイトを表示できます。 権限が与えられている場合は、この値を編集して、表示する情報を増減できます。

以下の手順に従います。

1. TIM システム設定ページにアクセスします。
   a. CEM コンソールで、［設定］-［監視］を選択します。
   b. TIM の IP アドレスをクリックします（右端の列）。
   c. ユーザ名とパスワードを入力します。

   システム セットアップ ページのデフォルト ユーザ名は admin です。

   ［TIM System Setup］ページが表示されます。
2. ［Configure TIM Settings］をクリックします。

   ［TIM Settings］ページが表示されます。
3. ［MaxDefectRequestBodySize］をクリックします。
4. ［New value］フィールドに、表示する最大サイズ（バイト単位）を入力します。

   必要以上に大きな値を設定しないでください。大きな値を設定すると、TIM と Enterprise Manager の両方にとって処理に多くの時間がかかります。
5. ［Change］をクリックします。

   変更はすぐに適用されます。 TIM を再起動する必要はありません。
6. 複数の TIM がある場合は、各 TIM について上記の手順を繰り返します。

障害情報の表示の制限

以下 2 つの方法のいずれか（または両方）を使用して、表示される障害情報の量を制限できます。

- Query および Post パラメータ情報と、要求および応答本文の情報を収集して表示することの選択（「包括的な障害詳細をキャプチャ（P. 166）」を参照）

- 特定のプライベート パラメータの非表示への設定

  パラメータ名がプライベート パラメータのいずれかに一致する場合、Post、Query、Cookie、および URL パラメータは非表示になります（値が「***」に置き換えされます）。

  プライベート パラメータを使用すると、以下を非表示にすることができます。

  - 特定のパラメータ。正確なパラメータ名を入力します。
  - パラメータのタイプ。ワイルドカード（「*」）とパラメータ名のパターンを使用します。
  - すべてのパラメータ。パラメータ名のパターンに「*」を使用して新しいプライベート パラメータを作成します。つまり、すべてのパラメータがプライベートになります。

  詳細については、「プライベート パラメータの定義 (P. 160)」を参照してください。

包括的な障害詳細をキャプチャ

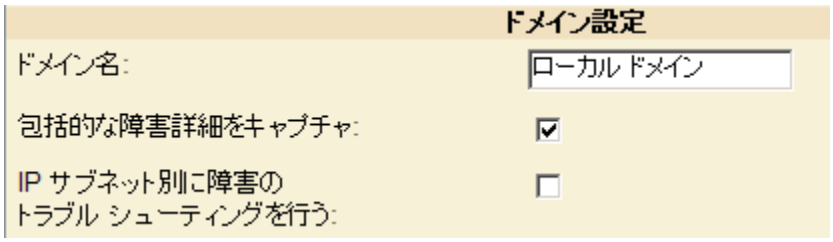
Query および Post パラメータと、要求および応答本文の情報を表示する機能は、デフォルトでは無効になっています。［包括的な障害詳細をキャプチャ］チェック ボックス（［設定］ -［ドメイン］ページ）をオンにしていない場合、TIM は Query および Post 情報と、要求および応答本文の情報をキャプチャしません。

重要: セキュリティ上の懸念がある場合は、このデフォルトを変更せず、［包括的な障害詳細をキャプチャ］チェック ボックスを CEM システム管理者すら使用できないようにすることを検討してください。 詳細については、「［包括的な障害詳細をキャプチャ］チェック ボックスの使用可能/使用不可能の切り替え (P. 168)」を参照してください。

ただし、機密データの読み取り権限を持つユーザが障害に関するこの追加情報を表示できるようにする場合は、［包括的な障害詳細をキャプチャ］チェック ボックスをオンにします。

Query、Post、要求本文、および応答本文の各情報の表示を可能にする方法

1. ［設定］ - ［ドメイン］を選択します。
2. ［包括的な障害詳細をキャプチャ］をオンにします。



［包括的な障害詳細をキャプチャ］チェック ボックスがページに表示されない場合は、［ドメイン］ - ［監視］ページに TIM が 1 つ以上表示されていることを確認してください （TIM を有効にする必要はありません）。

［包括的な障害詳細をキャプチャ］チェック ボックスを使用できない場合は、権限があれば、以下のいずれかの方法を使用して、CA EEM またはローカルの権限を更新します。

- CA EEM 内で CA CEM ユーザおよびアクセス ポリシーを設定している場合は、「［包括的な障害詳細をキャプチャ］チェック ボックスの使用可能/使用不可能の切り替え (P. 168)」を参照してください。
- ローカルによるセキュリティを使用している場合は、CEM システム管理者グループのメンバとしてログインします。

3. ［保存］をクリックします。
4. 監視を同期します。

注: ほかの CA CEM 構成を行っている場合は、監視の同期が一度だけで済むように、構成タスクをすべて完了してから同期を実行することをお勧めします。

監視を同期すると、障害に関する Query および Post 情報と、要求および応答本文の情報の収集が TIM によって開始されます。 その後、機密データの読み取り権限を持つユーザは、監視が同期された後にキャプチャされた障害のデータを表示できます。

後でこのチェック ボックスをオフにしても、オンになっていたときに収集された障害情報は表示できます。

[包括的な障害詳細をキャプチャ]チェック ボックスの使用可能/使用不可能の切り替え

デフォルトでは、CEM システム管理者グループに属するすべてのユーザが、［包括的な障害詳細をキャプチャ］チェック ボックスをオンにすることができます。 その理由は、CEM システム管理者グループのすべてのメンバがデフォルトで、システム構成設定 - 包括的な障害詳細をキャプチャ アクセス ポリシーを持っているからです。

［包括的な障害詳細をキャプチャ］チェック ボックスへのアクセス権を他のユーザに与えるには、そのユーザのグループをシステム構成設定 - 包括的な障害詳細をキャプチャのアクセス ポリシーに追加します。

注:［包括的な障害詳細をキャプチャ］チェック ボックスが［設定］-［ドメイン］ページに表示されるには、［ドメイン］-［監視］ページに TIM が 1 つ以上表示されている必要があります。

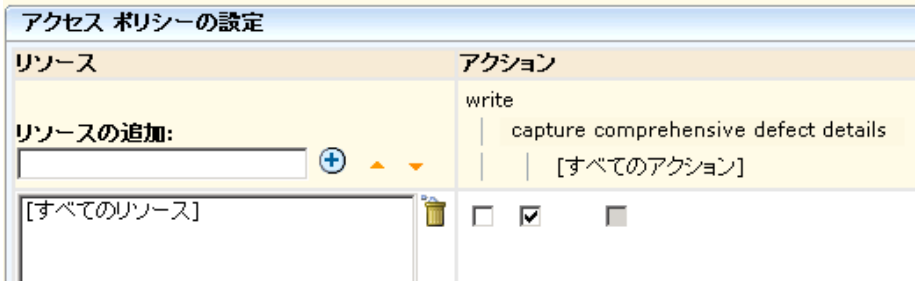
以下の手順に従います。

1. システム構成設定 - 包括的な障害詳細をキャプチャのアクセス ポリシーを編集するには、「CA EEM での CA CEM アクセス ポリシーの更新 (P. 155)」の手順に従います。

   ［選択された ID］に追加した管理ユーザまたはグループは、［包括的な障害詳細をキャプチャ］チェック ボックスを編集できるようになります。このチェック ボックスは、機密データの読み取り権限を持つすべてのユーザが、その他の HTTP 機密データ（Query および Post 情報と、要求および応答本文の情報）を表示することを許可します。

2. ユーザまたはグループがシステム構成設定リソース クラスへの書き込みアクセス権を持っていることを確認します（これによって、［ドメイン］ページを編集するユーザ権限が与えられます）。

3. ポリシーを保存する前に、[包括的な障害詳細をキャプチャ]アクションが選択されていることを確認します。



重要: [包括的な障害詳細をキャプチャ] チェック ボックスをオンにすると、CA CEM ユーザは機密性のあるデータを表示できるようになります。機密データの表示を厳しく制限する場合は、すべてのユーザだけでなく、デフォルトでアクセス権を持つ CEM システム管理者ですら、このチェック ボックスを使用できないようにすることができます。

[包括的な障害詳細をキャプチャ]チェック ボックスを使用不可能にする方法

1. CEM コンソールで、[設定] - [ドメイン] ページに移動し、[包括的な障害詳細をキャプチャ] チェック ボックスがオンになっていないことを確認します。
2. システム構成設定 - 包括的な障害詳細をキャプチャのアクセス ポリシーを編集するには、「CA EEM での CA CEM アクセス ポリシーの更新 (P. 155)」の手順に従います。
3. [包括的な障害詳細をキャプチャ] をオフにするか、[選択された ID] リスト内のすべてのエントリを削除し、包括的な障害詳細をキャプチャのアクセス ポリシーを保存します。

   [包括的な障害詳細をキャプチャ] アクションが選択されたポリシーがない場合、CA CEM ユーザは Query および Post 情報と、要求および応答本文の情報を TIM がキャプチャできるようにすることができません。

キャプチャされた応答本文の最大サイズの変更

デフォルトでは、応答本文の先頭の 10 KB をキャプチャできます。キャプチャする応答本文のサイズを増減するには、以下の手順に従います。

以下の手順に従います。

1. TIM システム設定ページにアクセスします。
   a. CEM コンソールで、[設定] - [監視] を選択します。

b. TIM の IP アドレスをクリックします（右端の列）。

c. ユーザ名とパスワードを入力します。

システム セットアップ ページのデフォルト ユーザ名は admin です。

［TIM System Setup］ページが表示されます。

2. ［Configure TIM Settings］をクリックします。

［TIM Settings］ページが表示されます。

3. ［MaxDefectResponseBodySize］をクリックします。

4. ［新しい値］フィールドに、キャプチャする最大サイズ（バイト単位）を入力します。

許可される範囲は 0 ～ 200,000 （200 KB）です。

必要以上に大きな値を設定しないでください。大きな値を設定すると、処理に時間がかかり、格納に必要な領域も増えます。

5. ［Change］をクリックします。

変更はすぐに適用されます。 TIM を再起動する必要はありません。

6. 複数の TIM がある場合は、各 TIM について上記の手順を繰り返します。

FIPS 140-2 準拠の暗号化

FIPS 140-2 について

連邦情報処理標準（FIPS） 140-2 の文書では、ソフトウェア製品とプロトコルの暗号化に使用される暗号のライブラリおよびアルゴリズムのセキュリティ標準を規定しています。

暗号化は、ソフトウェア セキュリティの以下の面に影響します。

- パスワードの格納および検証。
- 製品コンポーネント間および製品間で送信されるすべての機密データの通信および格納。

CA CEM と FIPS 140-2 について

FIPS 140-2 準拠のセキュリティを強化するため、CA CEM にはいくつかの変更が行われています。

- 電子メール サーバ用のパスワードは、FIPS 準拠の 128 ビット AES および SHA アルゴリズムを使用して暗号化されます。
- CA Unicenter Service Desk のパスワードは、FIPS 準拠の 128 ビット AES アルゴリズムを使用して暗号化されます。
- 障害およびユーザ セッション ID 内に含まれる HTTP 情報を、プレーンテキストの代わりに 128 ビット暗号化形式で APM データベースに格納できます。 この HTTP 情報は機密データである可能性があります。

  HTTP 情報には、ユーザ名、ユーザ セッション ID、パスワード、クレジット カード番号、Cookie などの機密データが含まれる場合があります。 ユーザ セッション ID は、ユーザ セッションのハイジャックに悪用される可能性があります。

CA CEM の FIPS 104-2 暗号化機能

以下の表に、APM データベース内で暗号化される（暗号化できる）データの種類をまとめます。 パスワードはデフォルトで暗号化されます。

アルゴリズムは、RSA Security Inc. の Crypto-J 3.5 ライブラリに含まれる、FIPS 認定の Pure Java バージョン（jsafeFIPS）です。

暗号化の対象	UI の場所	オプションかどうか？	暗号化のタイプ	詳細
SMTP パスワード	［システム］-［電子メール設定］	×	FIPS 準拠 AES	*CA APM 設定および管理ガイド*
障害に含まれる HTTP 情報（要求および応答の本文を含む）	［CEM］-［インシデント管理］-［障害］	○	FIPS 準拠 AES	障害に含まれる HTTP 情報の暗号化 (P. 172)
ユーザ セッション ID	ユーザ セッション ID が UI に表示されるのは、障害の包括的な詳細と一緒に表示される場合だけです。	○	FIPS 準拠 AES	ユーザ セッション ID の暗号化 (P. 173)

障害に含まれる HTTP 情報の暗号化

デフォルトでは、障害に関連付けられた HTTP 情報は、APM データベース内の障害メタ値のテーブルにプレーン テキストで格納されます。 FIPS 140-2 準拠ソフトウェアの使用が強制される場合は、以下の手順に従って、APM データベースに格納する HTTP 情報を暗号化してください。 キャプチャされた場合、障害と関連付けられた応答および要求の本文が暗号化されます。

この情報は、データを APM データベース内で暗号化する場合であっても、［CEM］ -［インシデント管理］ -［障害詳細］ページに表示するときは暗号化されません。

HTTP 情報		
ResponseHeader	Date:	Mon, 16 Jun 2009 21:12:39 GMT
ResponseHeader	Pragma:	no-cache
ResponseHeader	Server:	WebLogic WebLogic Server 7.0 SP1 Mon Sep 9 2002 206753
ResponseHeader	Content-Language:	en
ResponseHeader	Content-Length:	11191
ResponseHeader	Content-Type:	text/html; charset=ISO-8859-1
ResponseHeader	Expires:	Thu, 01 Jan 1970 00:00:00 GMT
Cookie	JSESSIONID_SAMPLEPORTAL:	lWXHgGLGMR6o96l011iAzdp290Z35D0GMyxsS 614758663

重要: 暗号化を選択または選択解除すると、HTTP 情報（APM データベース内の障害メタ値のテーブルに格納された）は、要求および応答の本文を含めてすべて削除されます。 これによって、同一のデータベース テーブルにプレーン テキスト形式のデータと暗号化されたデータが一緒に格納されることを回避します。

このテーブル内のデータは重要ではありません。 デフォルトでは、週単位で削除されます。

以下の手順に従います。

1. ［セキュリティ］ - ［FIPS 設定］を選択します。
2. ［HTTP 障害情報］をクリックします。

   暗号化を選択または選択解除すると、APM データベースに格納されたすべての HTTP 障害情報が削除されるという警告が表示されます。
3. ［保存］をクリックします。

   以前に格納された HTTP 情報は削除され、これ以降、障害の HTTP 情報は暗号化されます。

ユーザ セッション ID の暗号化

デフォルトでは、ユーザ セッション ID は APM データベースにプレーン テキスト形式で格納されます。 FIPS 140-2 に準拠するため、この情報は暗号化することもできます。

FIPS 140-2 準拠ソフトウェアの使用が強制される場合は、以下の手順に従って、APM データベースに格納するユーザ セッション ID を暗号化してください。

重要: 暗号化を選択または選択解除すると、ユーザ セッション ID （APM データベース内のユーザ セッション テーブルに格納されます）はすべて削除されます。これによって、同一のデータベース テーブルにプレーン テキスト形式のデータと暗号化されたデータが一緒に格納されることを回避します。

この削除が行われる理由は、FIPS 設定が変更されると、セッションを行っているすべてのユーザが未指定のユーザ グループに割り当てられるからです。 したがって、FIPS 設定の変更は、システム上のユーザ トラフィック量が最小のとき、またはアップグレード直後に Enterprise Manager を再起動するときに行うことをお勧めします。

以下の手順に従います。

1. ［セキュリティ］ - ［FIPS 設定］を選択します。
2. ［ユーザ セッション ID］をクリックします。

   暗号化を選択または選択解除すると、すべてのユーザ セッション ID が削除されるという警告が表示されます。
3. ［保存］をクリックします。

   以前に格納されたユーザ セッション ID は削除され、これ以降、ユーザ セッション ID は暗号化されます。

HTTPS を介した TIM 通信の構成

デフォルトでは、TIM と、TIM コレクション サービスを実行する Enterprise Manager とは、HTTP を介して通信します。 ただし、セキュリティを強化するため、SSL over HTTP （HTTPS）を使用して通信するように構成することもできます。

それには、TIM Collection サービスを実行する Enterprise Manager 上の *tess-customer.properties* ファイルに *timTessCommunication.useSsl* という名前のプロパティを追加します。

SSL を使用すると、Enterprise Manager と TIM 間の通信が遅くなる場合があるため、このことを考慮したうえで構成を適用します。 たとえば、Enterprise Manager と TIM が同じファイアウォール内に配置される一般的なシナリオでは、この構成を適用しないでください。

ただし、DMZ （ネットワーク非武装地帯）や、TIM データが WAN （ワイド エリア ネットワーク）上で送信されるセキュリティ保護されていない環境など、管理 VLAN の外部に TIM が配置されている場合は、この構成の適用を検討してください。

以下の手順に従います。

1. Enterprise Manager プロパティのデフォルト値を変更する場合は、「CA APM 設定および管理ガイド」の手順に従います。
2. *tess-customer.properties* ファイルを編集の目的で開き、以下の行を追加します。

   ```
   timTessCommunication.useSsl=1
   ```

   timTessCommunication.useSsl プロパティに 1 を設定すると、Enterprise Manager と TIM が HTTPS を介して通信するように構成されます。
3. Enterprise Manager を再起動します。

詳細については、「CA APM 設定および管理ガイド」を参照してください。

HTTPS のみによる Enterprise Manager アクセスの制限

デフォルトでは、HTTP 通信はブラウザと Enterprise Manager 間でのみ許可されます。 Enterprise Manager Web サーバを HTTPS 用に構成するときは、*<EM_Home>¥config* ディレクトリにある *IntroscopeEnterpriseManager.properties* ファイルの *introscope.enterprisemanager.webserver.jetty.configurationFile* プロパティを設定します。 詳細については、「CA APM 設定および管理ガイド」を参照してください。

CA APM Transaction Generator（CA APM TG）のセキュリティについて

CA CEM は、CA APM Transaction Generator （CA APM TG）によって実行された合成トランザクションを追跡および監視できます。 CA CEM 内の具体的な合成トランザクションを指定し、CA APM TG トランザクション用の個別のユーザ グループを作成することによって、それらの合成トランザクションを実際のトランザクションとは切り離して監視することもできます。

CA CEM 内で CA APM TG トランザクションを合成トランザクションとして識別できるので、実際のユーザに影響が及ぶ前に、Web サイトまたは Web アプリケーション内の問題にプロアクティブに対処できます。 CA APM TG を CA CEM 分析と組み合わせて使用すると、実際の Web アプリケーション ユーザが、シミュレートされたユーザに似たような問題を経験しているかどうかを判断できます。

CA APM TG を使用して合成トランザクションを生成する場合、CA APM TG 管理サーバに対するアクセス権を制御するアクセス ポリシーを設定できます。 CA APM TG 管理サーバで CEM コンソールと同じログイン クレデンシャルが使用されるように構成できるので、単一セットのクレデンシャルを管理できるようになります。 CEM コンソールと CA APM TG エージェントの構成においてユーザ名とパスワードの組み合わせを 1 つ覚えるだけなので、CA CEM ユーザにとってはメリットになります。

CA CEM に対してローカルによるセキュリティを使用していて、CEM システム管理者または CEM 構成管理者セキュリティ グループのいずれかでユーザが定義されている場合、そのユーザは CA APM TG 管理者の権限も持ちます。

CA CEM に対して CA EEM によるセキュリティを使用していて、システム管理者設定またはシステム構成設定のアクセス ポリシーのいずれかについて *書き込み*および*すべてのアクション*の権限がユーザに与えられている場合、そのユーザは CA APM TG 管理者の権限も持ちます。

注: CA EEM 内で*すべてのアクション*権限を設定するには、［すべてのアクション］チェック ボックスをオンにします。

詳細については、「*CA APM Transaction Generator 実装ガイド*」を参照してください。

第 5 章: CA CEM と nCipher の併用

Thales 社の nCipher ハードウェア セキュリティ モジュール（HSM）によって保護された Web サーバからのトラフィックを監視するには、CA CEM TIM に nCipher HSM をインストールする必要があります。

この章では、TIM に nCipher HSM をインストールして設定する方法について説明します。

CA CEM は、nCipher HSM によって保護されている Web サーバの SSL 秘密鍵の読み取りをサポートしています

ここでは、CA CEM を nCipher HSM と併用する際に必要な知識について説明します。

1. CA CEM における nCipher HSM のサポート方法について（P. 177）
2. TIM での nCipher の設定（P. 180）
3. 秘密鍵およびオペレータ用カード向けの実施可能な手順について（P. 192）
4. 秘密鍵またはオペレータ用カードが変更された場合の鍵およびカードの更新方法について（P. 198）
5. nCipher のインストールおよび構成に関するトラブルシューティング（P. 198）
6. （オプション）CA CEM における旧バージョンの nCipher のサポートについて

CA CEM と nCipher の併用

TIM で nCipher HSM を使用すると、SSL 秘密鍵による高度なセキュリティ保護が可能になります。これは、FIPS 境界内にあるキー ストレージに準拠して実行されます。HSM のセキュリティ境界である nCipher PCI シリーズは、FIPS 140-2 Level 2 と Level 3 および Common Criteria EAL4+ の認定を取得しています。 nCipher HSM を使用することで、TIM は保護された API を介して HTTPS 暗号化解除に必要な情報を要求することができます。

以下の TIM で nCipher HSM を使用できます。

- TIM ソフトウェア アプライアンス
- Multi-Port Monitor 上の TIM

  注: Multi-Port Monitor での TIM のデプロイについては、「*CA APM CA Infrastructure Management 統合ガイド*」を参照してください。

nCipher HSM は TIM ソフトウェアと直接連携するため、この章の説明は両方のデプロイに該当します。

環境

nCipher に対する CA CEM のサポートは、以下のハードウェア環境およびソフトウェア環境で保証されます。

ハードウェア

- CA CEM TIM アプライアンス
- nShield Solo PCI カード

ソフトウェア

- CA APM リリース 9.5
- nCipher Software Supplement （nCSS）バージョン 11.30

重要: nCipher がサポートするバージョンには、TIM および Web サーバの必須バージョンが含まれています。 以前のリリースを使用すると、予期しない結果が生じる可能性があります。

テスト

上記バージョンの CA CEM と nCipher は、Sun OS 5.10 上の Sun Java System Web Server 7.0 でテスト済みです。

nCipher がサポートする環境については、nCipher のドキュメントを参照してください。 CA CEM 構成に関して不明点がある場合は、CA サポートにお問い合わせください。

前提条件

この機能を使用するには、以下の点が満たされている必要があります。

- SSL 秘密鍵が nCipher Security World によって保護されている Web サーバが 1 つ以上ある。 すべての Web サーバ秘密鍵が同一の Security World によって保護されている必要があります。
- TIM と Web サーバの nCipher のバージョンが同じである。
- Web サーバにアクセスできる。Web サーバの以下のものにアクセス可能である必要があります。
  - Security World
  - Administrator Card Set
  - Operator Card Set
  - Pass phrase
- TIM マシンにアクセスし、以下を実行できる。
  - TIM マシンに Thales-nCipher ハードウェア セキュリティ モジュール（HSM）をインストールする。
  - nCipher 製品のドキュメントに従って、TIM 上にカーネル ドライバを構築する。
  - nCipher Software Supplement を TIM にインストールし、HSM にアクセスするよう構成する。
  - nCipher Software Supplement （nCSS） 11.30 を使用する。 機能の中には以前のソフトウェア リリースと同じものもありますが、このドキュメントにおける nCipher ドキュメントの参照は「*nShield User Guide for Unix-based OS version 6.3*」を対象としています。
- CA CEM、TIM マシン、および CA CEM ドキュメントをよく理解している。
- Thales-nCipher 製品ドキュメント、特に TIM マシンおよび Web サーバ内の HSM 用ユーザ ガイドをよく理解している。

nCipher をサポートするための CA CEM の設定

以降のセクションでは、nCipher ハードウェア セキュリティ モジュール（HSM）によって保護された SSL 秘密鍵を読み取るように TIM を設定する方法について説明します。

以下は、TIM を nCipher HSM と連携させるために必要な一連の手順です。

1. TIM 内への nCipher ハードウェアのインストール（P. 180）
2. TIM への nCipher ソフトウェアのインストール（P. 181）
3. カーネル ドライバの構築（P. 182）
4. TIM 上の nCipher インストールの確認（P. 182）
5. nCipher Security World への TIM HSM の登録（P. 184）
6. CA CEM への Web サーバの nCipher 秘密鍵のアップロード（P. 187）
7. TIM での nCipher HSM の構成（P. 188）
8. nCipher で保護された Web トラフィックの確認（P. 192）

これらの手順をすべて完了すると、TIM と nCipher HSM を併用した HTTPS トラフィックの監視を始めることができます。

TIM 内への nCipher ハードウェアのインストール

以下は、TIM の*内部*に nCipher ハードウェアをインストールするための基本的な手順です。 詳細な手順については、nCipher のドキュメントを参照してください。

注: TIM マシンが複数あり、nCipher を搭載しないマシンもある場合は、nCipher を搭載した TIM マシンに対して nCipher で保護された Web サーバを監視するための構成を行う必要があります。 これによって、負荷分散の効率が向上します。

以下の手順に従います。

1. nShield HSM ハードウェア（PCI カードおよびカード リーダ）を用意します。
2. お使いのハードウェアと環境に適した nCipher ドキュメントを用意します。

3. TIM マシンに付属するハードウェア ドキュメントを用意します。
4. nCipher ドキュメントの説明に従って、TIM マシンにハードウェアをインストールします。 必要に応じて、TIM マシンのハードウェア ドキュメントを参照してください。
5. 接続部がコネクタに完全に差し込まれていることを確認します。
6. バック パネルがシャーシ内のアクセス スロットに正しく接続されていることを確認します。
7. 次の手順「TIM への nCipher ソフトウェアのインストール (P. 181)」に進みます。

TIM への nCipher ソフトウェアのインストール

以下は、TIM *上に* nCipher ソフトウェアをインストールするための基本的な手順です。 詳細については、nCipher のドキュメントを参照してください。

以下の手順に従います。

1. お使いのハードウェアと環境に適した nCipher ソフトウェアを用意します。
2. お使いのソフトウェアと環境に適した nCipher ドキュメントを用意します。

   nCipher ドキュメントの説明に従って、TIM サーバに nCipher ソフトウェアをコピーしてインストールします。 具体的には、nCipher CD に含まれる nShield_Quick_Start_Guide および version.txt ファイルを参照してください。 version.txt ドキュメントにはすべてのパッケージ名が記載されています。

   注: TIM の開始後に nCipher ソフトウェアがインストールされた場合は、nCipher ハードウェアとの接続を確立するために TIM を再起動します。

3. ［TIM System Setup］ページに、以下の nCipher メニュー オプションが表示されることを確認します。
   - View nCipher status
   - Configure nCipher

   これらのメニュー オプションは、nCipher ソフトウェアのインストール完了後に表示されます。
4. 次の手順「カーネル ドライバの構築 (P. 182)」に進みます。

カーネル ドライバの構築

TIM と nShield HSM を併用するには、カーネル ドライバを構築します。nCipher では、ロード可能なモジュールとしてドライバを構築できるように、nCipher PCI カーネル ドライバ（*nfp*）と *makefile* のソースが提供されています。

必要な開発ツール（Red Hat ディストリビューションに含まれる RPM）をダウンロードします。

また、TIM マシンに nCipher ソフトウェアをインストールして構成する際に、関連する実装ドキュメント（お使いのソフトウェアに適したバージョンの本ドキュメントと、Thales nCipher のドキュメント）が必要です。

以下の手順に従います。

重要: TIM 上の Red Hat のバージョンに一致する RPM をダウンロードします。

1. Thales からドキュメント「*nShield User Guide for Unix-based OS*」および「*nShield Quick Start Guide for Unix-based OS*」を入手します。
2. nCipher ドキュメントに従って、カーネル ドライバを構築します。
3. 次の手順「TIM 上の nCipher インストールの確認 (P. 182)」に進みます。

TIM 上の nCipher インストールの確認

nCipher ハードウェアおよびソフトウェアのインストールが完了したら、［TIM nCipher Status］ページを使用して、新しいハードウェアおよびソフトウェアを確認できます。

ソフトウェアの確認

nCipher ソフトウェアが TIM 上で使用可能であることを確認します。

以下の手順に従います。

1. ［TIM System Setup］ - ［View nCipher Status］ページに移動します。
2. ページ上の出力を確認します。 */opt/nfast/bin/enquiry* の出力の最初の部分は、以下のように表示されます。

```
Server:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        ...
 mode                 operational
```

3. 出力に「operational」と表示されない場合は、nCipher ドキュメントを参照してください。

ハードウェアの確認

nCipher ハードウェアが TIM 上で使用可能であることを確認します。

以下の手順に従います。

1. ［TIM System Setup］ - ［View nCipher Status］ページに移動します。
2. ページ上の出力を確認します。 */opt/nfast/bin/enquiry* の出力に Module セクションが少なくとも 1 つ含まれていることを確認します。この場合、以下のように表示されます。

```
Module #1:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        ...
 mode                 operational
```

3. 出力に「operational」と表示されない場合は、nCipher ドキュメントを参照してください。
4. 次の手順「nCipher Security World への TIM HSM の登録 (P. 184)」に進みます。

nCipher Security World への TIM HSM の登録

TIM マシンにインストールされた HSM が Web サーバ秘密鍵にアクセスできるようにするためには、Web サーバの鍵を保護する Security World 環境に HSM を登録する必要があります。 nCipher Security World フレームワークは以下で構成されます。

- ハードウェア セキュリティ モジュール（HSM）- PCI ハードウェア カード
- Administrator Card Set （ACS） - 管理および構成用アクセスを制御するスマート カード
- Operator Card Set （OCS） - アクセスを制御するスマート カード
- SSL 秘密鍵と証明書データ

nCipher Security World の概念の詳細については、「*nShield User Guide for Unix-based OS*」を参照してください。

重要: 登録を開始する前に、Web サーバおよび TIM の両方で nCipher ソフトウェアの最低限のバージョンが実行されていることを確認してください。 「ソフトウェア (P. 178)」を参照してください。

登録プロセスでは、以下が必要になります。

- TIM マシンとその nCipher HSM への物理的なアクセス
- TIM マシン上での、root としての、または *nfast* グループのメンバであるユーザとしてのコマンド ライン セッションの開始
- Security World 用の Administrator Card Set （ACS）のクォーラム
- すべての Operator Card Set にそれぞれ 1 つずつのパス フレーズ

重要: 開始する前に、Web サーバの */opt/nfast/kmdata/local* ディレクトリ（Windows の場合は *%NFAST_KMDATA%¥local*）のバックアップ コピーを、内容もすべて含めて作成してください。 バックアップは安全な場所に保存してください。

Web サーバから TIM への Security World のコピー

登録プロセスを開始するには、TIM に Web サーバの Security World をコピーする必要があります。

以下の手順に従います。

1. Web サーバの */opt/nfast/kmdata/local* ディレクトリ（Windows の場合は *%NFAST_KMDATA%¥local*）を、内容もすべて含めてコピーします。
2. */opt/nfast/kmdata/local* ディレクトリのコピーを、すべての内容が含まれた状態で TIM マシンに配置します。
3. この TIM 上の新しいディレクトリ内に、Security World の各スマートカードセットの 'world' ファイル、'cards_*' ファイル、および 'card_*' ファイルが、また Security World によって保護される各鍵の 'key_*' ファイルが含まれていることを確認します。

Security World への TIM の登録

Security World に TIM を登録するには、TIM マシン上でのコマンド ライン セッションが必要です。

以下の手順に従います。

1. nCipher HSM 背面のスイッチを「I」の位置に移動させます。
2. コマンド ラインで以下を実行します。

   /opt/nfast/bin/nopclearfail -ca

   -ca オプションを指定することで、*nopclearfail* コマンドによって利用可能なすべての nCipher モジュールが初期化されます。
3. 次の手順に進む前に ACS カードの正確な数とそれぞれのパス フレーズをメモしておいてください。

4. コマンド ラインで以下を実行します。

   /opt/nfast/bin/new-world -l

   new-world ユーティリティにより、ACS カードを挿入して、そのパス フレーズを入力するよう求める指示が、クォーラムに到達するまで表示されます（*-l* オプションは、既存の Security World にモジュールを追加することを示します）。

   new-world が完了するまでカードの処理を繰り返します。

   new-world ユーティリティの詳細については、nCipher ドキュメントを参照してください。

5. nCipher HSM 背面のスイッチを「O」の位置に移動させます。
6. コマンド ラインで以下を実行します。

   /opt/nfast/bin/nopclearfail -ca

   以上の手順が完了したら、この Security World で保護されたすべての秘密鍵が HSM で使用できるようになります。 TIM HSM が Security World に登録され、Web サーバ秘密鍵にアクセスできます。

登録の確認

Security World と TIM HSM が使用可能であり、Web サーバ秘密鍵にアクセスできることを確認する必要があります。

以下の手順に従います。

1. ［TIM System Setup］ - ［View nCipher Status］ページに移動します。
2. ［TIM System Setup］ - ［View nCipher Status］ページ上の出力を確認します。 */opt/nfast/bin/enquiry* の出力の最初の部分に、operational モードであることが以下のように表示されます。

```
Server:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        ...
 mode                 operational
```

3. 出力に「operational」と表示されない場合は、nCipher ドキュメントを参照してください。

4. ［TIM System Setup］ - ［View nCipher Status］ページ上の出力を確認します。 */opt/nfast/bin/nfkminfo* の出力内の Security World とモジュールの両方に「Usable」（単語の前に感嘆符なし）と表示されていることを確認します。

```
World
 generation  2
 state       0x7270000 Initialised Usable Recovery !PINRecovery !ExistingClient
RTC NVRAM !FTO SEEDebug
 n_modules   1
。
。
。
Module #1
 generation 2
 state       0x2 Usable
 flags       0x10000 ShareTarget
 n_slots     2
```

5. 出力に「Usable」と表示されない場合は、nCipher ドキュメントを参照してください。

6. */opt/nfast/bin/preload ... pause* を発行することで、保護されているすべての鍵を HSM にロードできます。「...」の部分は保護されている特定の鍵を指定するためのオプションに置き換えます（詳細については、「*preload -help*」を参照してください）。

   注: 鍵を保護する OCS によって、NotPersistent オプションが使用される場合があります。この場合、カードがスロット内に残っている限り、アプリケーションはプリロードされた鍵を使用できます。 しかし、カードが取り外されると、ロードされた鍵は無効になり、アプリケーションがプリロードされた鍵を使用しようとすると、暗号化オペレーションで失敗します。 鍵を再ロードするには、アプリケーションとプリロード プロセスを再度実行する必要があります。

7. 「CA CEM への Web サーバの nCipher 秘密鍵のアップロード (P. 187)」に進みます。

CA CEM への Web サーバの nCipher 秘密鍵のアップロード

TIM では、アプリケーション タイプが *embed* の秘密鍵のみを受け入れます。 Web サーバが Apache 以外の場合は、アップロードする前に鍵を再ターゲットする必要があります。

秘密鍵の保護は、HSM 単独でも、OCS を使用しても可能です。 OCS 自体はパス フレーズで保護できます。

nCipher Operator Card Set は複数のカードを含むことができます（また、それらのカードがすべて必要であるかもしれません）。ただし、TIM でサポートされるカードは 1 つだけです（これは、プロセスが TIM 内部で自動化されるためです）。 Web サーバが複数のカードを使用している場合は、TIM 用にそれらを統合する必要があります。

CA CEM に秘密鍵をアップロードする方法

1. Web サーバの秘密鍵のアプリケーション タイプが *embed* でない場合は、秘密鍵を再ターゲットする必要があります。「Web サーバ秘密鍵の再ターゲット (P. 193)」を参照してください。
2. ファイル */tmp/webserver1.pem* を CA CEM にアップロードします。「CA APM 設定および管理ガイド」の「CA CEM でのセキュア Web アプリケーションの監視」の章を参照してください。
3. 既存の Operator Card Set が TIM カードを収容するのに大きさが足りない場合は、新しいセットを作成できます。「新しい Operator Card Set の作成 (P. 195)」を参照してください。
4. TIM で複数の秘密鍵を使用する必要がある場合は、同一の Operator Card Set で保護することをお勧めします。詳細については、「Operator Card Set の統合 (P. 196)」を参照してください。

秘密鍵のアップロードを確認する方法

1. ［TIM System Setup］ - ［View TIM SSL Server Status］ページに移動します。
2. Web サーバの IP アドレスとポート番号を確認します。
3. 次の手順「TIM での nCipher HSM の構成 (P. 188)」に進みます。

TIM での nCipher HSM の構成

nCipher HSM およびオプションの OCS と連携するよう TIM を構成する準備はすでに整っています。

TIM の構成

以下の手順に従います。

1. ［TIM System Setup］ - ［Configure nCipher］ページに移動します。
2. TIM で nCipher サポートを有効にする必要がある場合は、［Enable nCipher HSM］をクリックします。

   次回 TIM を再起動したときに有効になります。
3. TIM で nCipher サポートを無効にする必要がある場合は、［Disable nCipher HSM］をクリックします。

   次回 TIM を再起動したときに無効になります。
4. TIM の再起動時に常に nCipher HSM サポートを利用可能にする場合は、Operator Card Set 名を入力して、［Save］をクリックする必要があります。

   詳細については、「自動オペレーションについて (P. 191)」を参照してください。
5. オペレータ用カードにパス フレーズが設定されている場合は、保存しておくか、TIM の再起動時に常に入力するかを選択できます。

   a. 保存しておくオペレータ用カードのパス フレーズを入力して、［Save］をクリックします。

      パス フレーズは暗号化されて保存され、TIM Web ページを使用して読み取ることはできなくなります。 オペレータ用カードにパス フレーズが設定されている場合は、これを自動オペレーションとして使用できます。 詳細については、「自動オペレーションについて (P. 191)」を参照してください。

   または

   b. オペレータ用カードのパス フレーズを入力し、［Start TIM with this pass phrase］をクリックします。

      パス フレーズは保存されません。
6. 保存されているパス フレーズを消去する必要がある場合は、［Erase the stored pass phrase］をクリックします。

TIM の再起動と構成の確認

nCipher を有効化または無効化する場合、およびパス フレーズを保存した後は、TIM を再起動する必要があります。

以下の手順に従います。

1. ［Return to TIM Setup］をクリックします。
2. ［Start or Stop TIM］をクリックします。
3. ［Start (or restart) TIM］をクリックします。
4. 構成の変更内容を確認します。

   ページ上にステータスが、以下のように表示されます。

```
TIM Control
Stopping old nCipher preload process
Using nCipher HSM
Running background nCipher preload
Operator card set "testocs1" specified
preload log:
-------------------------------------------
Loading cardsets:
testocs1 on modules 1
Checking modules and reading cards ...
Checking modules and reading cards ...
Loading `testocs1':
Module 1 slot 0: `testocs1' #3
Module 1 slot 0: Enter passphrase: (reading cards)
Module 1 slot 0: Enter passphrase:
********
Module 1 slot 0:- passphrase supplied - reading card
Module #1 Slot #0: Processing ...
Card reading complete.
Stored Cardset: testocs1 (1ff8...) on module #1
Stored Unsure -- multiple objects on module #1
Loaded embed aee3ef6fefb153f743843a284954828c09328500 key (RSAPrivate) on
modules 1
-------------------------------------------
The action you requested may take several seconds to complete.
```

   注: 同じ nCipher ログ情報が、*/etc/wily/cem/tim/logs/ncipher/preload-log.txt* 内にもあります。

5. カードセット名が正しいことを確認します。

6. 以下の行を探します。

```
Card reading complete.
Loaded embed < key > (RSAPrivate) on modules < n >
```

7. 次の手順「nCipher で保護された Web トラフィックの確認 (P. 192)」に進みます。

自動オペレーションについて

通常、システムが起動すると、TIM は自動的に開始されます。 TIM を HSM と連携させるには、以下の手順に従います。

- TIM マシン用に使用する Operator Card Set ではクォーラムを 1 に設定する必要があります。 これは、Web サーバ マシン用の Operator Card Set とは関係ありません。
- TIM マシン用のオペレータ用カードにはパス フレーズを設定しないでおくか、［TIM System Setup］-［Configure nCipher］ページを使用して、パス フレーズを保存または入力する必要があります。 オペレータ用カードからパス フレーズを削除する方法の詳細については、「オペレータ用カードからのパス フレーズの削除 (P. 195)」を参照してください。
- オペレータ用カードは、TIM マシンの HSM に接続されたカード リーダ内に残しておく必要があります。
- Operator Card Set 名を保存するには、［TIM System Setup］-［Configure nCipher］ページを使用する必要があります。

重要: オペレータ用カードのパス フレーズが、保存されているパス フレーズと一致しない場合、またはカード リーダ内に不正なカードがある（またはカードがない）場合、TIM は自動的に開始されません（これは TIM ログには記録されませんが、*/etc/wily/cem/tim/logs/ncipher/preload1-log.txt* および *preload2-log.txt* ファイルに記録されます）。この場合、nCipher 構成ページを使用して、すぐに TIM を開始するか、必要な情報を保存してから［TIM System Setup］-［Start or Stop TIM］ページを使用して TIM を開始できます。

nCipher で保護された Web トラフィックの確認

nCipher を併用する際の CA CEM の機能を確認します。 Web トラフィックを確認することで実施できます。

TIM トランザクション検査を使用して、SSL 機能を確認する方法

注: 「CA APM 設定および管理ガイド」の「CA CEM でのセキュア Web アプリケーションの監視」の章を参照してください。*SSL に対応した CA CEM の機能の確認*に関する情報を参照してください。

TIM SSL サーバのステータスを使用して、SSL 機能を確認する方法

1. ［TIM System Setup］ - ［View TIM SSL Server Status］ページに移動します。
2. nCipher サーバへの接続が表示され、デコードの失敗がない場合、TIM は nCipher を使用して Web サーバ トラフィックを監視できます。

TIM 追跡を使用して SSL 機能を確認する方法

1. ［TIM System Setup］ - ［Configure TIM Trace Options］ページに移動します。
2. 追跡 HTTP コンポーネント オプションの有効化を選択します。
3. 暗号化されたサーバへのコンポーネントが TIM ログに表示され、そのサーバが nCipher を使用していれば、暗号化解除は機能しています。

nCipher 鍵とオペレータ用カードの使用

このセクションでは、TIM で使用するための Web サーバ秘密鍵の準備方法について説明します。ここで説明するタレス nCipher ユーティリティ オペレーションは、Web サーバ上で実行する必要があります。

重要: 開始する前に、*/opt/nfast/kmdata/local* （Windows の場合は *%NFAST_KMDATA%¥local*）のバックアップ コピーを作成してください。これは TIM マシンと Web サーバの両方にとって重要です。

このセクションには、以下のトピックが含まれます。

Web サーバ秘密鍵の再ターゲット

注: このセクションは、Web サーバ用の秘密鍵がすでに nCipher によって生成されていると仮定します。

nCipher Security World によって、PKCS#11、Java JCE、OpenSSL、Microsoft CAPI（Windows 上）、nCipher のネイティブ API といったさまざまなアプリケーション プログラミング インターフェース（API）で鍵を利用できるようになります。 鍵の生成時に指定したアプリケーション タイプに応じて、さまざまな情報が実際に暗号化されたキー マテリアルに保存されるため、その API からのアクセスが容易になります。

既存の鍵をほかのアプリケーションが利用できるようにすることができます。 この処理を「再ターゲット」と呼びます。 再ターゲット オペレーションによって、新しい鍵 BLOB がファイル システムに保存されます。この鍵 BLOB には、新しいアプリケーション タイプと同じ暗号化されたキー マテリアルおよび新しいアクセス情報が含まれます。

以下は、各種の Web サーバ ソフトウェア パッケージで使用される API の限定的なリストです。

サーバ	プラットフォーム	API	アプリケーション
Apache	すべて	OpenSSL	embed
Sun ONE	すべて	PKCS#11	pkcs11
MS IIS	Windows	MS CAPI	mscapi
Tomcat	すべて（Java）	JCE	jce

TIM マシンでは、アプリケーション タイプが *embed* の鍵が必要です。embed 鍵には、*/opt/nfast/kmdata/local* ディレクトリ内の暗号化された鍵 BLOB に加えて、*embedsavefile* というファイルが付随しています。このファイルによって、使用する特定の鍵 BLOB が OpenSSL に対して指定されます。

Sun ONE Web Server 鍵のアプリケーション タイプを pkcs11 から embed に変換する方法

- アプリケーション タイプが *pkcs11* の鍵を *embed* タイプに再ターゲットするには、以下の例を参照してください。

  この例では、対象の鍵を保護しているのは *MyOCS* という 1/N オペレータ用カードで、HSM カード リーダ内にあると仮定します。 デフォルト値をそのまま使用する場合は、Enter キーまたは Return キーを押します。

```
$ /opt/nfast/bin/generatekey --retarget embed
from-application: Source application? (custom, embed, hwcrhk, pkcs11, simple)
  [default custom] > pkcs11
from-ident: Source key identifier?
(uc66d0f2df3103e32c5703e8de0cfb172a1b35cf82-9051fc31c13c7716a1ac140fdea2eded04c0f
419)
[default
uc66d0f2df3103e32c5703e8de0cfb172a1b35cf82-9051fc31c13c7716a1ac140fdea2eded04c0f4
19]
>
embedsavefile: Filename to write key to? []
> /tmp/webserver1.pem
plainname: Key name? [] > webserver1
key generation parameters:
 operation         Operation to perform      retarget
 application       Application               embed
 slot              Slot to read cards from   0
 verify            Verify security of key    yes
 from-application  Source application        pkcs11
 from-ident        Source key identifier
uc66d0f2df3103e32c5703e8de0cfb172a1b35cf82-9051fc31c13c7716a1ac140fdea2eded04c0f4
19
 embedsavefile     Filename to write key to  /tmp/webserver1.pem
 plainname         Key name                  webserver1

Loading `MyOCS':
 Module 1: 0 cards of 1 read
 Module 1 slot 0: `MyOCS' #1
 Module 1 slot 0:- passphrase supplied - reading card
Card reading complete.
```

```
Key successfully retargetted.
Path to key:
/opt/nfast/kmdata/local/key_embed_b4c36e18ff38d2d45a2df425abd9febfaf873da4
```

オペレータ用カードからのパス フレーズの削除

OCS で保護されている鍵で自動的に TIM を実行するには、1 つの方法として、TIM カード リーダ内にある OCS カードからパス フレーズを削除します。

以下の手順に従います。

- *cardpp* を使用します。

```
$ /opt/nfast/bin/cardpp --change -m 1

Checking/changing passphrase(s):
 Module 1 slot 0: `MyOCS' #1
 Module 1 slot 0: Enter passphrase:                                [^D: done]
 Module 1 slot 0:- passphrase supplied - reading card
 Module 1 slot 0: Enter new passphrase: <return>                   [^D: done]
 Module 1 slot 0:- no passphrase specified - removing passphrase
 Module #1 Slot #0: Processing ...                                 [^D: done]
 Module 1 slot 0: `MyOCS' #1: Passphrase removed
Insert/change card in module (or change module mode)               [^D: done]
<Control-D>

Done.
```

注: TIM はパス フレーズが設定されていない OCS カードで実行できますが、Web サーバ ソフトウェアではサポートされていない場合があります。

新しい Operator Card Set の作成

既存の Operator Card Set （OCS）が TIM を収容するのに大きさが足りない場合は、新しいセットを作成できます。

たとえば、既存の Web サーバにカード セットが 1 つしかない場合は、TIM マシンのカードを収容するために新しいセット（少なくとも 2 つのカードで構成される）を作成する必要があります。

注: この操作は、TIM マシン上で、*/opt/nfast/kmdata/local* のローカル コピーを使用して、再ターゲットされた鍵で実行してください。

以下の手順に従います。

- *createocs* を使用します。

  ```
  /opt/nfast/bin/createocs -Q 1/n -N name
  ```

  n はカードセットのサイズで、*name* はカードセットに設定する名前です。

新しい Operator Card Set が作成されたら、「Operator Card Set の統合 (P. 196)」の説明に従って、鍵を回復できます。

Operator Card Set の統合

TIM で複数の鍵が使用される場合、同じ Operator Card Set （OCS）で保護すれば効果的になることがあります。 複数の鍵が異なる OCS で保護されており、かつ、これらの鍵が同じ Security World に含まれており、かつ、これらの鍵でリカバリが有効になっている場合は、同じ OCS にこれらの鍵をすべて回復することで、鍵をロードして、単一の OCS からアクセス可能にすることができます。

以下の手順に従います。

注: このオペレーションでは、許可のために Administrator Card Set （ACS）のクォーラムへのアクセス権が必要です。

重要: 稼働中の Web サーバ鍵に対して *rocs* オペレーションを実行しないでください。 TIM マシン上にコピーを作成し、そのコピーで実行してください。

注: 鍵を再ターゲットする必要がある場合は、OCS を操作する前にこれを実行してください。 詳細については、「Web サーバ秘密鍵の再ターゲット (P. 193)」を参照してください。

1. 鍵のリカバリが有効化されているかどうかを確認するには、*nfkminfo* を使用します。

   ```
   $ /opt/nfast/bin/nfkminfo -k embed
   Key listing AppName embed (1 keys):
    AppName embed                Ident 5dce27b0a84b517b0db7b5aa2f09452e27a13d38
   $ /opt/nfast/bin/nfkminfo -k embed 5dce27b0a84b517b0db7b5aa2f09452e27a13d38
   ```

```
Key AppName embed Ident 5dce27b0a84b517b0db7b5aa2f09452e27a13d38
 BlobKA length          1052
 BlobPubKA length       444
 BlobRecoveryKA length 1208
 name                   "MyKey"
 hash                   d96ee8282cc7f76ea32df1ce299ab087a206e530
 recovery               Enabled
...
```

2. 最初の呼び出しから 2 つ目の呼び出しに識別子をコピーします。*recovery Enabled* の行は、鍵を新しい OCS に回復できることを示しています。

```
$ /opt/nfast/bin/rocs -i
`rocs' key recovery tool
Useful commands: `help', `help intro', `quit'.
rocs> list cardsets
No. Name                    Keys (recov) Sharing
  1 iWorld1of1              0 (0)        1 of 1; persistent
  2 NonPersistentOCS        9 (9)        1 of 1
rocs> target 1
rocs> list keys
  No. Name                    App        Protected by
    1 MyKey                   caping     module
    2 MyKey                   caping     module
    3 MyKey                   embed      module
    4 Example label           pkcs11     NonPersistentOCS
    ...
rocs> mark 4
rocs> recover

Authorising OCS replacement:
 Module 1: 0 cards of 1 read
 Module 1 slot 0: empty
 Module 1 slot 0: Admin Card #1
... prompt for the ACS passphrase ...
 Module 1 slot 0:- passphrase supplied - reading card
Card reading complete.


Loading `iWorld1of1':
 Module 1: 0 cards of 1 read
 Module 1 slot 0: Admin Card #1
 Module 1 slot 0: empty
 Module 1 slot 0: `iWorld1of1' #1
... prompt for the OCS passphrase ...
```

```
 Module 1 slot 0:- passphrase supplied - reading card
Card reading complete.

rocs> save 4
rocs> quit
```

秘密鍵とオペレータ用カードの更新

Web サーバで鍵管理データが更新された場合（新しい鍵やカード セットが作成されたときなど）、鍵管理データ ファイルの TIM コピーも更新する必要があります。

TIM HSM 用に新しい鍵またはカード セットを用意したときは、この手順に従ってください。

以下の手順に従います。

1. nCipher Security World への TIM HSM の登録（P. 184）
2. CA CEM への Web サーバの nCipher 秘密鍵のアップロード（P. 187）
3. TIM での nCipher HSM の構成（P. 188）
4. nCipher で保護された Web トラフィックの確認（P. 192）

CA CEM と nCipher の併用に関するトラブルシューティング

CA CEM にインストールした nCipher に関するトラブルシューティングが必要になる場合があります。

症状:

nCipher カードをインストールした後、TIM が開始しない。または、TIM にインストールした nCipher が動作しない。

解決方法:

1. ［TIM System Setup］ - ［View nCipher Status］ページを確認します。
2. 「TIM 上の nCipher インストールの確認（P. 182）」を参照してください。

症状:

nCipher HSM が予想したとおりに機能しない。

解決方法:

1. カードがスロットに挿入されるごとに、挿入数が増加します。 このため、カードが正しく挿入されず、再度挿入した場合も、それが挿入数に反映されます。
2. ［TIM System Setup］ - ［View TIM SSL Server Status］ページを確認します。 「nCipher で保護された Web トラフィックの確認 (P. 192)」を参照してください。
3. */etc/wily/cem/tim/logs/ncipher/preload-log.txt* の nCipher ログ情報を確認します。 「TIM の再起動と構成の確認 (P. 190)」を参照してください。
4. TIM ログを確認します。
5. 鍵を再ターゲットすると（generatekey）、「ERROR: Module #1: LoadBlob (loading private blob) failed: Malformed」というメッセージが表示される場合があります。 nCipher ソフトウェアのバージョンに不一致がある場合に、このエラーが発生することがあります。 Web サーバを TIM 上の nCipher のバージョンと一致するものに更新するか 、Thales 社のテクニカル サポートにお問い合わせください。
6. オペレータ用カードのパス フレーズが、保存されているパス フレーズと一致しない場合、またはカード リーダ内に不正なカードがある（またはカードがない）場合、TIM は自動的に開始されません（これは TIM ログには記録されませんが、*/etc/wily/cem/tim/logs/ncipher/preload1-log.txt* および *preload2-log.txt* ファイルに記録されます）。この場合、nCipher 構成ページを使用して、すぐに TIM を開始するか、必要な情報を保存してから［TIM System Setup］-［Start or Stop TIM］ページを使用して TIM を開始できます。
7. TIM スタートアップ ログを確認します。
8. Web サーバからの OCS およびオペレータ用カードがありますか。これらがないと、TIM が開始しない場合があります。
9. Web サーバから TIM への Security World 環境のバイナリ コピーを実行しましたか。 していないと、再ターゲット時に BLOB の書式エラーの原因になります。
10. new-world を実行する際に kmdata があることを確認します。

11. new-world を実行する前に ACS の数とそれらのパス フレーズを把握しておきます。
12. TIM HSM が「I」の位置に設定され、ジャンパが「OFF」に設定されて、初期化の準備ができていることを確認します。
13. nCipher HSM が初期化前（new-world の実行前）は「I」の位置に、new-world の実行後は「O」の位置に設定されていることを確認します。
14. new-world を実行する前に、必ず登録をクリアしてください。

症状:

nCipher カードおよびソフトウェアをインストールしましたが、TIM が Web サーバからのデータを復号化していません。また、TIM の起動時、ログには以下のメッセージが表示されます。

```
Initializing SSL crypt engine
Sslinterface: "chil" SSL engine initialization failed
```

解決方法:

1. nCipher バンドル Chil SSL がインストールされていることを確認します。
   a. TIM コンソールにログインします（PuTTY または同様の ssh クライアントを使用）。
   b. この nCipher バンドルが存在することを確認します（*/opt/nfast/toolkit/hwcrhk/libnfhwcrhk.so*）。
2. nCipher バンドル Chil SSL が存在しない場合は、nCipher CD からインストールします。
   a. 詳細については、nCipher のインストール ガイドを参照してください （nCipher 11.30 で、このバンドルの名前は、*/<CD>/linux/lib6-3/nfast.hwcrhk/user.tar* です）。
   b. TIM を再起動します。

      TIM ログに、Chil SSL バンドルが初期化されていることが示されます。

      ```
      Wed Mar 30 02:09:20 2011 19826   Initializing SSL crypt engine
      Wed Mar 30 02:09:20 2011 19826   sslinterface: "chil" SSL engine found
      Wed Mar 30 02:09:20 2011 19826  sslinterface: "chil" SSL engine initialized
      ```

症状:

Web サーバによって nCipher で暗号化された HTTPS トラフィックを TIM が復号化していることを確認するにはどうすればよいですか。

解決方法:

TIM のログで、接続の追跡コンポーネントおよび HTTPS の追跡コンポーネントを探します。

接続コンポーネントと HTTPS コンポーネントの両方が見つかります。 たとえば、https サーバが 172.16.163.52 のポート 9966 上にある場合、接続追跡が有効になっていれば、コンポーネントは以下のように表示されます。

```
Wed Mar 30 02:34:00 2011 19826   Trace: [172.16.163.32]:3691->[172.16.163.52]:9966
opened
```

また、コンポーネント追跡が有効になっていれば、以下のように表示されます。

```
Wed Mar 30 02:34:00 2011 19826   Trace: Component #18 request:
172.16.163.52/testpage.html client=[172.16.163.32]:3691
server=[172.16.163.52]:9966 at 02:34:00
```

TIM がトラフィックを復号化できない場合は、接続メッセージのみが表示されます。

```
Wed Mar 30 02:34:00 2011 19826   Trace: [172.16.163.32]:3691->[172.16.163.52]:9966
opened

Wed Mar 30 02:34:00 2011 19826   Trace: [172.16.163.32]:3691->[172.16.163.52]:9966
closed
```

第 6 章: CA APM でのスマート カード認証の使用

この章では以下のトピックについて説明します。

CA APM でのスマート カードの使用について

安全な環境では、アクセス管理を容易にするために、単一のエントリ ポイントの使用が必要となることがよくあります。 単一のエントリ ポイントを使用しない場合、セキュリティ管理者は、セキュリティ レベル、要件、およびユーザ アクセスの異なるいくつかのプログラムを管理する必要があります。 すべての制御されたリソースにアクセスするためにスマート カードの使用が必要とされることにより、スマート カードは単一のエントリ ポイントを提供します。

アクセス権は、CA APM で定義されたローカル セキュリティまたは CA EEM の権限に基づいて、ユーザに付与されます。

CA APM は、WebView、Web Start、および CEM コンソール用のスマート カード認証を提供します。

このセクションには、スマート カード認証について紹介するトピックが含まれています。

スマート カード確認オプション

以下のいずれかのオプションを使用するようにスマート カード確認を構成できます。

- *証明書破棄リスト（CRL）*

  証明書が有効であることを確認する最も一般的な方法。

  CRL ファイルは、破棄された証明書のシリアル番号が含まれるフラット ファイルです。 CRL ファイルは、証明機関によって追加が定期的に行われるので、頻繁に更新されます。 CRL ファイルは、事前に指定された時間に期限切れになるので、再びロードする必要があります。 大量のメモリを消費するので、ローカル ファイル システムに配置する必要があります。 通常、システム管理者およびセキュリティ管理者が OCSP サーバまたは OCSP レスポンダに対するアクセス権を持っていない場合は、このオプションを選択します。

- *オンライン証明書ステータス プロトコル（OCSP）*

  通常、システム管理者とセキュリティ管理者が OCSP サーバおよび OCSP レスポンダをセットアップするためのリソースとソフトウェアを持っている場合は、このオプションを選択します。 OCSP は、より少ない帯域幅を使用して、妥当性チェックを高速化します。

  OCSP は、CRL 情報を抽象化してデータベースに格納することによって、CRL ファイルをロードするのに必要な時間を削減します。OCSP サーバは、証明書を確認するリクエストを受け付けます。 管理者がいつでも証明書を破棄できるので、OCSP サーバおよび OCSP レスポンダが古くなることはほとんどありません。 製品サーバとは異なるサーバに OCSP を配置できます。

証明書が本物で有効であると確認されると、スマート カードが受け入れられます。 定義された許可権限に基づいて、アクセス権が CA APM に付与されます。 CA EEM を使用して許可する場合は、権限は *realms.xml* ファイルで定義されています。ローカル許可を使用する場合は、権限は *users.xml* ファイルで定義されています。

スマート カード認証コンポーネント

スマート カード認証では、ハイパーテキスト転送プロトコル（HTTP）、Lightweight Directory Access Protocol （LDAP）、および Secure Sockets Layer （SSL）などの基本的な通信プロトコルが使用されます。 CA APM 用のスマート カード認証をセットアップする前に、これらの概念の基本的な理解をしておくことが必要です。

さらに、スマート カード認証では以下のコンポーネントを使用します。

- スマート カード破棄確認サービス（SCARVES）
- CA Embedded Entitlements Manager （CA EEM）
- CA APM のローカルによるセキュリティ

SCARVES について

SCARVES は、スマート カードから取得したセキュリティ証明書を検証する機能を提供します。 確認と検証のプロセスには、証明書を確認するために OCSP サーバまたは CRL サーバを使用するオプションが含まれます。

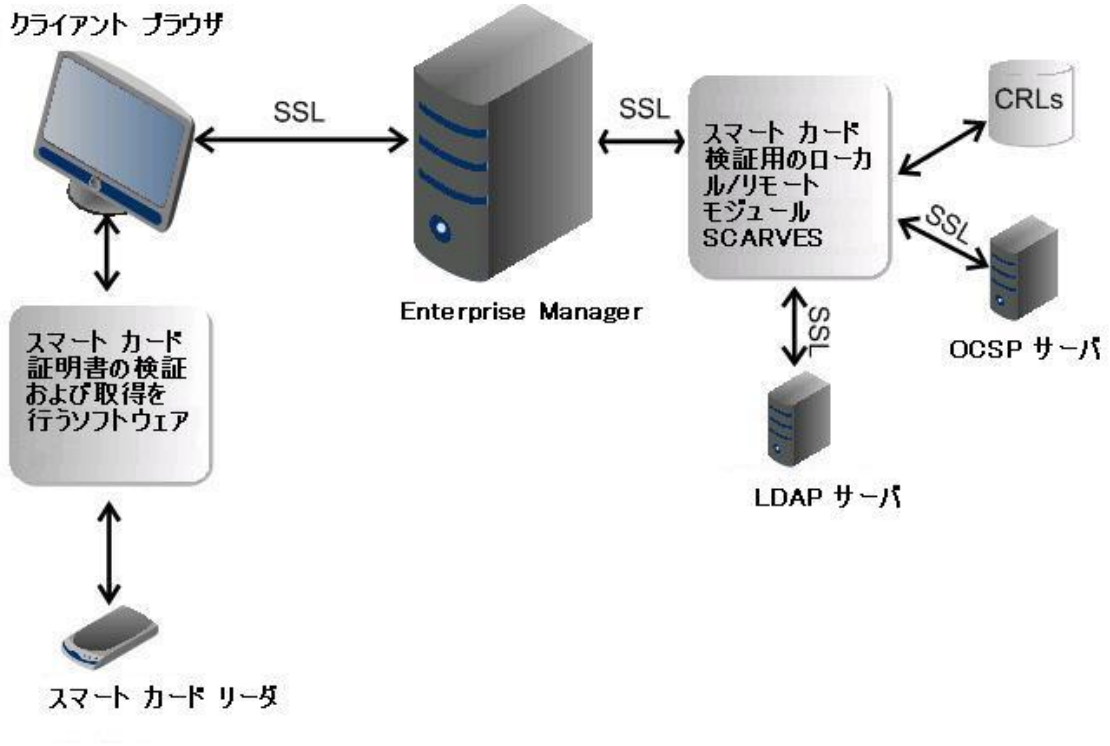
証明書の確認が成功すると、ユーザ レコードが存在する場合は、証明書と関連付けられたユーザ情報が LDAP サーバを介して取得されます。 SCARVES は、検証プロセスの一部として LDAP ユーザ情報検索を行います。その後、Enterprise Manager がユーザ情報を受信し、ローカルによるセキュリティまたは CA EEM を使用してユーザ ロールとアクセス権限を確認することにより、許可プロセスを続行します。

SCARVES デーモンは、証明書の確認および検証処理を行うプロセスです。基本的に、デーモンは、OCSP サーバまたは CRL サーバのいずれかに対するプロキシとして機能する、実行中のプロセスです。 構成の必要性に応じて、ユーザの環境で 1 つ以上のデーモンを実行することができます。使用するデーモンの数には、CRL サーバまたは OCSP サーバの使用などの要素が含まれます。

注: スタンドアロンの Enterprise Manager、コレクタ、または Manager of Managers（MOM）に対してスマート カード認証を有効にできます。MOM に対してスマート カードを有効にする場合は、スマート カード認証がクラスタ全体に適用されるように、MOM で構成を行う必要があります。

CA APM がスマート カード データを使用して認証を行う方法

以下の図は、CA APM がスマート カード データを使用して処理および認証を行う方法を示したものです。



スマート カード データは以下のように処理されます。

1. CA APM ユーザが、オペレーティング システムまたはデスクトップにログインしているときに、スマート カード リーダにスマート カードを挿入します。
2. ユーザがクライアント ブラウザを使用して CA APM にログインしようとすると、個人識別番号（PIN）の入力が要求されます。
3. ユーザがスマート カード用の正しい PIN を入力した後、スマート カードに格納されているすべての証明書を含む証明書選択ダイアログ ボックスが表示されます。 Web 認証に進むには、正しい証明書を選択する必要があります。
4. ユーザが証明書を選択した後、ブラウザ クライアントは SSL 接続を使用して Enterprise Manager に証明書を送信します。

5. Enterprise Manager は証明書を受信し、次に、SSL 接続を使用して SCARVES にその証明書を渡します。
6. SCARVES は証明書を受信し、OCSP サーバまたは CRL フラット ファイルからの確認を要求します。
7. OCSP 確認または CRL 確認が成功した場合、SCARVES は、リクエストされたユーザ情報を LDAP サーバから取得します。
8. SCARVES は、確認結果と、LDAP から取得したユーザ情報を、Enterprise Manager に XML 形式で返します。
9. Enterprise Manager は、定義された許可権限に基づいて、CA APM へのアクセス権を付与します。CA APM が CA EEM を使用して許可するように構成されている場合は、権限は *realms.xml* ファイルで定義されています。ローカル許可を使用する場合は、権限は *users.xml* ファイルで定義されています。

スマート カード認証用の CA APM のセットアップ

CA APM 環境用のスマート カード認証を有効にするには、指定された順序で以下の手順に従います。

1. お使いの環境が必要な要件を満たしていることを確認します。詳細については、「Smart カード認証要件 (P. 209)」を参照してください。
2. SCARVES コンポーネントを解凍してインストールします。詳細については、「SCARVES コンポーネントの解凍およびインストール (P. 210)」を参照してください。

   注: スタンドアロンの Enterprise Manager、コレクタ、または Manager of Managers （MOM）に対してスマート カード認証を有効にできます。MOM に対してスマート カードを有効にする場合は、スマート カード認証がクラスタ全体に適用されるように、MOM で構成を行う必要があります。

3. 必要なキーストアに証明書をロードします。 詳細については、以下のトピックを参照してください。
   - daemon-cert キーストアに証明書をロードする (P. 212)
   - daemon-trust キーストアに証明書をロードする (P. 212)
   - Enterprise Manager キーストアに SCARVES 証明書をロードする (P. 212)
4. 証明書パスワードを暗号化します。 詳細については、「キーストア用証明書パスワードの暗号化 (P. 215)」を参照してください。
5. CRL を使用するためにスマート カード確認を構成する場合は、CRL ファイルをロードします。 「(オプション) CRL ファイルをロードする (P. 215)」を参照してください。
6. SCARVES を使用するように Enterprise Manager を構成します。 詳細については、「SCARVES を使用するために Enterprise Manager を構成する (P. 216)」を参照してください。
7. SCARVES ラッパ ファイルを構成します。 詳細については、「SCARVES ラッパの構成 (P. 217)」を参照してください。
8. SCARVES を構成します。 詳細については、「SCARVES の構成 (P. 217)」を参照してください。
9. SCARVES を起動します。詳細については、「SCARVES の起動と停止 (P. 230)」を参照してください。
10. スマート カード認証が正常にインストールおよび構成されていることを確認します。 詳細については、「スマート カード インストールの確認 (P. 231)」を参照してください。

スマート カード認証要件

ハードウェアの前提条件:

- スマート カード
- スマート カード リーダ

ソフトウェア要件

- CA APM 9.0 以降
- スマート カード証明書の検証および取得を行う、ActivClient などのソフトウェア
- Internet Explorer 6 または 7

構成に対する要件

- システムで使用されるすべてのスマート カード用のルートおよび中間のセキュリティ証明書
- スマート カードの確認および検証で使用するために既存の LDAP ディレクトリを統合する LDAP サーバ情報
- OCSP サーバの使用を計画している場合は、OCSP サーバ情報をすべて収集します。
  - 応答 URL
  - OCSP サーバの証明書
- CRL ファイルの使用を計画している場合は、システムで使用されるスマート カード用の CRL ファイルをすべて収集します。
  - 必要な SCARVES デーモンの数を決定する要因の 1 つは、スマート カード ネットワーク ソリューションを構成する方法です。たとえば、CRL ファイルは大きくなる傾向があり、SCARVES デーモンはメモリに CRL ファイルをすべて保持します。

    計算の基準として、1 つのデーモンあたりの CRL ファイルの合計サイズを 256 メガバイト未満にします。 単一のサーバで処理できるデーモン数より多くのデーモンが必要な場合は、専用 OCSP サーバを構成することを検討してください。

- 構成を準備するために、デーモンの数の計算に加えて、以下の SCARVES デーモン値の計画および記録を行います。
  - 各デーモンの名前
  - 各デーモンのポート番号
  - 各 CRL ファイルのディレクトリ名
    （*<SCARVES_HOME>/crls/<daemon_name>* など）

Windows 上での SCARVES コンポーネントの解凍およびインストール

SCARVES コンポーネントを解凍すると、SCARVES を構成して、スマート カード認証を有効にできます。

Windows で有効

1. SCARVES コンポーネントを格納するためのディレクトリを作成します。たとえば、*<drive>:¥SmartCard¥scarves* です。

   作成するディレクトリは、スマート カードのホーム ディレクトリになります。このホーム ディレクトリは、*<SCARVES_HOME>* として参照されます。

2. Enterprise Manager がインストールされている最上位のディレクトリに移動します。 たとえば *<EM_HOME>* です。

3. *examples¥SmartCardAuthentication* に移動し、環境に適した *scarve_0.1* ファイルの内容を抽出します。Enterprise Manager のインストール方法の詳細については、「CA APM インストールおよびアップグレード ガイド」を参照してください。

   以下のディレクトリが作成されます。

   - bin
   - conf
   - crls
   - keystores

- lib
- logs

4. *<SCARVES_HOME>¥bin* ディレクトリから *InstallScarves-NT.bat* を実行します。

   ファイルの実行が成功すると、SCARVES コンポーネントがインストールされます。

UNIX および Linux で有効

1. */etc/init.d* に移動し、*<SCARVES_HOME>*/bin/scarves スクリプトをリンクします。
2. 以下のように *rc?.d* ディレクトリをリンクします。
   - ln -s <SCARVES_HOME>/bin/scarves /etc/init.d/scarves
   - ln -s /etc/init.d/scarves /etc/rc3.d/S99scarves
   - ln -s /etc/init.d/scarves /etc/rc2.d/K15scarves
   - /sbin/chkconfig --add scarves

重要: スクリプトは構成ファイルを見つけるためにリンクを使用するので、これらのリンクはシンボリック リンクである必要があります。

証明書のロード

スマート カードは、SSL 経由で一連の証明書を使用して認証します。 さまざまなキーストアに証明書をロードする必要があります。 詳細については、以下のトピックを参照してください。

- daemon-cert キーストアに証明書をロードする（P. 212）
- daemon-trust キーストアに証明書をロードする（P. 212）
- Enterprise Manager キーストアに SCARVES 証明書をロードする（P. 212）

daemon-cert キーストアに証明書をロードする

クライアント アプリケーションにデーモンの詳細を提供するには、daemon-cert キーストアにサーバ証明書をロードします。 これは、SSL で SCARVES に通信するとき、Enterprise Manager がクライアントとして機能できるようにするために必要です。

証明書を操作するさまざまなコマンドの詳細については、「証明書を操作するコマンド (P. 212)」を参照してください。

daemon-trust キーストアに証明書をロードする

SSL を介して OCSP サーバおよび LDAP サーバに通信するには、daemon-trust キーストアに証明書をロードする必要があります。

注: OCSP を使用するために SCARVES を構成する場合は、エイリアス名をメモします。 エイリアス名は、SCARVES を構成するために必要です。 詳細については、「（オプション） OCSP を使用するために SCARVES を構成する (P. 227)」を参照してください。

Enterprise Manager キーストアに証明書をロードする

SCARVES と通信するには、Enterprise Manager に SCARVES 証明書をロードする必要があります。 SSL を使用して Enterprise Manager と SCARVES の間でクライアント証明書を送受信するときに、確認が行われます。 証明書を操作するさまざまなコマンドの詳細については、「証明書を操作するコマンド (P. 212)」を参照してください。

証明書コマンド

証明書コマンドを使用すると、キーストアからの証明書のインポート、生成、およびエクスポートを実行できます。 詳細については、以下のセクションを参照してください。

- 自己署名証明書の生成 (P. 213)
- 証明書のインポート (P. 214)
- 証明書のエクスポート (P. 214)

自己署名証明書の生成

-genkey コマンドを使用して、自己署名セキュリティ証明書を生成できます。 このコマンドは、キーストアのいずれか用の自己署名証明書を生成するために使用できます。

以下の手順に従います。

1. CA APM サーバに root としてログインし、コマンド プロンプトにアクセスします。
2. *$JAVA_HOME/bin/keytool* に移動し、*-genkey* コマンドを使用して、ユーティリティを実行します。 例：

   ```
   -genkey -keyalg RSA -keystore <SCARVES_HOME>/keystores/daemoncert -alias
   <cert_alias>
   ```

   次のような情報を表示する、組織の内容を指定する対話型プロセスが開始されます。

   ```
   キーストアのパスワードを入力してください: changeit
   新規パスワードを再入力してください: changeit
   姓名を入力してください。
     [Unknown]:  name.company.com
   組織単位名を入力してください。
     [Unknown]:  ABC
   組織名を入力してください。
     [Unknown]:  NOC
   都市名または地域名を入力してください。
     [Unknown]:  Anytown
   州名または地方名を入力してください。
     [Unknown]:  Alaska
   この単位に該当する 2 文字の国番号を入力してください。
     [Unknown]:  US
   CN=name.company.com、OU=ABC、O=NOC、L=Anytown、
   ST=Alaska、C=US でよろしいですか?
     [no]:  yes

   <newcert> の鍵パスワードを入力してください。
           (キーストアのパスワードと同じ場合は RETURN を押してください):
   ```

証明書のインポート

証明書をインポートするには、*-importcert* コマンドを使用します。 このコマンドは、キーストアのいずれかに証明書をインポートするために使用できます。

以下の手順に従います。

1. CA APM サーバに root としてログインし、コマンド プロンプトにアクセスします。
2. *$JAVA_HOME/bin/keytool* に移動し、*-importcert* コマンドを使用して、ユーティリティを実行します。 例：

```
keytool -importcert -keystore <SCARVES_HOME>/keystores/daemoncert -alias
cert_alias -file cert_file
```

証明書のエクスポート

証明書をエクスポートするには、*-exportcert* コマンドを使用します。 このコマンドは、キーストアのいずれかから証明書をエクスポートするために使用できます。

以下の手順に従います。

1. CA APM サーバに root としてログインし、コマンド プロンプトにアクセスします。
2. *$JAVA_HOME/bin/keytool* に移動し、*-exportcert* コマンドを使用して、ユーティリティを実行します。 例：

```
keytool -exportcert -keystore <SCARVES_HOME>/keystores/daemoncert -alias
cert_alias -file cert_file
```

キーストア用証明書パスワードの暗号化

キーストアは、暗号化された証明書パスワードのみを格納します。 暗号化されたパスワードは証明書を保護します。 暗号化アルゴリズムは Advanced Encryption Standard （AES）です。 このアルゴリズムは、クリアテキストを使用しないサービスおよびデーモン コードにキーを埋め込みます。 暗号化されたパスワードは Base64 エンコードされるため、印刷可能な文字列を生成できます。

以下の手順に従います。

1. *<SCARVES_HOME>/lib* に移動し、*scarve_client.jar* ファイルを開きます。

   このファイルに、キーストア用の暗号化が必要なパスワードを設定して、保存します。

2. 以下のコマンドを実行します。

   ```
   java –cp scarve_client.jar com.ca.scarve.common.xml.cond e p
   <password_that_requires_encryption>
   ```

   暗号化されたパスワードは、*SCARVESconfig.xml* ファイルで使用できます。

（オプション）CRL ファイルをロードする

CRL を有効にするために SCARVES を構成する場合は、CRL ファイルをロードすることも必要です。

以下の手順に従います。

- CRL ファイルを *<SCARVES_HOME>/crls/<DAEMON_NAME>* ディレクトリにコピーします。

  注: CRL を使用するために SCARVES を構成する場合は、CRL の場所をメモします。 CRL の場所は、SCARVES を構成するために必要です。 詳細については、「（オプション） CRL を使用するために SCARVES を構成する (P. 225)」を参照してください。

SCARVES を使用するために Enterprise Manager を構成する

スマート カード認証を有効にするために Enterprise Manager を構成する必要があります。

以下の手順に従います。

1. *<EM_HOME>¥config* に移動し、*IntroscopeEnterpriseManager.properties* ファイルを開いて、以下のプロパティを設定します。
   - *introscope.enterprisemanager.scauth.SCARVES.hostname=<scarves_machine_name>*
   - *introscope.enterprisemanager.scauth.SCARVES.port=9998*
   - *introscope.enterprisemanager.webserver.scauth.keystore=/internal/daemoncert*
   - *introscope.enterprisemanager.webserver.scauth.keypass=パスワード*
   - *introscope.enterprisemanager.webserver.scauth.enable=true*
2. *<EM_HOME>¥config* に移動し、*em-jetty-config.xml* ファイルを開いて、以下のプロパティを設定します。
   - *needclientauth= true*
3. *<EM_HOME>¥config* に移動し、*IntroscopeEnterpriseManager.properties* ファイルを開いて、以下の手順に従います。
   a. *introscope.enterprisemanager.webserver.jetty.configurationFile=em-jetty-config.xml* プロパティのコメント化を解除します。
   b. *needclientauth* プロパティを *true* に設定します。
4. *<EM_HOME>¥config* に移動し、*introscopewebview.properties* ファイルを開いて、以下の手順に従います。
   a. *introscope.webview.jetty.configurationFile=webview-jetty-config.xml* プロパティのコメント化を解除します。
   b. *needclientauth* プロパティを *true* に設定します。
5. Enterprise Manager を再起動します。

SCARVES ラッパの構成

SCARVES ラッパは、SCARVES を実行する Java プログラムを起動するのに必要な情報を提供する構成ファイルです。

以下の手順に従います。

1. *<SCARVES_HOME>/conf* に移動し、*wrapper.conf* ファイルを開きます。
2. 以下のプロパティを設定します。
   - wrapper.java.command=java
   - wrapper.app.parameter.2=../conf/SCARVESconfig.xml
3. ファイルを保存します。

SCARVES の構成

スマート カード コンポーネントを解凍した後、テンプレート構成ファイルを更新します。*SCARVESconfigtemplate.xml* ファイルをテンプレートとして使用して、キーストアの場所、各 SCARVES デーモンの説明、SCARVES が OCSP と CRL のどちらを使用するか、などの詳細を定義します。

重要: SCARVES 構成設定を正常に適用するには、*SCARVESconfigtemplate.xml* テンプレートを *SCARVESconfig.xml* として保存する必要があります。

一般的な XML の形式は以下のとおりです。

```
<?xml version="1.0" encoding="UTF-8"?>
<SmartCardService>
    ... サービス パラメータ ...
    ... 1 つ以上のデーモンの記述 ...
</SmartCardService>
```

以下の手順に従います。

1. *<SCARVES_HOME>/conf* に移動し、*SCARVESconfigtemplate.xml* を開きます。
2. XML 編集ツールを使用して、以下の一般的な SCARVES 設定を設定します。
   - SCARVES サービス パラメータを構成する (P. 218)
   - SCARVES デーモンを構成する (P. 220)
   - LDAP を使用するために SCARVES を構成する (P. 222)

また、スマート カード確認プロトコルも指定します。

- （オプション） OCSP を使用するために SCARVES を構成する (P. 227)
- （オプション） CRL を使用するために SCARVES を構成する (P. 225)

注: お使いの環境に対して有効にできるプロトコルは 1 つのみです。

3. そのファイルを *SCARVESconfig.conf* という名前で保存します。
4. SCARVES サービスを開始します。 詳細については、「SCARVES の起動と停止 (P. 230)」を参照してください。

SCARVES サービス パラメータを構成する

SCARVES サービス パラメータでは、キーストアの場所およびパスワードの詳細を指定します。

一般的な XML の形式は以下のとおりです。

```
<SmartCardService>
    <trust-keystore>キーストアのファイル名</trust-keystore>
    <trust-keystore-pass>キーストアの暗号化されたパスワード</trust-keystore-pass>
    <jvm-arg>-mx1024m</jvm-arg> <!-- optional, param for all Daemon JVMs -->
    ... 1 つ以上のデーモンの記述 ...
</SmartCardService>
```

以下のパラメータが構成できます。

<trust-keystore>

すべてのデーモンに対する信頼キーストアを指定します。 ファイルには、スマート カードをすべて受け入れるためにルートおよび中間の証明書がすべて含まれる必要があります。 このパラメータは、以下のパラメータを持つすべてのデーモンに渡されます。

-Djavax.net.ssl.trustStore=ファイル名 JVM

注: すべてのデーモンは同じ信頼キーストアを使用します。

<trust-keystore-pass>

信頼キーストアのパスワードを指定します。 このパスワードは、XML ファイル内で暗号化されている必要があります。以下のパラメータを持つすべてのデーモンにクリアテキストで渡されます。

`-Djavax.net.ssl.trustStorePassword=`パスワード

<debug>

デバッグ用ログ記録のレベルを設定します。利用できる値は以下のとおりです。

- 0- デバッグ用ログ記録を行わないことを指定します。 これがデフォルト値です。
- 1- デバッグ レベルの詳細を最低レベルに指定します。
- 2- デバッグ レベルの詳細を標準的な中間レベルに指定します。
- 3- デバッグ レベルの詳細を最高レベルに指定します。

<jvm-arg>

すべてのデーモン JVM のパラメータを指定します。このパラメータは、使用可能なメモリ容量を調節します。

構成設定を適用する方法の詳細については、「SCARVES の構成 (P. 217)」を参照してください。

SCARVES デーモンを構成する

SCARVES デーモン パラメータは、CRL または OCSP を使用するかどうかと、LDAP の詳細を指定します。 CRL と OCSP の両方を指定できますが、有効にできるのは 1 つのみです。したがって、1 つをコメント アウトする必要があります。

一般的な XML の形式は以下のとおりです。

```
<SmartCardService>
    ... サービス パラメータ ...
    <Daemon name="name" port="port number">
        <keystore>...キーストアのファイル名...</keystore>
        <keystore-pass>...キーストアの暗号化されたパスワード...</keystore-pass>
        <jvm-arg>-mx1024m</jvm-arg> <!-- optional, param for this Daemon JVM -->
        ... プロトコルの説明...
        ... LDAP の説明...
    </Daemon>
    ... その他のデーモンの説明 ...
</SmartCardService>
```

以下のパラメータが構成できます。

name

各デーモン名の一意の名前を指定します。 これは、内部で追跡に使用され、ログ ファイルでは適切なエラー コードおよびデバッグ コードの前に付けられます。

port

デーモンがリスンする TCP ポートを指定します。

<keystore>

デーモンが SSL 通信に使用する証明書が含まれるキーストア ファイルを指定します。

<keystore-pass>

キーストアのパスワードを指定します。 このパスワードは、XML ファイル内で暗号化されている必要があります。

<jvm-arg>

すべてのデーモン JVM のパラメータを指定します。このパラメータは、このセクションで指定された *各*デーモンで使用可能なメモリ容量を調節します。 基本的な SCARVES サービス パラメータ セクションの <jvm-arg> タグと違う点は、このパラメータはデーモンの *すべて*には送信されない点です。

構成設定を適用する方法の詳細については、「SCARVES の構成 (P. 217)」を参照してください。

LDAP を使用するために SCARVES を構成する

デーモンが LDAP を使用する場合、この認証方法の詳細を指定するパラメータを定義する必要があります。

一般的な XML の形式は以下のとおりです。

```
<SmartCardService>
    ... サービス パラメータ ...
    <Daemon ...parameters...>
        ... デーモンのその他のパラメータ...
        ... プロトコルの説明...
        CA LDAP Server for z/OS
            <ldap-enabled>true</ldap-enabled>
            <ldap-hostname>renge01-winvm</ldap-hostname>
            <ldap-port>24132</ldap-port>
            <ldap-ssl>false</ldap-ssl>
            <ldap-user-dn>uid=GGantt,ou=people,dc=ca,dc=com</ldap-user-dn>

<ldap-user-pass>05V2irWBg8O39H6ANGic241UWooJuIbJiHE+ZqKPvUY=</ldap-user-pass>
            <ldap-base-dn>ou=people,dc=ca,dc=com</ldap-base-dn>
            <cert-uniqueid-field>subject</cert-uniqueid-field>
            <cert-uniqueid-regex>CN=¥w*¥.¥w*¥.(¥d+),</cert-uniqueid-regex>

<ldap-uniqueid-search-field>facsimileTelephoneNumber</ldap-uniqueid-search-field>
            <ldap-cache-lifetime>300</ldap-cache-lifetime>
        </ldap>
    </Daemon>
    ... その他のデーモンの説明 ...
</SmartCardService>
<ldap-enabled>
```

以下のパラメータが構成できます。

<ldap-enabled>

LDAP の有効/無効を指定します。 利用できる値は以下のとおりです。

- *true* は、デーモンに対して LDAP を有効にします。
- *false* は、デーモンに対して LDAP を無効にします。この値を false に設定すると、構成ファイルの CA LDAP Server for z/OS セクションに、未使用の設定を格納できます。

<ldap-hostname>

LDAP サーバのホスト名を指定します。

<ldap-port>

LDAP サーバのポートを指定します。

<ldap-ssl>

値を *true* に設定する場合、SSL を使用するために LDAP サーバを指定します。 この機能を有効にする場合は、LDAP サーバ証明書が信頼キーストア内にあることを確認します。

<ldap-user-dn>

デーモンが LDAP サーバにログインするために使用する識別名を指定します。サーバは、この識別名に検索権限を付与する必要があります。

<ldap-user-pass>

デーモンが LDAP サーバにログインするために使用するパスワードを指定します。 パスワードは、XML ファイル内で暗号化されている必要があります。

<ldap-base-dn>

ベースとなる識別名を指定します。これは LDAP 検索で出発点となります。 検索対象のすべての識別名は、ベースとなる識別名の下に表示される必要があります。

<cert-uniqueid-field>

Electronic Data Interchange Personal Identifier（EDIPI）またはほかの一意の識別が含まれる証明書フィールドを指定します。 有効な値は、*subject*、*subuid*、*an_other*、および *an_rfc822* です。

<cert-uniqueid-regex>

指定されたフィールドから一意の識別を抽出する方法を詳細に示す正規表現を指定します。

<ldap-uniqueid-search-field>

EDIPI またはほかの一意の識別が含まれる LDAP エントリ フィールドを指定します。

<ldap-cache-lifetime>

キャッシュされた LDAP ルックアップが有効な最長時間（秒単位）を指定します。

デフォルト値の *ゼロ*が設定される場合、LDAP ルックアップはキャッシュされません。

LDAP エントリが変更されると、キャッシュがタイム アウトになるまで、キャッシュされたエントリが誤った値を返すので、この値はあまり大きく設定しないでください。

暗号化

XML ファイル内に格納されたパスワードが暗号化される必要があることを指定します。暗号化アルゴリズムは、Advanced Encryption Standard（AES）です。このアルゴリズムは、クリアテキストを使用しないサービスおよびデーモン コードにキーを埋め込みます。暗号化されたパスワードは、XML ファイルに格納できる印刷可能な文字列を生成するために Base64 エンコードされます。

構成設定を適用する方法の詳細については、「SCARVES の構成 (P. 217)」を参照してください。

（オプション）CRL を使用するために SCARVES を構成する

CRL パラメータは、ファイル ストレージの詳細を指定します。一度に 1 つの CRL しか構成できません。

重要: CRL を使用するために *SCARVESconfig.xml* を構成する場合、単一のデーモンでエラーを発生させずに SCARVES を起動するために、*<ocsp-enabled>* パラメータの OCSP 値を *false* に設定する必要があります。

一般的な XML の形式は以下のとおりです。

```
<SmartCardService>
    ... サービス パラメータ ...
    <Daemon ...parameters...>
        ... デーモンのその他のパラメータ...
        <crl>
            <crl-enabled>true</crl-enabled>
            <crl-dp>false</crl-dp>
            <crl-url>...CRL ファイルが含まれる URL...</crl-url>
            <crl-dir>...CRL ファイルが含まれるディレクトリ名...</crl-dir>
            <crl-poll-int>30</crl-poll-int>
        </crl>
        ... LDAP の説明...
    </Daemon>
    ... その他のデーモンの説明 ...
</SmartCardService>
```

以下のパラメータが構成できます。

<crl-enabled>

値を *true* に設定することによって、CRL ファイルを使用することをデーモンに指定します。 値を *false* に設定すると、デーモンは OCSP を使用できます。

<crl-dp>

CRL ファイルがダウンロードされる配布拠点を指定します。

<crl-url>

CRL ファイルが含まれる URL を指定します。

<crl-dir>

CRL ファイルが含まれるディレクトリの名前を指定します。

<crl-poll-int>

CRL ディレクトリまたは CRL URL で新規 CRL ファイルまたは変更された CRL ファイルをスキャンする頻度を秒単位で指定します。 スキャンされた証明書がキャッシュされます。 このパラメータが指定されていない場合は、デフォルトの間隔は 60 秒です。

構成設定を適用する方法の詳細については、「SCARVES の構成 (P. 217)」を参照してください。

（オプション）OCSP を使用するために SCARVES を構成する

OCSP パラメータは、スマート カード検証に OCSP を使用するのに必要な詳細を指定します。 このプロトコルを使用する場合、構成ファイル内の CRL プロトコル オプションをコメント アウトすることが必要です。

重要: OCSP を使用するために *SCARVESconfig.xml* を構成する場合、単一のデーモンでエラーを発生させずに SCARVES を起動するために、*<crl-enabled>* パラメータの CRL 値を *false* に設定する必要があります。

一般的な XML の形式は以下のとおりです。

```
<SmartCardService>
    ... サービス パラメータ ...
    <Daemon ...parameters...>
        ... デーモンのその他のパラメータ...
        <ocsp>
            <ocsp-enabled>true</ocsp-enabled>
            <ocsp-aia>false</ocsp-aia>
            <ocsp-cert-alias>ocsp_qacle3</ocsp-cert-alias>
            <ocsp-url>http://qacle3:3501/responder</ocsp-url>
        </ocsp>
        ... LDAP の説明...
    </Daemon>
    ... その他のデーモンの説明 ...
</SmartCardService>
```

以下のパラメータが構成できます。

<ocsp-enabled>

この値を *true* に設定すると、OCSP を使用するデーモンが指定されます。

<ocsp-aia>

スマート カード認証が実装されるときに、この値を *true* に設定すると、Authority Info Access （AIA）が指定されます。

<ocsp-cert-alias>

OCSP レスポンダが応答に署名するために使用する証明書のエイリアスを指定します。 この機能を有効にする場合は、OCSP サーバ証明書が信頼キーストア内にあることを確認します。

<ocsp-url>

OCSP レスポンダの URL を指定します。

構成設定を適用する方法の詳細については、「SCARVES の構成 (P. 217)」を参照してください。

サンプルの SCARVES 構成ファイル

以下のコード サンプルは、*SCARVESconfig.xml* 構成ファイルの一部を示しています。 CRL および LDAP サーバを使用して、スマート カードを確認する 2 つのデーモンが定義されています。

両方のオプションが存在する XML を構成することはできますが、構成プロパティは OCSP または CRL のみに有効である必要があります。

```
<?xml version="1.0" encoding="UTF-8"?>

<SmartCardService>
<trust-keystore>../keystores/daemontrust</trust-keystore>
<trust-keystore-pass>YEDZLwyEVTnCfzS+rYTfC41UWooJuIbJiHE+ZqKPvUY=</trust-keystore
-pass>
<debug>0</debug>

<jvm-arg>-mx1024m</jvm-arg>

<Daemon name="daemon-crl-1" port="9999">
   <keystore>../keystores/daemoncert</keystore>
   <keystore-pass>YEDZLwyEVTnCfzS+rYTfC41UWooJuIbJiHE+ZqKPvUY=</keystore-pass>

   <crl>
    <crl-enabled>true</crl-enabled>
    <crl-dp>false</crl-dp>
    <crl-url />
    <crl-dir>../crls/daemon-crl</crl-dir>
    <crl-poll-int>600</crl-poll-int>
   </crl>
```

```
  <ldap>
    <ldap-enabled>true</ldap-enabled>
    <ldap-hostname>host1</ldap-hostname>
    <ldap-port>24000</ldap-port>
    <ldap-ssl>false</ldap-ssl>
    <ldap-base-dn>ou=people,dc=abc,dc=com</ldap-base-dn>
    <ldap-user-dn>uid=JDoe,ou=people,dc=abc,dc=com</ldap-user-dn>
    <ldap-user-pass>05V2irWZg8O39L6ANGic241UWi0JuIbJiHE+ZqKPvUY=</ldap-user-pass>
    <cert-uniqueid-field>subject</cert-uniqueid-field>
    <cert-uniqueid-regex>CN=¥w*¥.¥w*¥.(¥d+),</cert-uniqueid-regex>

<ldap-uniqueid-search-field>facsimileTelephoneNumber</ldap-uniqueid-search-field>
  </ldap>
</Daemon>

<Daemon name="daemon-ocsp-1" port="9998">
  <keystore>../keystores/daemoncert</keystore>
  <keystore-pass>YEDZLwyEVTnCfzS+rYTfC41UWooJuIbJiHE+ZqKPvUY=</keystore-pass>

  <ocsp>
    <ocsp-enabled>true</ocsp-enabled>
    <ocsp-aia>false</ocsp-aia>

    <ocsp-cert-alias>ocsp_qacle3</ocsp-cert-alias>

    <ocsp-url>http://qacle3:3501/responder</ocsp-url>
  </ocsp>
  <ldap>
    <ldap-enabled>true</ldap-enabled>
    <ldap-hostname>host1</ldap-hostname>
    <ldap-port>24001</ldap-port>
    <ldap-ssl>false</ldap-ssl>
    <ldap-base-dn>ou=people,dc=abc,dc=com</ldap-base-dn>
    <ldap-user-dn>uid=JDoe,ou=people,dc=abc,dc=com</ldap-user-dn>
    <ldap-user-pass>05V2irWBg8O39H6ANGic377UWooJuIbJiHE+ZqKPvUY=</ldap-user-pass>
    <cert-uniqueid-field>subject</cert-uniqueid-field>
    <cert-uniqueid-regex>CN=¥w*¥.¥w*¥.(¥d+),</cert-uniqueid-regex>

<ldap-uniqueid-search-field>facsimileTelephoneNumber</ldap-uniqueid-search-field>
    <ldap-cache-lifetime>300</ldap-cache-lifetime>
  </ldap>
</Daemon>

</SmartCardService>
```

SCARVES の起動と停止

SCARVES は、*SCARVESconfig.xml* 構成ファイルを読み取ることによってデーモンを制御し、指定したポートごとにデーモン プログラムを起動する Java プログラムです。 SCARVES は、以下のいずれかが発生した場合、デーモンを停止して、新しいデーモンを開始します。

- デーモンがクラッシュした場合
- デーモンが通信に応答できない場合
- デーモンが XML ping に応答できない場合

以下の手順に従います。

- CA APM サーバに root としてログインし、コマンド プロンプトにアクセスします。

  Windows で有効

  - SCARVES を起動するには、以下の起動バッチを実行します。
    `<SCARVES_HOME>¥bin¥StartSCARVES-NT.bat`
  - SCARVES を停止するには、以下の停止バッチを実行します。
    `<SCARVES_HOME>¥bin¥StopSCARVES-NT.bat`

  Linux で有効

  - SCARVES を起動するには、以下の起動スクリプトを実行します。
    `/etc/init.d/SCARVES start`
  - SCARVES を停止するには、以下の停止スクリプトを実行します。
    `/etc/init.d/SCARVES stop`
  - SCARVES を再起動するには、以下の再起動スクリプトを実行します。
    `/etc/init.d/SCARVES restart`

  UNIX で有効

  - SCARVES を起動するには、以下の起動コマンドを実行します。
    `<SCARVES_HOME>/bin/scarves start`
  - SCARVES を停止するには、以下の停止コマンドを実行します。
    `<SCARVES_HOME>/bin/scarves stop`
  - SCARVES ステータスを取得するには、以下のステータス コマンドを実行します。
    `<SCARVES_HOME>/bin/scarves status`

スマート カード インストールの確認

スマート カード認証をセットアップした後で、認証方法が正常にインストールされて有効にされたことを確認します。

以下の手順に従います。

1. スマート カード認証用に CA APM をセットアップした後で、WebView、Web Start、または CEM コンソールを起動します。

   ユーザ識別および個人識別番号（PIN）の入力を要求するページが表示されます。

2. PIN を入力します。
3. *<SCARVES_HOME>¥logs* ディレクトリにあるログ ファイルに初期化メッセージが記録されたことを確認します。

CA APM スマート カード認証のトラブル シューティング

トラブルシューティング情報は、スマート カード認証で発生する問題やエラー メッセージを解決するのに役立ちます。

以下のセクションでは役に立つ情報を提供します。

SCARVES の起動に失敗する

Windows、UNIX、および Linux で有効

症状：

スマート カード認証を使用して認証しようとすると、SCARVES の起動に失敗し、以下のエラー メッセージが表示されます。

```
[ERROR] [btpool0-2] [Manager.SCAuth]
com.wily.introscope.spec.server.user.SCException: Error getting user from given
certificate. java.net.ConnectException: Connection refused: connect
```

解決方法：

SCARVES の起動に失敗し、エラー メッセージが返される場合、トラブル シューティングを行って問題を特定できます。

SCARVES の起動に関する問題をトラブル シューティングする方法

1. *<SCARVES_HOME>¥logs* にある *scarve.log* ファイルを開きます。
2. *DEBUG モードの構成*エラー メッセージがログ記録される場合、SCARVES は適切に起動されていません。 以下の手順に従うことによりトラブル シューティングできます。
   - *wrapper.conf* ファイルで指定されている JVM 引数が有効であることを確認します。 例：

     ```
     wrapper.java.command=C:/Progra~1/Java/jdk1.6.0_20/bin/java
     ```
   - ポート バインド エラーが *scarve.log* ファイル内にログ記録されているかどうかを確認します。 ログ記録されている場合、以下のコマンドを入力して、デーモン ポート番号の可用性を確認します。

     ```
     netstat –ao | find <port-no>
     ```

     このポート番号が使用されている場合は、デーモンには一意のポート番号が必要なので、新しいポート番号を割り当てます。
   - *SCARVESconfigtemplate.xml* 内に設定されたプロパティが正しくフォーマットされていることを確認します。
   - *<SCARVES_HOME>/keystores* 内にあるキーストア ファイルが使用可能であることを確認します。

3. *DEBUG モードの構成*エラー メッセージがログ記録されない場合は、SCARVES を再インストールしてください。

   注: SCARVES をアンインストールして再インストールする場合、*config* サブディレクトリおよび *keystores* サブディレクトリ内のファイルは保持されます。

4. SCARVES を再起動します。

   スマート カードを使用して認証できます。

OCSP の検証に失敗する

Windows、UNIX、および Linux で有効

症状：

Web ブラウザを使用して有効な証明書を選択すると、OCSP の検証に失敗し、以下のエラー メッセージが表示されます。

```
[ERROR] [btpool0-0] [Manager.SCAuth]
com.wily.introscope.spec.server.user.SCException: Problem contacting OCSP Server
```

解決方法：

OCSP サーバの再起動により OCSP サーバにアクセスできることを確認します。

OCSP を再起動する方法

1. *services.msc* から OCSP サーバを再起動します。
2. ブラウザを開き、有効な証明書を選択します。

   OCSP 検証が成功します。

CRL の検証に失敗する

Windows、UNIX、および Linux で有効

症状：

CRL 構成環境用のスマート カードを使用して認証しようとすると、失敗します。

解決方法：

CRL を使用した検証で問題が発生する場合、トラブル シューティングを行ってその問題を特定できます。

SCARVES の起動に関する問題をトラブル シューティングする方法

1. *<SCARVES_HOME>¥logs* にある *scarve.log* ファイルを開きます。
2. CRL 有効期限日の詳細が存在する場合、CRL ファイルは期限切れです。

   注: CRL ファイルは週単位で期限切れになります。
3. 最新の CRL ファイルをダウンロードします。

   CRL 検証が成功します。

OCSP サーバが応答しない

Windows、UNIX、および Linux で有効

症状：

スマート カード認証で OCSP オプションを使用しようとすると、OCSP サーバが失敗し、以下のメッセージが表示されます。

```
[ERROR] [btpool0-0] [Manager.SCAuth]
com.wily.introscope.spec.server.user.SCException:
```

解決方法：

このメッセージは、OCSP サーバが起動に失敗するために表示されます。トラブル シューティングを行って問題を特定できます。

OCSP サーバをトラブル シューティングする方法

- *services.msc* から OCSP サーバを再起動して、レスポンダがハングしていないことを確認します。
- SCARVES と OCSP の間で日時が同じであることを確認します。 日時が異なる場合、エラー メッセージが表示されます。

LDAP サーバが応答しない

Windows、UNIX、および Linux で有効

症状：

スマート カード認証を使用しようとすると、LDAP の起動に失敗し、以下のエラー メッセージが表示されます。

```
[ERROR] [btpool0-2] [Manager.SCAuth]
com.wily.introscope.spec.server.user.SCException: LDAP Server not responding
```

解決方法：

LDAP サーバの起動に失敗する場合、*SCARVESconfig.xml* ファイルで指定された LDAP インスタンスにアクセスできません。

LDAP サーバをトラブル シューティングする方法

- LDAP 構成が適用可能な値で設定されていることを確認します。
- LDAP サーバが使用可能であることを確認します。
- LDAP サーバが開始され実行されていることを確認します。

受信 CRL エラー

Windows、UNIX、および Linux で有効

症状：

スマート カード認証で CRL オプションを使用しようとすると、*<SCARVES_HOME>/logs* ディレクトリ内にある *scarve.log* ファイルに以下のエラー メッセージが記録されます。

```
[ERROR] [btpool0-12] [Manager.SCAuth]
com.wily.introscope.spec.server.user.SCException: Certificate is expired or revoked
or not able to validate.
```

注: 無効な CRL ファイルの詳細は、Enterprise Manager ログ ファイルにログ記録されません。

解決方法：

CRL を使用するように構成された環境でスマート カードを使用して正常に認証できない場合は、その問題をトラブル シューティングします。

CRL をトラブル シューティングする方法

- *SCARVESconfig.xml* ファイルで *<SCARVES_HOME>/crls* ディレクトリにあるフォルダを指定していることを確認します。 指定されていない場合は、以下を実行します。
  1. *<SCARVES_HOME>/conf* に移動し、*SCARVESconfig.xml* を開きます。
  2. 指定された <daemon-name> の名前をコピーします。
  3. *<SCARVES_HOME>/crls* ディレクトリに移動し、<daemon-name> を名前に持つフォルダを作成します。
  4. このディレクトリに CRL ファイルをコピーし、SCARVES を再起動します。
- CRL デーモンに指定された絶対パスが正しいことを確認します。
  1. *<SCARVES_HOME>/conf* に移動し、*SCARVESconfig.xml* を開きます。
  2. CRL デーモンに指定されたパスが正しいことを確認します。
  3. これによって、SCARVES が、CRL ファイルが含まれる CRL フォルダを追跡できることが確認されます。

受信ユーザ LDAP 不在エラー

Windows、UNIX、および Linux で有効

症状：

スマート カード認証を使用しようとすると、以下のエラー メッセージが *<EM_HOME>/logs/IntroscopeEnterpriseManager.log* ファイルにログ記録されます。
受信ユーザ LDAP 不在エラー

解決方法：

この問題は、LDAP でユーザ ディレクトリにユーザの詳細が定義されていないときに発生します。 LDAP ユーザ ディレクトリを追加することにより、この問題を解決できます。

LDAP ユーザ ディレクトリを追加する方法

1. <SCARVES_HOME>/conf に移動し、*SCARVESconfig.xml* を開きます。
2. 以下の属性を定義します。

   facismilenumber

   使用される証明書の EDIPI 番号を入力します。

   uid

   属性に、Enterprise Manager およびユーザ ログイン資格情報に存在するユーザ名を入力します。
3. SCARVES を再起動します。

受信接続拒否エラー

Windows、UNIX、および Linux で有効

症状：

スマート カード認証を使用しようとすると、以下のエラー メッセージが表示されます。

```
[ERROR] [btpool0-2] [Manager.SCAuth]
com.wily.introscope.spec.server.user.SCException: Error getting user from given
certificate. java.net.ConnectException: Connection refused: connect
```

定義された SCARVES インスタンスが開始されないかアクセスできないとき、この Enterprise Manager エラーがログ記録されます。

解決方法：

- *<SCARVES_HOME>/conf* に移動し、*SCARVESconfig.xml* を開いて、SCARVES ホスト名が正しいことを確認します。

受信 LDAP 未構成エラー

Windows、UNIX、および Linux で有効

症状：

スマート カード認証を使用しようとすると、以下のエラー メッセージが Enterprise Manager ログ ファイルにログ記録されます。

```
[ERROR] [btpool0-0] [Manager.SCAuth]
com.wily.introscope.spec.server.user.SCException: LDAP Not configured
```

定義された SCARVES インスタンスが開始されないかアクセスできないとき、この Enterprise Manager エラーがログ記録されます。

解決方法：

- *<SCARVES_HOME>/conf* に移動し、*SCARVESconfig.xml* を開いて、このファイルに LDAP に関する内容があり、正確であることを確認します。

ハンドシェイク例外が Enterprise Manager で発生する

Windows、UNIX、および Linux で有効

症状：

スマート カード認証を使用しようとすると、ハンドシェイク例外が表示されます。

解決方法：

ハンドシェイク例外が発生するとき、トラブル シューティングを行って問題を特定できます。

ハンドシェイク例外をトラブル シューティングする方法

1. *<SCARVES_HOME>/conf* に移動し、*SCARVESconfigtemplate.xml* を開きます。
2. *SCARVESconfigtemplate.xml* 内に定義されたキーストア属性が正確であることを確認します。
3. 有効な自己署名証明書が SCARVES から、プロパティ ファイル内に定義されたキーストアにインポートされていることを確認します。
4. *<EM_HOME>¥config* 内のキーストアの属性が正確で、自己署名証明書が *<SCARVES_HOME>/keystores/daemoncert* ディレクトリにあることを確認します。 自己署名証明書が存在しない場合は、Enterprise Manager キーストアに証明書をエクスポートします。

詳細については、以下を参照してください。

証明書のロード (P. 211)
証明書コマンド (P. 212)