

# CA Access Control

統合ガイド

12.7



このドキュメント（組み込みヘルプシステムおよび電子的に配布される資料を含む、以下「本ドキュメント」）は、お客様への情報提供のみを目的としたもので、日本 CA 株式会社（以下「CA」）により随時、変更または撤回されることがあります。

CA の事前の書面による承諾を受けずに本ドキュメントの全部または一部を複製、譲渡、開示、変更、複製することはできません。本ドキュメントは、CA が知的財産権を有する機密情報です。ユーザは本ドキュメントを開示したり、  
(i) 本ドキュメントが関係する CA ソフトウェアの使用について CA とユーザとの間で別途締結される契約または (ii) CA とユーザとの間で別途締結される機密保持契約により許可された目的以外に、本ドキュメントを使用することはできません。

上記にかかわらず、本ドキュメントで言及されている CA ソフトウェア製品のライセンスを受けたユーザは、社内でユーザおよび従業員が使用する場合に限り、当該ソフトウェアに関連する本ドキュメントのコピーを妥当な部数だけ作成できます。ただし CA のすべての著作権表示およびその説明を当該複製に添付することを条件とします。

本ドキュメントを印刷するまたはコピーを作成する上記の権利は、当該ソフトウェアのライセンスが完全に有効となっている期間内に限定されます。いかなる理由であれ、上記のライセンスが終了した場合には、お客様は本ドキュメントの全部または一部と、それらを複製したコピーのすべてを破棄したことを、CA に文書で証明する責任を負いません。

準拠法により認められる限り、CA は本ドキュメントを現状有姿のまま提供し、商品性、特定の使用目的に対する適合性、他者の権利に対して侵害のないことについて、黙示の保証も含めいかなる保証もしません。また、本ドキュメントの使用に起因して、逸失利益、投資損失、業務の中断、営業権の喪失、情報の喪失等、いかなる損害（直接損害か間接損害かを問いません）が発生しても、CA はお客様または第三者に対し責任を負いません。CA がかかる損害の発生の可能性について事前に明示に通告されていた場合も同様とします。

本ドキュメントで参照されているすべてのソフトウェア製品の使用には、該当するライセンス契約が適用され、当該ライセンス契約はこの通知の条件によっていかなる変更も行われません。

本ドキュメントの制作者は CA です。

「制限された権利」のもとの提供: アメリカ合衆国政府が使用、複製、開示する場合は、FAR Sections 12.212、52.227-14 及び 52.227-19(c)(1)及び(2)、ならびに DFARS Section 252.227-7014(b)(3) または、これらの後継の条項に規定される該当する制限に従うものとします。

Copyright © 2012 CA. All rights reserved. 本書に記載された全ての製品名、サービス名、商号およびロゴは各社のそれぞれの商標またはサービスマークです。

## サードパーティに関する通知

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

© Copyright IBM Corporation 1999, 2002

All Rights Reserved

## サンプル スクリプトおよびサンプル SDK コード

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

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

## CA Technologies 製品リファレンス

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

- CA Access Control
- CA ControlMinder
- CA Single Sign-On (eTrust SSO)
- CA Top Secret®
- CA ACF2™
- CA Audit
- CA Network and Systems Management (CA NSM、旧 Unicenter NSM and Unicenter TNG)
- CA Software Delivery (旧 Unicenter Software Delivery)
- Unicenter Service Desk (旧 Unicenter Service Desk)
- CA User Activity Reporting Module (旧 [set the CALM variable for your book])
- Identity Manager

## ドキュメントの表記規則

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

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

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

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

### 例: コマンドの表記規則

以下のコードは、本書でのコマンド表記規則の使用方法を示しています。

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

この例の内容

- 標準的な等幅フォントで表示されているコマンド名 (`ruler`) は表示されているとおりに入力します。
- 斜体で表示されている `className` オプションは、クラス名 (`USER` など) のプレースホルダです。

- 2 番目の角かっこで囲まれた部分を指定しなくても、コマンドは実行できます。この部分は、オプションのオペランドを示します。
- オプションのパラメータ (props) を使用する場合は、キーワード *all* を選択するか、またはカンマで区切られたプロパティ名を 1 つ以上指定します。

## ファイル ロケーションに関する規則

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

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

## CA への連絡先

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

## マニュアルの変更点

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

- **CA ControlMinder REST API** -- カスタムまたはサードパーティプログラムと、エンタープライズ管理サーバ ユーザ インターフェースをバイパスする 共有アカウント管理 データベースの間の通信のための **REST** リクエストが追加されました。



# 目次

---

<b>第 1 章: 本書の内容</b>	<b>13</b>
<b>第 2 章: CA User Activity Reporting Module との統合</b>	<b>15</b>
CA User Activity Reporting Module について.....	15
CA User Activity Reporting Module 統合アーキテクチャ.....	16
CA User Activity Reporting Module 統合コンポーネント.....	17
CA ControlMinder と CA User Activity Reporting Module 間の監査データ フローの概要.....	19
CA ControlMinder に対する CA User Activity Reporting Module のセットアップ方法.....	21
コネクタの詳細.....	22
抑制ルールおよび要約ルール.....	23
コネクタ設定の要件.....	23
設定によるレポートエージェントへの影響.....	25
CA User Activity Reporting Module からのイベントのフィルタリング.....	27
SSL を使用した安全な通信.....	28
CA User Activity Reporting Module 統合のための監査ログ ファイルのバックアップ.....	28
CA User Activity Reporting Module 統合用の既存の Windows エンドポイントの設定.....	29
CA User Activity Reporting Module 統合用の既存の UNIX エンドポイントの設定.....	31
CA ControlMinder イベントのクエリおよびレポート.....	32
CA ControlMinder で CA User Activity Reporting Module レポートを有効にする方法.....	33
[set the CALM variable for your book] の trusted 証明書のキーストアへの追加.....	33
CA User Activity Reporting Module への接続の設定.....	35
監査コネクタの設定.....	37
<b>第 3 章: ObserveIT Enterprise との統合</b>	<b>39</b>
本書の内容.....	39
ObserveIT の統合について.....	40
統合をセットアップする方法.....	41
統合を準備する方法.....	42
セッション記録スクリプトのデプロイ.....	45
ObserveIT への接続の定義.....	46
セッションをログ記録する方法.....	48
セッションがログ記録される場所.....	49
セッションの再生.....	49

---

<b>第 4 章: RSA SecurID との統合</b>	<b>51</b>
CA Access Control エンタープライズ管理 を RSA SecurID と統合する方法	51
RSA SecurID がユーザ ログインを認証する仕組み	53
リバース プロキシサーバとしての Web サーバの設定	54
例: リバース プロキシサーバとしての Windows Server 2008 上での Internet Information Services 7.0 の設定	54
例: Apache Web Server .2.2.6 を Red Hat Enterprise Linux 5.0 上でリバース プロキシサーバとして設定	57
<b>第 5 章: 複数の LDAP サーバとの連携</b>	<b>59</b>
概要	59
複数の LDAP サーバを設定する方法	60
CA Directory ルータの設定	62
CA Directory ルータ定義のカスタマイズ	65
DIT を作成するための CA Directory データベースへの入力	68
<b>第 6 章: CA SiteMinder との統合</b>	<b>69</b>
概要	69
CA SiteMinder で CA ControlMinder ユーザを認証する方法	70
CA SiteMinder と統合する方法	71
例: エンタープライズ管理サーバでの Apache Web サーバプロキシプラグインの設定	73
例: Apache Web サーバ用の CA SiteMinder の設定	75
例: エンタープライズ管理サーバ用の CA SiteMinder の設定	77
例: CA SiteMinder Web エージェントの設定	78
例: エンタープライズ管理サーバを保護するための CA SiteMinder の設定	79
例: ユーザ認証に CA SiteMinder を使用するためのエンタープライズ管理サーバの設定	82
<b>第 7 章: CA ControlMinder REST API</b>	<b>85</b>
REST ベースの API	85
HTTP 動詞	86
例: HTTP 操作	87
REST-based 認証	88
スキーマの取得	88
アカウントの作成	89
アカウントの更新	91
アカウントの削除	93
アカウントの取得	94

---

アカウントの取得.....	95
アカウントのチェックイン.....	95
アカウントのチェックアウト.....	96
アカウントの <b>break glass</b> .....	97
パスワードのリセット.....	98
パスワードの自動リセット.....	99
エンドポイントの作成.....	100
エンドポイントの更新.....	102
エンドポイントの削除.....	103
エンドポイントの取得.....	103
エンドポイントの取得.....	104
エンドポイント タイプの取得.....	104
アカウント リクエストの作成.....	105
アカウント リクエストの削除.....	106
リクエストするアカウントパスワードの取得.....	107
アカウント リクエストの取得.....	108



# 第 1 章：本書の内容

---

このガイドでは、CA Access Control をサードパーティ ソフトウェアに統合する方法について説明します。これらのソフトウェアには、CA User Activity Reporting Module、CA Directory、CA SiteMinder、RSA SecurID、および ObserveIT Enterprise が含まれます。このガイドの章は、CA Access Control のみに適用されます。

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



# 第 2 章: CA User Activity Reporting Module との統合

---

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 User Activity Reporting Module について \(P. 15\)](#)

[CA User Activity Reporting Module 統合アーキテクチャ \(P. 16\)](#)

[CA ControlMinder に対する CA User Activity Reporting Module のセットアップ方法 \(P. 21\)](#)

[設定によるレポート エージェントへの影響 \(P. 25\)](#)

[CA User Activity Reporting Module 統合用の既存の Windows エンドポイントの設定 \(P. 29\)](#)

[CA User Activity Reporting Module 統合用の既存の UNIX エンドポイントの設定 \(P. 31\)](#)

[CA ControlMinder イベントのクエリおよびレポート \(P. 32\)](#)

[CA ControlMinder で CA User Activity Reporting Module レポートを有効にする方法 \(P. 33\)](#)

## CA User Activity Reporting Module について

CA User Activity Reporting Module は、IT のコンプライアンスおよび保証に重点的に取り組んでいます。これを使用することによって、IT アクティビティを収集し、標準化し、集約して報告し、コンプライアンス違反が発生した場合にアクションを必要とするアラートを生成することができます。異なるセキュリティ デバイスおよびセキュリティ以外のデバイスからデータを収集できます。

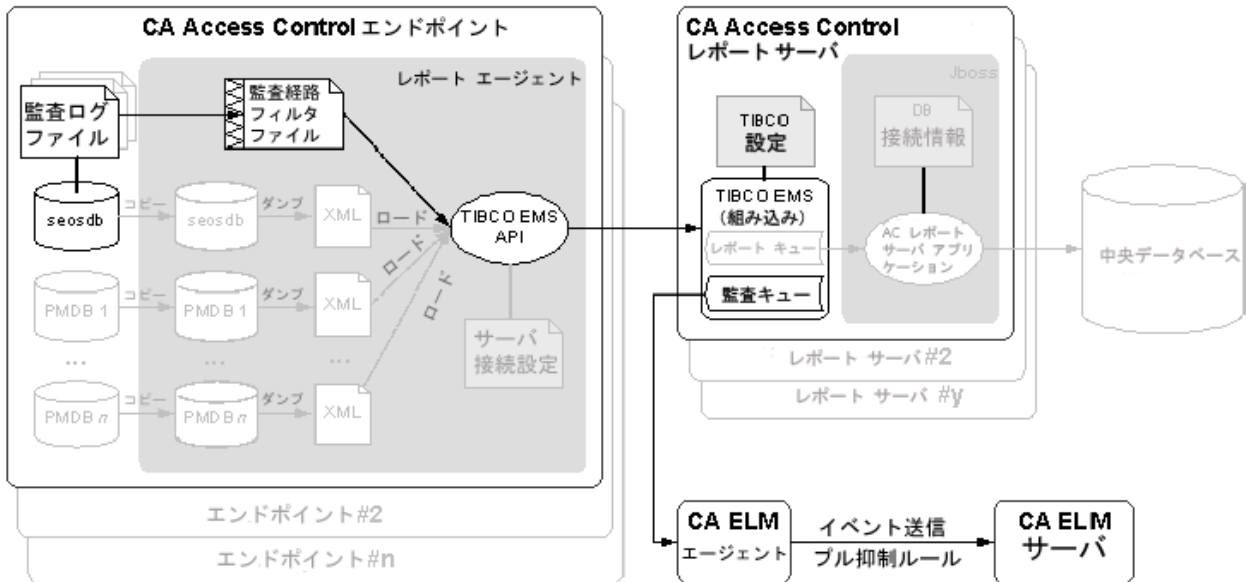
## CA User Activity Reporting Module 統合アーキテクチャ

CA User Activity Reporting Module との統合により、それぞれのエンドポイントから CA ControlMinder 監査イベントを送信して、CA User Activity Reporting Module で収集とレポートを実行できます。

ローカルエンドポイント上の監査ファイルから配布サーバ上のリモート監査キューに、監査イベントを送信するように CA ControlMinder を設定できます。次に、CA User Activity Reporting Module コネクタが監査キューに接続して、そこからイベント（メッセージ）をプルできるように設定します。CA User Activity Reporting Module はこれらのイベントを処理して、CA User Activity Reporting Module サーバに送信します。

CA ControlMinder インストールは CA User Activity Reporting Module 統合をサポートします。

以下の図に、CA User Activity Reporting Module 統合コンポーネントのアーキテクチャを示します。



上の図は、以下のことを示します。

- CA ControlMinder データベース (seosdb) が含まれる各エンドポイントには、レポートエージェント コンポーネントがインストールされています。
- レポート エージェントはエンドポイントから監査データを収集し、配布サーバに送信します。

- 配布サーバは監査データを監査キューに蓄積します。
- CA User Activity Reporting Module エージェントは監査キューからイベントを収集し、処理のために CA User Activity Reporting Module サーバに送信します。

**注:** CA User Activity Reporting Module 統合はレポートするサービス コンポーネントに依存します。そのため、CA User Activity Reporting Module 統合では使用されないその他のレポート サービスのコンポーネントや機能もアーキテクチャに含まれます。そのようなコンポーネントや機能は、図中で淡色表示されています。

**注:** デフォルトでは、CA Access Control エンタープライズ管理 はエンタープライズ管理サーバに配布サーバをインストールします。可用性を高めるには、別のコンピュータに配布サーバをインストールします。

## CA User Activity Reporting Module 統合コンポーネント

CA User Activity Reporting Module 統合では、以下の CA ControlMinder コンポーネントを使用します。これらのコンポーネントは、CA ControlMinder エンタープライズ レポートング サービスの一部です。

- レポート エージェントは、CA ControlMinder または UNAB の各エンドポイント上で実行される Windows サービスまたは UNIX デーモンで、配布サーバ上にある設定されたメッセージ キューのキューに情報を送信します。CA User Activity Reporting Module 統合の場合、レポート エージェントが監査ログ ファイルからエンドポイント監査メッセージを定期的に収集し、収集したイベントを設定済みの配布サーバ上にある監査キューに送信します。
- メッセージ キューは、配布サーバのコンポーネントの 1 つで、レポート エージェントが送信するエンドポイント情報を受信するように設定されています。レポートに関しては、メッセージ キューは、CA ControlMinder Web サービスを使用して、エンドポイント データベースのスナップショットを中央データベースに転送します。冗長性およびフェールオーバーを実現するために、複数の配布サーバを使用して情報の収集および転送を行うことができます。

**注:** デフォルトでは、CA Access Control エンタープライズ管理 はエンタープライズ管理サーバに配布サーバをインストールします。

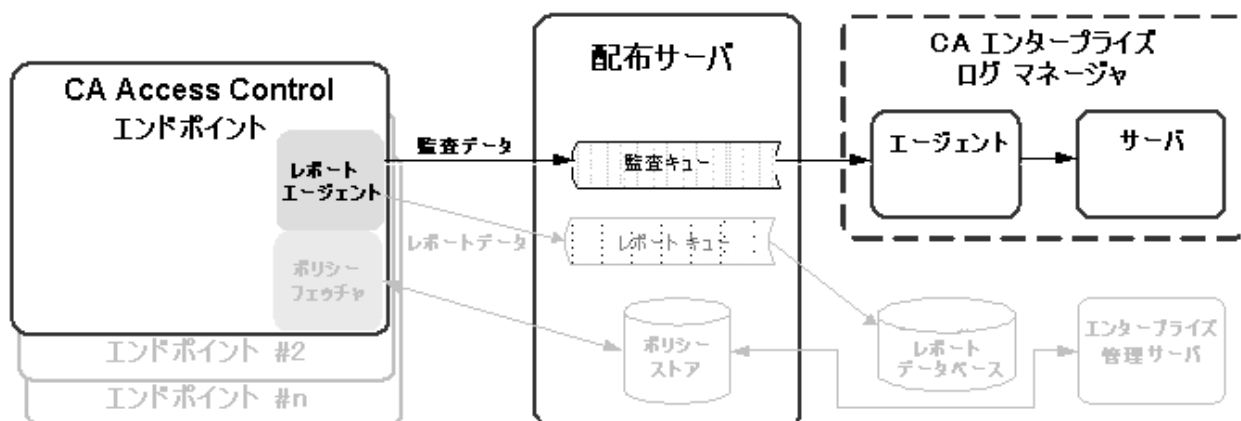
CA User Activity Reporting Module 統合では次の CA User Activity Reporting Module コンポーネントも使用します。

- CA User Activity Reporting Module エージェントは、コネクタによって設定される汎用サービスであり、そのそれぞれが単一のイベントソースから生のイベントを収集して、そのイベントを処理のために CA User Activity Reporting Module サーバに送信します。CA ControlMinder 監査データの場合、エージェントが CA ControlMinder コネクタをデプロイします。
- CA ControlMinder コネクタは、CA ControlMinder 監査イベント ソース用の使いやすい CA User Activity Reporting Module 統合です。コネクタによって、CA ControlMinder 配布サーバからの生のイベント収集が可能になり、変換されたイベントをイベント ログストアにルールベースで送信できるようになります。イベント ログストアでイベントはホットデータベースに挿入されます。
- 収集サーバは、受信イベント ログの調整、ホットデータベースへの受信イベント ログの挿入、設定サイズに達したホット データベースのウォーム データベースへの圧縮、関連管理サーバへのウォーム データベースの定期的な自動アーカイブを行う CA User Activity Reporting Module サーバです。

注: CA User Activity Reporting Module コンポーネントの詳細については、CA User Activity Reporting Module のマニュアルを参照してください。

## CA ControlMinder と CA User Activity Reporting Module 間の監査データフローの概要

CA ControlMinder が CA User Activity Reporting Module とどのように統合されるか、また、この統合の設定に関して何を検討すべきか理解するには、最初に CA ControlMinder と CA User Activity Reporting Module の間の監査データのフローを検討する必要があります。以下の図は、CA ControlMinder が監査イベントを配布サーバ上のメッセージキューにルーティングする方法を示しています。配布サーバ上で、CA User Activity Reporting Module エージェントの CA ControlMinder コネクタによってイベントのプル、マップ、および変換が行われ、CA User Activity Reporting Module サーバに送信されます。



1. レポート エージェントはローカルエンドポイントの監査ファイルから監査イベントを収集し、フィルタリングポリシーを適用し、配布サーバ上にある監査キューにイベントを格納します。
2. CA User Activity Reporting Module エージェントによってデプロイされた CA User Activity Reporting Module コネクタが監査キューと接続し、そこからイベント（メッセージ）をプルします。

3. CA User Activity Reporting Module コネクタ/エージェントは、データマッピングおよび解析ファイルを使用して Common Event Grammar (CEG) にイベントをマップし、CA User Activity Reporting Module サーバにイベントをルーティングする前に、抑制および要約ルールを適用します。
4. CA User Activity Reporting Module サーバはイベントを受け取り、場合により、イベントを格納する前に追加の抑制および要約ルールを適用します。

注: CA User Activity Reporting Module の動作の詳細については、CA User Activity Reporting Module のマニュアルを参照してください。

## CA ControlMinder に対する CA User Activity Reporting Module の セットアップ方法

CA User Activity Reporting Module を使用して、すべての CA ControlMinder エンドポイントからの監査データを含むレポートを作成するには、最初にエンタープライズ レポートを実装します。CA User Activity Reporting Module との統合の前に、エンタープライズ レポートを実装する必要があります。これは、エンタープライズ レポートによってエンドポイントでレポート エージェントが有効になったためです。エンタープライズ レポートを実装したら、CA User Activity Reporting Module を CA ControlMinder 用に設定します。

CA ControlMinder に対して CA User Activity Reporting Module をセットアップするには、以下の手順に従います。

1. CA User Activity Reporting Module サーバをインストールします。  
**注:** 詳細については、「*CA User Activity Reporting Module Implementation Guide*」を参照してください。

2. CA User Activity Reporting Module エージェントを配布サーバ上またはその近辺にインストールします。

エージェントは配布サーバからアクセス可能であり、指定されたポートを使用して、配布サーバと通信する必要があります。CA User Activity Reporting Module サーバにもアクセス可能である必要があります。

**注:** CA User Activity Reporting Module エージェントをインストールする前に、オペレーティング システムが [set the CALM variable for your book] エージェントをサポートしていることを確認してください。エージェントのインストールの詳細については、「*CA User Activity Reporting Module Agent Installation Guide*」を参照してください。

3. CA Access Control エンタープライズ管理 をインストールします。

**注:** 詳細については、「*実装ガイド*」を参照してください。

4. エージェントの新しいコネクタを作成します。

CA User Activity Reporting Module エージェントをインストールして CA User Activity Reporting Module サーバとの通信を開始したら、新しいコネクタを作成し、そのコネクタが CA ControlMinder のイベント ソース（配布サーバ上の監査キュー）にアクセスできるように設定する必要があります。

注: 以下のトピックでは、統合が成功するために設定する必要がある、コネクタの詳細およびコネクタ設定要件など、CA ControlMinder のイベント収集に必要な設定について説明します。F コネクタの作成方法の詳細については、「*CA User Activity Reporting Module Administration Guide*」および「オンラインヘルプ」をご覧ください。

5. CA Access Control エンタープライズ管理 から CA User Activity Reporting Module への接続を作成します。
6. (オプション) 監査コネクタを設定します。
7. 監査データ収集用の CA ControlMinder エンドポイントを設定します。

### コネクタの詳細

コンピュータに CA User Activity Reporting Module エージェントをインストールすると、そのコンピュータは CA User Activity Reporting Module サーバ管理インターフェースに表示されます (たとえば、「デフォルトエージェントグループ」のコンピュータを表示するには、[管理] - [ログ収集] - [エージェントエクスペローラ] - [デフォルトエージェントグループ] をクリックし、*computer\_name* をクリックします)。このとき、コネクタを作成する必要があります。このトピックでは、コネクタ作成ウィザードの [コネクタの詳細] ページで行う必要がある設定について説明します。

#### 統合

テンプレートとして使用する統合を指定します。

適切な CA ControlMinder 統合を選択します。

例: `AccessControl_R12SP5_TIBCO`。

任意でコネクタ名を変更して、説明を追加することもできます。さらに、コネクタによって処理されるイベントに抑制ルールを適用できます。

注: イベント収集をカスタマイズできるその他のオプション設定については、「*CA User Activity Reporting Module Administration Guide*」および「オンラインヘルプ」を参照してください。

## 抑制ルールおよび要約ルール

コネクタを作成してコネクタの詳細を指定したら、任意でコネクタ作成ウィザードの [抑制ルールの適用] ページで抑制ルールを適用できます。

CA ControlMinder の抑制および要約ルールに関する理想モデルの名前は、ホスト IDS/IPS です。ルールを作成する場合、イベントを特定するために必要に応じてイベント カテゴリ、イベント クラス、およびイベントアクションの値を選択してください。

**注:** イベント収集をカスタマイズできるその他のオプション設定については、「*CA User Activity Reporting Module Administration Guide*」および「オンラインヘルプ」を参照してください。フィールドの意味や個々の値の詳細については、CA User Activity Reporting Module オンラインヘルプの「Common Event Grammar Reference」を参照してください。

## コネクタ設定の要件

コネクタを作成してコネクタの詳細を指定したら、コネクタを設定できます。このトピックでは、イベント収集を開始するために、コネクタ作成ウィザードの [コネクタ設定] ページで行う必要がある設定について説明します。

**注:** イベント収集をカスタマイズできるその他のオプション設定については、「*CA User Activity Reporting Module Administration Guide*」および「オンラインヘルプ」を参照してください。

### TIBCO サーバ

メッセージキュー (TIBCO サーバ) のホスト名または IP アドレスを次の形式で指定します。

```
Protocol://server IP or name:Port number
```

メッセージキューは CA Access Control エンタープライズ管理にインストールされます。

- 以下の値を定義します。

```
ssl://ACentmsserver:7243
```

ポート値および通信方法は CA Access Control エンタープライズ管理が使用するデフォルトポートです。CA Access Control エンタープライズ管理をインストールした後に別の値を設定した場合、そのポートと通信方法の値を使用します。

#### TIBCO ユーザ

メッセージキューの認証用のユーザ名を指定します。CA ControlMinder では、「reportserver」という名前のデフォルトユーザを定義します。

#### TIBCO パスワード

メッセージキューの認証用のパスワードを指定します。CA Access Control エンタープライズ管理のインストール時に、[通信パスワード] ダイアログボックスで定義したパスワードを入力します。

#### イベントログ名

イベントソースのログ名を指定します。

デフォルトの「CA ControlMinder」を使用します。

#### ポーリング間隔

メッセージキューが使用不可になったり切断された場合に、イベントをポーリングするまでエージェントが待機する秒数を指定します。

#### SourceName

メッセージキューの識別子を指定します。

デフォルトの「queue\_audit」を使用します。

#### TIBCO キュー

ログセンサによるメッセージ（イベント）の読み取り元であるメッセージキューの名前を指定します。

デフォルトの「queue/audit」を使用します。

#### コレクションスレッドの数

メッセージキューのメッセージを読み取るためにログセンサが生成するスレッドの数を指定します。

この値を調整する場合、メッセージキュー内のイベントの数および CA User Activity Reporting Module エージェントシステムの CPU を考慮する必要があります。

**制限：**最小値は 1 です。ログセンサが生成できるスレッドの最大数は 20 です。

## 設定によるレポート エージェントへの影響

CA User Activity Reporting Module 統合の場合、レポート エージェントが監査ログ ファイルからエンドポイント監査メッセージを定期的に収集し、そのイベントを設定済み配布サーバ上の監査キューにルーティングします。レポート エージェントの設定をチューニングすると、パフォーマンスを向上させることができます。

**注:** レポート エージェントは CA ControlMinder エンタープライズ レポート サービスの一部であり、エンドポイント レポートの目的でデータベース スナップショットの送信も担当します。このプロセスは、CA User Activity Reporting Module への監査イベント ルーティングのためにレポート エージェントが行うアクションのみを示します。

監査収集を有効にした場合（`audit_enabled` 設定を 1 に設定）、レポート エージェントでは以下を実行します。

- エンドポイント監査ファイルを読み取ってメモリにコミットすることによって、新しい監査レコードを収集します。

レポート エージェントは、`audit_read_chunk` 設定に定義された監査レコードの数を読み取り、`audit_sleep` 設定に定義された間だけ待機してから、監査ファイルを再度読み取ります。レポート エージェントは、アクティブな監査ログおよびすべてのバックアップ監査ファイル内の読み取られていないレコードを読み取ります。そして、監査フィルタ ファイルに定義した監査フィルタ（`audit_filter` 構成設定）を通過するレコードをメモリにコミットします。

- メモリにある監査レコードのグループを `audit_queue` 設定に定義された配布サーバメッセージ キューに送信します。

次のいずれかの場合に該当すると、レポート エージェントは監査レコードを送信します。

- メモリのレコードの数が `audit_send_chunk` 構成設定で定義された数に達する。
- 最後の監査レコードが送信されてから経過した時間が、`audit_timeout` 設定で定義された間隔に等しい。

### 例: 監査収集とルーティングに関するレポートエージェントのデフォルト設定

この例は、レポートエージェントのデフォルト構成設定がどのように設定されているか、その設定がどのような環境に適するか、およびその設定がパフォーマンスにどのように影響するかを示します。

平均的な環境で、秒あたりのイベント数 (EPS) 30 を想定しています。したがって、レポートエージェントは毎秒通過する 30 のイベントを読み取ります。その他の実行中のアプリケーションに対する影響 (CPU 使用およびコンテキストスイッチ) を減らすために、以下のようにレポートエージェントのイベント読み取りを 10 秒ごとに 300 としています。

```
audit_sleep=10  
audit_read_chunk=300
```

レポートエージェントと配布サーバ間のメッセージ伝送のために CA ControlMinder が使用するメッセージバスは、短い間隔で小さなパケットを処理するよりも長い間隔で送信される大きなパケットを処理するのに適しています。次の構成設定は、レポートエージェントが収集する監査レコードの数が定義された数に達すると、それらのレコードをレポートエージェントが配布サーバに送信するように指定しています。1 秒間 30 イベントとすると、レポートエージェントがおよそ 1 分 (60 秒) 間隔で監査レコードを送信するようにするには、レポートエージェントを次のように設定する必要があります。

```
audit_send_chunk=1800
```

ただし、夜間などの時間帯で 1 秒間 30 未満のイベントになると、1 分間 1800 未満のイベントになります。レポートエージェントが今後も定期的に監査レコードを配布サーバに送信するためには、監査レコード送信間隔を次のとおり最大 5 分に設定します。

```
audit_timeout=300
```

## CA User Activity Reporting Module からのイベントのフィルタリング

フィルタ ファイルを使用して、CA ControlMinder がログ ファイル内のすべての監査レコードを CA User Activity Reporting Module に送信するのを防ぐことができます。フィルタ ファイルは、CA User Activity Reporting Module に送信されない監査レコードを指定します。

**注:** このフィルタ ファイルによって、指定された監査イベントを CA ControlMinder が配布サーバに送信しないようにしますが、CA ControlMinder が監査イベントをローカル ファイルに書き込むことを防ぐわけではありません。ローカルの監査ファイルから監査イベントを除外するには、logmgr セクションの AuditFiltersFile 設定に定義されているファイルでフィルタ ルールを変更します（デフォルトでは audit.cfg）。

CA User Activity Reporting Module からのイベントをフィルタするには、エンドポイント上の監査フィルタ ファイルを編集します。同じフィルタ ルールを複数のエンドポイントに適用する場合、監査フィルタリング ポリシーを作成し、そのポリシーを対象のエンドポイントへ割り当てることをお勧めします。

**注:** 詳細については、「リファレンス ガイド」を参照してください。

### 例: 監査フィルタ ポリシー

監査フィルタ ポリシーの例を以下に示します。

```
env config
er config auditrouteflt.cfg line+("FILE;*;*;R;P")
```

この例は、次の行を auditrouteflt.cfg ファイルに書き込みます。

```
FILE;*;*;R;P
```

この行は、ファイル リソースへの読み取りアクセスのためにアクセサが行った許可された試行を記録した監査レコードをフィルタします。CA ControlMinder はこの監査レコードを配布 サーバに送信しません。

## SSL を使用した安全な通信

CA Access Control エンタープライズ管理 をインストールする場合、SSL を使用して配布サーバとレポート エージェントの間の通信を保護するか、通信を保護しないか選択できます。いずれのオプションを選択した場合でも、エンドポイントにレポート エージェントをインストールするときと同じオプションを指定する必要があります。

たとえば、SSL を使用してレポート エージェントと配布サーバ間の通信を暗号化する場合（デフォルト）、レポート エージェントが配布サーバと通信するときに必要なパスワードなどの認証情報を、CA Access Control エンタープライズ管理 のインストール時に提供する必要があります。

これは、CA User Activity Reporting Module エージェントの [Connector Configuration] ページで、エンドポイントの CA ControlMinder レポート エージェントを設定するときに指定するパスワードです。

レポート エージェントをインストールするときに、同じ情報を指定する必要があります。正しい証明書とパスワード情報を提供できるレポート エージェントのみが、配布サーバ上の監査キューにイベントを書き込むことができ、書き込まれたイベントは CA User Activity Reporting Module によって取得されます。

## CA User Activity Reporting Module 統合のための監査ログ ファイルのバックアップ

監査データを収集するために、レポート エージェントは構成設定に従って CA ControlMinder 監査ログ ファイルを読み取ります。レポート エージェントは、設定された時間間隔で設定された数の監査レコードを監査ログ ファイルから読み取ります。デフォルトのレガシーインストールの場合、またはインストール時に監査ログルーティングを有効にしていない場合、CA ControlMinder はサイズによる監査ログ バックアップ ファイルのみを保存します。監査ログが設定された最大サイズに達するたびに、既存の監査ログ バックアップ ファイルが上書きされてバックアップ ファイルが作成されます。そのため、レポート エージェントがすべてのレコードを読み取る前に、バックアップ ファイルが上書きされる可能性があります。

CA ControlMinder が監査ログ ファイルのタイムスタンプ付きバックアップを保存するように設定することを強くお勧めします。こうすると、保存されるべき監査ログ ファイルの設定された最大数に達するまで、CA ControlMinder はバックアップの監査ログ ファイルを上書きしません。これは、エンドポイント上へのインストール時に、監査ログルーティング サブ機能を有効にした場合のデフォルト設定です。

### 例: 監査ログ バックアップの設定

この例は、推奨の構成設定がどのように CA User Activity Reporting Module 統合に影響するかを示します。エンドポイント上へのインストール時に、監査ログルーティング サブ機能を有効にすると、CA ControlMinder は logmgr セクションの以下の環境設定を行います。

```
BackUp_Date=yes  
audit_max_files=50
```

この場合、CA ControlMinder は監査ログ ファイルの各バックアップ コピーにタイムスタンプを付け、最大 50 のバックアップ ファイルを保存します。これによって、レポート エージェントがすべての監査レコードをファイルから読み取ったり、必要に応じてバックアップ ファイルを安全に保管するために手動でコピーしたりすることが行いやすくなります。

**重要:** `audit_max_files` を 0 に設定すると、CA ControlMinder はバックアップ ファイルを削除せずに蓄積し続けます。バックアップ ファイルを外部プロセスによって管理する場合、CA ControlMinder がデフォルトでバックアップ ファイルを保護することに注意してください。

## CA User Activity Reporting Module 統合用の既存の Windows エンドポイントの設定

CA Access Control エンタープライズ管理 のインストールおよび設定の完了後、監査データを配布サーバに送信するようにエンドポイントを設定することができます。これを行うには、レポート エージェントを有効にして設定します。

**注:** CA ControlMinder をインストールすると、監査データの収集および送信のためにエンドポイントを設定することが可能になります。この手順は、インストール時にこのオプションを設定しなかった場合に、監査データ送信のために既存のエンドポイントを設定する方法です。

### CA User Activity Reporting Module 統合用に既存の Windows エンドポイントを設定する方法

1. [スタート] - [コントロールパネル] - [プログラムの追加と削除] を選択します。  
[プログラムの追加と削除] ダイアログ ボックスが表示されます。
2. プログラム リストをスクロールして **CA ControlMinder** を選択します。
3. [変更] をクリックします。

CA ControlMinder のインストール ウィザードが表示されます。

レポート エージェント機能および監査ルーティング サブ機能が有効になるように、CA ControlMinder インストールを変更するウィザードのプロンプトに従います。

また、監査ログ ファイルのタイムスタンプ付きバックアップを保存するように指定していることを確認してください。

**注:** レポート エージェントおよび監査ルーティングを有効にした後、パフォーマンス関連の CA ControlMinder 構成設定を変更できます。この操作を行う前に、[レポート エージェントが監査イベントを収集して配布サーバにルーティングする方法について理解しておく必要があります \(P. 25\)](#)。レポート エージェントの構成設定の詳細については、「リファレンス ガイド」を参照してください。

## CA User Activity Reporting Module 統合用の既存の UNIX エンドポイントの設定

CA Access Control エンタープライズ管理 のインストールおよび設定の完了後、監査データを配布サーバに送信するようにエンドポイントを設定することができます。これを行うには、レポート エージェントを有効にして設定します。

**注:** CA ControlMinder をインストールすると、監査データの収集および送信のためにエンドポイントを設定することが可能になります。この手順は、インストール時にこのオプションを設定しなかった場合に、監査データ送信のために既存のエンドポイントを設定する方法です。

以下の手順に従います。

1. `ACSharedDir/lbin/report_agent.sh` を実行します。

```
report_agent config -server hostname [-proto {ssl|tcp}] [-port port_number  
[-rqueue queue_name] -audit -bak
```

設定オプションを省略すると、デフォルト設定が使用されます。

**注:** `report_agent.sh` スクリプトの詳細については、「リファレンス ガイド」を参照してください。

2. データベース内に `+reportagent` ユーザを作成します。

このユーザは、ADMIN 属性および AUDITOR 属性、ならびにローカル端末への書き込みアクセス権を有する必要があります。また、`epassword` をレポート エージェント共有秘密キー（配布サーバのインストール時に定義）に設定する必要があります。

3. レポート エージェント プロセス用に SPECIALPGM を作成します。

SPECIALPGM は、`root` ユーザを `+reportagent` ユーザにマップします。

**注:** レポート エージェントおよび監査ルーティングを有効にした後、パフォーマンス関連の CA ControlMinder 構成設定を変更できます。この操作を行う前に、[レポート エージェントが監査イベントを収集して配布サーバにルーティングする方法について理解しておく必要があります \(P. 25\)](#)。レポート エージェントの構成設定の詳細については、「リファレンス ガイド」を参照してください。

### 例: selang を使用した CA User Activity Reporting Module 統合のための UNIX エンドポイントの設定

次の `selang` コマンドは、レポート エージェントを有効にして設定した場合に、どのように必要なレポート エージェント ユーザを作成し、レポート エージェント プロセスの特別なセキュリティ権限を指定するかを示します。

```
eu +reportagent admin auditor logical epassword(Report_Agent) nonative
auth terminal (terminal101) uid( +reportagent) access(w)
er specialpgm (/opt/CA/AcessControl/bin/ReportAgent) Seosuid(+reportagent) ¥
Nativeuid(root) pgmtype(none)
```

## CA ControlMinder イベントのクエリおよびレポート

CA ControlMinder のクエリ、レポート、およびアクション警告は、CA User Activity Reporting Module インターフェースの [Server Resource Protection] タグにまとめられています。

注: 詳細については、<http://ca.com/jp/support> にある [CA User Activity Reporting Module 製品ページ](#) を参照してください。

## CA ControlMinder で CA User Activity Reporting Module レポートを有効にする方法

CA Access Control エンタープライズ管理 で CA User Activity Reporting Module レポートを表示できるようにするには、CA User Activity Reporting Module レポートを有効にし、CA User Activity Reporting Module 証明書をエクスポートして追加し、CA Access Control エンタープライズ管理 から CA User Activity Reporting Module への接続を設定する必要があります。

1. 高度な設定により、CA User Activity Reporting Module レポートを有効にします。
2. [CA User Activity Reporting Module の trusted 証明書をエクスポートして、キーストアに追加します。](#) (P. 33)
3. [\[set the CALM variable for your book\] への接続を設定します](#) (P. 35)。
4. [\(オプション\) 監査コレクタを設定します](#) (P. 37)。

共有アカウント管理 監査イベントを CA User Activity Reporting Module に送信する場合は、監査コレクタを設定します。

### [set the CALM variable for your book] の trusted 証明書のキーストアへの追加

[set the CALM variable for your book] レポートは、トラステッド証明書を使用して認証されます。証明書は、レポートに表示されている情報がトラステッド [set the CALM variable for your book] ソースのものであることを証明します。トラステッド [set the CALM variable for your book] ソースはデータの信頼性を証明します。

CA Access Control エンタープライズ管理 で [set the CALM variable for your book] を表示するには、まず証明書をエクスポートし、次にそれをキーストアに追加します。

#### [set the CALM variable for your book] の trusted 証明書のキーストアへの追加方法

1. Web ブラウザで [set the CALM variable for your book] サーバの URL を「`https://host:port`」形式で入力します。  
セキュリティの警告ダイアログ ボックスが開きます。
2. [証明書を表示] をクリックします。  
[証明書] ダイアログ ボックスが表示されます。

3. [詳細] - [ファイルへのコピー] をクリックします。  
[証明書のエクスポート] ウィザードが表示されます。
4. 以下の指示に従って、ウィザードを完了します。
  - **ファイル形式のエクスポート - Base-64 エンコード X.509 (.CER)** を選択します。
  - **エクスポートするファイル** - エクスポートされた証明書ファイルの完全パス名を定義します。  
たとえば、「C:¥certificates¥computer.base64.cer」のように指定します。

エクスポートが正常に完了したことを通知するメッセージが表示されます。

5. 証明書をキーストアにインポートします。以下に例を示します。

```
C:¥jdk1.5.0¥jre¥lib¥security>c:¥jdk1.5.0¥bin¥keytool.exe -import -file
computer.base64.cer -keystore
C:¥jboss-4.2.3.GA¥server¥default¥deploy¥IdentityMinder.ear¥custom¥ppm¥truststore¥ssl.keystore
```

6. キーストアのパスワードを入力します。デフォルトのパスワードは、「secret」です。
7. [はい] をクリックして、証明書を信頼します。  
証明書がキーストアに追加されます。

## CA User Activity Reporting Module への接続の設定

CA Access Control エンタープライズ管理 は CA ControlMinder の関連情報を記載したレポートを表示するために CA User Activity Reporting Module と通信します。これらのレポートを表示するには、CA User Activity Reporting Module への接続を設定する必要があります。

### CA User Activity Reporting Module への接続の設定方法

1. CA Access Control エンタープライズ管理 で、以下の手順を実行します。
  - a. [システム] をクリックします。
  - b. [接続管理] サブタブをクリックします。
  - c. 左側のタスク メニューで、UARM ツリーを展開します。  
[CA User Activity Reporting Module 接続の管理] タスクが使用可能なタスク リストに表示されます。
2. [CA User Activity Reporting Module 接続の管理] をクリックします。  
[CA User Activity Reporting Module 接続の管理 : *PrimaryCALMServer*] タスク ページが表示されます。
3. ダイアログ ボックスの以下のフィールドに入力します。以下のフィールドには、説明が必要です。

#### 接続名

CA User Activity Reporting Module 接続の名前を識別します。

#### 説明

(オプション) この接続に関する説明を定義します。

#### ホスト名

CA Access Control エンタープライズ管理 の動作対象となる CA User Activity Reporting Module の名前を定義します。

例 : host1.comp.com

#### ポート番号

CA User Activity Reporting Module ホストが通信に使用するポートを定義します。

デフォルト : 5250

### 認証局署名済み SSL 証明書

CA User Activity Reporting Module への接続に認証局が署名した SSL 証明書を使用するかどうかを指定します。

#### 証明書名

証明書の名前を定義します。

#### パスワード

証明書のパスワードを定義します。

4. [サブミット] をクリックします。

CA Access Control エンタープライズ管理 が CA User Activity Reporting Module の接続設定を保存します。

### 例: CA User Activity Reporting Module 証明書情報の取得

以下の例では、CA Access Control エンタープライズ管理 内で CA User Activity Reporting Module 接続設定を作成および管理する際に必要な CA User Activity Reporting Module 証明書情報の取得方法を示しています。

1. 以下の形式で、Web ブラウザに CA User Activity Reporting Module の URL を入力します。

`https://host:port/spin/calmap/api/products.csp`

例: `https://localhost:5250/spin/calmap/api/products.csp`

2. 有効なユーザ名とパスワードを入力して、CA User Activity Reporting Module にログインします。
3. CA User Activity Reporting Module に証明書を登録するための登録オプションを選択します。

新しい製品の登録画面が表示されます。

4. 証明書名とパスワードを入力し、登録を選択します。

証明書の登録が正常に完了したことを通知するメッセージが表示されます。

## 監査コレクタの設定

CA Access Control エンタープライズ管理 は、共有アカウント管理 監査イベントなどの監査イベントを収集し、中央データベースに格納します。監査イベントを CA User Activity Reporting Module に送信するように、CA Access Control エンタープライズ管理 を設定できます。

### 監査コレクタの設定方法

1. CA Access Control エンタープライズ管理 で、以下の手順を実行します。
  - a. [システム] をクリックします。
  - b. [接続管理] サブタブをクリックします。
  - c. 左側のタスク メニューで、**UARM** ツリーを展開します。  
[監査コレクタの作成] タスクが使用可能なタスク リストに表示されます。
2. [監査コレクタの作成] をクリックします。  
[監査コレクタの作成： 監査コレクタ検索画面] が表示されます。
3. (オプション) 既存の監査コレクタのコピーを以下のように作成します。
  - a. [UARM 送信者タイプのオブジェクトのコピーの作成] を選択します。
  - b. 検索属性を選択し、フィルタ値を入力し、[検索] をクリックします。  
フィルタ条件に一致する **UARM** 送信者のリストが表示されます。
  - c. 新規監査コレクタのベースとして使用するオブジェクトを選択します。
4. [OK] をクリックします。  
[監査コレクタの作成] タスク ページが表示されます。監査コレクタを既存のオブジェクトから作成した場合、ダイアログ ボックスのフィールドには、既存オブジェクトの値がすでに入力されています。

5. ダイアログ ボックスの以下のフィールドに入力します。以下のフィールドには、説明が必要です。

#### ジョブの有効化

監査コレクタを有効にするかどうかを指定します。

#### 名前

監査コレクタの名前を定義します。

#### キュー JNDI

CA Access Control エンタープライズ管理 が監査イベント メッセージを送信するメッセージキューの名前を定義します。

例: *queue/audit*

#### スリープ

データベース クエリの間隔を分単位で定義します。

デフォルト: 1

#### タイムアウト

監査イベント メッセージのメッセージキューへの送信に関して、コレクタのタイムアウト期間を分単位で定義します。

デフォルト: 10

注: このタイムアウト期間が経過すると、キュー内のメッセージ数が [メッセージブロック サイズ] フィールドで定義されたレベルに達していなくとも、コレクタはメッセージを送信します。

#### メッセージブロック サイズ

データベースに蓄積するメッセージの最大数を定義します。この数に達すると、メッセージはキューに送信されます。

デフォルト: 100

6. [サブミット] をクリックします。

CA Access Control エンタープライズ管理 は監査コレクタを作成します。

# 第 3 章: ObserveIT Enterprise との統合

---

このセクションには、以下のトピックが含まれています。

[本書の内容 \(P. 39\)](#)

[ObserveIT の統合について \(P. 40\)](#)

[統合をセットアップする方法 \(P. 41\)](#)

[セッションをログ記録する方法 \(P. 48\)](#)

## 本書の内容

この章では、CA Access Control を ObserveIT Enterprise セッション記録プログラムに統合する方法を説明します。この章では、共有アカウント管理セッションを記録するために行うプロセスと手順を説明します。

この章は、CA ControlMinder を使用して ObserveIT Enterprise セッション記録機能を利用するセキュリティ管理者とシステム管理者を対象にしています。

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

## ObserveIT の統合について

CA ControlMinder を ObserveIT Enterprise と統合すると、特権アカウントによる組織内のサーバへのアクセスの試行に対する制御が拡張されます。ObserveIT Enterprise セッションログ記録ソフトウェアにより、ターゲットシステムでのユーザ アクティビティが記録されます。記録が開始されるのは、ユーザが特権アカウントパスワードをチェックアウトするとき、およびエンドポイントにログインするときで、終了するのは、セッションが終了するときです（たとえば、ユーザが特権アカウントパスワードをチェックインするとき）。

記録されたセッションは、準備した専用のデータベースに格納されます。記録されたセッションは、ObserveIT ビューアを使用して CA Access Control エンタープライズ管理 から直接再生できます。

以下のリンクを使用して、ObserveIT 社から ObserveIT Enterprise セッションログ記録プログラムを取得できます。

<http://www.observeit-sys.com/download.asp>

以下のリンクで ObserveIT Enterprise のドキュメントを検索することができます。

<https://support.ca.com/cadocs/>

**注:** ObserveIT の詳細については、ObserveIT Enterprise のインストールメディアにある ObserveIT のマニュアルを参照してください。

## 統合をセットアップする方法

CA ControlMinder を ObserveIT Enterprise セッション記録ソフトウェアに統合するには、いくつかの手順を実行する必要があります。統合が終了すると、共有アカウント管理セッションはすべて ObserveIT Enterprise ソフトウェアによって記録されます。

**注:** 手順 1 ~ 5 を実行する方法の詳細については、ObserveIT のインストールメディアにある ObserveIT Enterprise のマニュアルを参照してください。

統合をセットアップするには、以下の手順に従います。

1. ObserveIT Enterprise のシステム要件およびインストール要件を確認します。  
使用するサーバが、ObserveIT Enterprise をインストールするための最小システム要件を満たしていることを確認します。
2. 中央データベースを準備します。  
記録されたセッションは、専用の Microsoft SQL Server に格納されます。
3. IIS (Internet Information Server) を設定します。  
ObserveIT Enterprise アプリケーションサーバは、IIS を使用して、エージェントから送信されたメタデータを処理します。
4. ObserveIT Enterprise サーバコンポーネントをインストールします。  
ObserveIT アプリケーションサーバ、エージェント、および管理コンソールもインストールされます。
5. ObserveIT Enterprise アプリケーションサーバを設定します。  
記録設定を設定します。
6. セッション記録スクリプトをエンタープライズ管理サーバにデプロイします。  
このスクリプトによって、セッション記録のトリガとなる共有アカウント管理自動ログインが有効になります。

7. サービス アカウントを作成します。  
エンタープライズ管理サーバで使用するサービス アカウントを作成します。
8. CA Access Control エンタープライズ管理 で **ObserveIT Enterprise** アプリケーション サーバへの接続を定義します。  
接続設定を設定して、セッション ログ記録を有効にします。

## 統合を準備する方法

ObserveIT Enterprise アプリケーション サーバのインストールが完了したら、CA ControlMinder との統合のためにサーバを準備します。ObserveIT Enterprise アプリケーション サーバの準備が完了すると、サーバは共有アカウント管理 セッションの記録および保存を開始するように設定されます。

統合を準備するには、以下の手順を実行します。

1. 管理コンソールを開きます。
2. サービス アカウントを作成します。

CA ControlMinder では、ObserveIT Enterprise アプリケーション サーバへの接続に、このサービス アカウントが使用されます。

## 管理コンソールを開きます。

ObserveIT Enterprise をインストールして起動すると、Web ベースの管理コンソールを起動できます。

### 管理コンソールを開く方法

1. ブラウザを使用して、ObserveIT Enterprise 管理コンソールを開きます。以下の URL を入力します。

`http://observeit_server_name:port/ObserveIT`

例：

`http://observeit_server:4884/ObserveIT`

2. インストール時に指定した管理者クレデンシャルを使用してログインします。

ObserveIT Enterprise 管理コンソールが開きます。

注： [スタート] - [プログラム] - [ObserveIT] - [ObserveIT WebConsole] に順にクリックして、ObserveIT Enterprise 管理コンソールを開くこともできます。

### サービス アカウントの作成

CA Access Control エンタープライズ管理 では、ObserveIT Enterprise アプリケーション サーバでの認証にサービス アカウントが使用されて、ユーザ アクティビティが記録されます。CA Access Control エンタープライズ管理で ObserveIT Enterprise アプリケーション サーバの接続設定を設定する際に、サービス アカウントのクレデンシャルを指定します。

#### サービス アカウントを作成する方法

1. ObserveIT Enterprise 管理コンソールから、[Configuration] - [Console Users] の順に選択します。  
コンソールユーザ画面が開きます。
2. [Create User] を選択します。  
コンソールユーザの追加ウィンドウが開きます。
3. ユーザ名とパスワードを入力し、パスワードを確認します。
4. 認証方法を [ObserveIT.Authentication] に、ユーザ ロールを [Admin] に設定します。
5. [Add] をクリックします。  
サービス アカウントが作成されます。

注: ユーザ管理の詳細については、ObserveIT Enterprise のインストールメディアにある *ObserveIT* のマニュアルを参照してください。

## セッション記録スクリプトのデプロイ

ユーザセッション記録は、共有アカウント管理の自動ログインと連携して動作します。ユーザが特権アカウントパスワードをチェックアウトし、エンドポイントへのログインを選択すると、リモート管理ソフトウェアが起動して、ユーザは自動的にログインされます。CA Access Control エンタープライズ管理では、エンドポイントタイプに基づいて、セッション記録スクリプトを使用してリモート管理プログラムが制御されます。

たとえば、ユーザが Windows エンドポイントへのログインを選択すると、CA Access Control エンタープライズ管理では、リモート デスクトップ ソフトウェアを開いてエンドポイントに接続するスクリプトが使用されます。

ObserveIT Enterprise アプリケーション サーバでセッションを記録するには、セッション記録スクリプトをエンタープライズ管理サーバにデプロイします。

### セッション記録スクリプトをデプロイする方法

1. CA サポート Web サイトから、セッション記録スクリプトをダウンロードし、一時ディレクトリに保存します。
2. エンタープライズ管理サーバで、以下のディレクトリ（ここで `JBoss_HOME` は、JBoss がインストールされているディレクトリを示します）へ移動します。  
`JBoss_HOME/server/default/deploy/IdentityMinder.ear/config/sso_scripts`
3. セッション記録スクリプトを `sso_scripts` ディレクトリにコピーします。  
上書きする前に、このディレクトリ内のファイルをバックアップすることをお勧めします。
4. 既存のファイルを新規ファイルで上書きすることを選択します。

ObserveIT Enterprise アプリケーション サーバへの接続設定を設定できるようになりました。

### ObserveIT への接続の定義

ObserveIT Enterprise との統合を完了するには、CA Access Control エンタープライズ管理 で ObserveIT Enterprise アプリケーション サーバへの接続設定を設定します。

#### ObserveIT への接続を定義する方法

1. CA Access Control エンタープライズ管理 で、 [システム] - [接続管理] - [セッション記録] - [接続の作成] の順に選択します。  
[Create Connection (接続の作成)] 画面が表示されます。
2. 以下の詳細を入力します。

#### 接続の説明

接続の説明をフリー テキストで記述します

#### 再生 URL

ObserveIT Enterprise アプリケーション サーバの URL を定義します

例： `http://observeit_host:4884/observeit/`

#### ユーザ ID

サービス アカウントのユーザ名を定義します

#### パスワード

サービス アカウントのパスワードを定義します

#### 詳細

以下の詳細な接続設定を指定します。

#### [ビューア ページ]

セッションが記録されることを示すメッセージを、画面の上部に表示するかどうかを指定します

#### [ビューア パラメータ]

ObserveIT ビューア ウィンドウの幅と高さを指定します

#### ActiveX URL

ObserveIT Enterprise の ActiveX ファイルがある場所のフルパス名を指定します。デフォルトでは、ObserveIT アプリケーションサーバの URL を指定します。

例：

`http://observeit_host:4884/ObserveIT/AgentInstall/Agent.cab#version=1,0,0,0`

#### サーバURL

ObserveIT Enterprise アプリケーションサーバが記録されたセッションを格納する場所のフルパス名を指定します。デフォルトでは、ObserveIT アプリケーションサーバの URL を指定します。

例：`http://observeit_host:4884/ObserveITApplicationServer`

3. [サブミット] をクリックします。

CA Access Control エンタープライズ管理により接続が作成されます。

## セッションをログ記録する方法

各 共有アカウント管理 セッションは記録されて、**ObserveIT Enterprise** データベースに格納されます。各セッションは、記録されたセッション全体から独立して再生できる個別のスライドに分割されます。

以下の手順では、共有アカウント管理セッションがログ記録される方法が説明されています。

1. ユーザが **CA Access Control** エンタープライズ管理 から特権アカウントパスワードをチェックアウトし、エンドポイントに自動的にログインすることを選択します。

このオプションを初めて使用する場合は、**ActiveX** をインストールするように求められます。

2. リモート管理セッションが開き、ユーザはパスワードの入力なしでログインされます。
3. エンドポイントにインストールされている **ObserveIT** エージェントにより、ユーザアクティビティの記録、および **ObserveIT Enterprise** アプリケーションサーバへのスライドの送信が開始されます。**ObserveIT Enterprise** アプリケーションサーバでは、そのデータがデータベースに保存されます。
4. ユーザがリモート管理セッションを閉じ、**ObserveIT** エージェントでは記録が停止されます。
5. 記録されたセッションが **CA Access Control** エンタープライズ管理 で表示されます。

**重要:** **Internet Explorer** による **ActiveX** のダウンロードを有効にするには、[ローカルイントラネットゾーン]または[信頼済みゾーン]で **ObserveIT** エンタープライズ ホスト名を指定し、[署名済み **ActiveX** コントロールのダウンロード] セキュリティオプションを有効にします。

**注:** セッション記録の詳細については、**ObserveIT Enterprise** のインストールメディアにある **ObserveIT** のマニュアルを参照してください。

## セッションがログ記録される場所

ObserveIT Enterprise アプリケーション サーバでは、専用の Microsoft SQL Server に共有アカウント管理のセッションがログ記録されます。ObserveIT データベース サーバでは、専用データベースが 2 つ使用されます。最初のデータベースは ObserveIT という名前で、設定とメタデータが保持されます。2 番目のデータベースは ObserveIT\_Data という名前で、記録されたセッションの実行中に ObserveIT エージェントで収集されたスクリーンショットが格納されます。

**注:** セッション ログ記録の詳細については、ObserveIT Enterprise のインストールメディアにある *ObserveIT* のマニュアルを参照してください。

## セッションの再生

記録された共有アカウント管理のセッションを CA Access Control エンタープライズ管理から再生します。セッションの再生を選択すると、CA Access Control エンタープライズ管理により、記録されたセッションが新しいウィンドウで再生されます。プレーヤウィンドウには、セッション内を移動するために使用するコントロールボタンがあります。記録されたセッション内でフリーテキスト検索を実行することもできます。

**注:** フリーテキスト検索の詳細については、ObserveIT Enterprise のインストールメディアにある *ObserveIT* のマニュアルを参照してください。

### セッションを再生する方法

1. CA Access Control エンタープライズ管理で、[特権アカウント]-[Audit subtask] の順に選択します。  
[特権アカウントの監査] タスクが、使用可能なタスク リストに表示されます。
2. [特権アカウントの監査] を選択します。  
[特権アカウントの監査] 検索ウィンドウが開きます。

**注:** 共有アカウント管理の Audit Manager ロールがこの手順の実行者に割り当てられていることを確認します。

3. 検索条件を指定し、表示する行数を入力して、[検索] をクリックします。

検索条件に適合するタスクが表示されます。

4. セッションの詳細列の再生アイコンをクリックして、セッションを再生します。

プレーヤ ウィンドウが開き、セッションが始めから再生されます。

**注:** セッション内を移動するには、ウィンドウ下部のコントロールを使用します。

# 第 4 章: RSA SecurID との統合

---

このセクションには、以下のトピックが含まれています。

[CA Access Control エンタープライズ管理 を RSA SecurID と統合する方法 \(P. 51\)](#)

[RSA SecurID がユーザ ログインを認証する仕組み \(P. 53\)](#)

[リバース プロキシ サーバとしての Web サーバの設定 \(P. 54\)](#)

## CA Access Control エンタープライズ管理 を RSA SecurID と統合する方法

ユーザの組織で RSA SecurID を使用してユーザの認証を行っている場合、RSA SecurID の機能を使用して CA Access Control エンタープライズ管理 へのユーザ ログインを認証できます。エンタープライズ管理サーバを RSA SecurID と統合する際に、CA Access Control エンタープライズ管理 はログイン中のユーザを認証しません。CA Access Control エンタープライズ管理は、ユーザ認証がサードパーティプログラムによって行われることを検出します。

以下のプロセスでは、CA Access Control エンタープライズ管理 を RSA SecurID と統合する方法について説明します。

1. エンタープライズ管理サーバを準備します。
2. サポートされている Web サーバをインストールします。
  - Windows - Internet Information Server 7.0 とアプリケーション リクエストルーティング (ARR) モジュール。
  - Linux - Apache 2.2.6 Web Server とプロキシ モジュール

3. [Web サーバをリバース プロキシサーバとして設定します \(P. 54\)](#)。

Web サーバは、すべてのログイン認証リクエストに対して、リバースプロキシサーバとして機能します。

4. Web サーバ以外からの CA Access Control エンタープライズ管理 へのすべてのネットワークアクセスをブロックするように RSA SecurID を設定します。

RSA SecurID は、ユーザが CA Access Control エンタープライズ管理 に直接アクセスするのを阻止します。

5. エンタープライズ管理サーバ コンポーネントをインストールします。

6. CA Access Control エンタープライズ管理 にログインする各 RSA SecurID ユーザについて、CA Access Control エンタープライズ管理 内にユーザアカウントを定義します。

CA Access Control エンタープライズ管理 へのアクセスを許可するユーザのみを定義します。

**重要:** Active Directory を使用している場合は、この手順を完了する必要はありません。

7. RSA Authentication Agent を以下のサーバにインストールします。

- (Linux) エンタープライズ管理サーバ
- Web サーバ

RSA Authentication Agent はユーザアクセス リクエストをインターセプトし、それを RSA Authentication Manager へ転送します。

8. RSA Web Agent を設定して、CA Access Control エンタープライズ管理 に対する Single Sign On (SSO) を有効にします。

9. RSA Authentication Manager を専用ホストにインストールします。

RSA Authentication Manager はユーザアクセス リクエストを認証します。

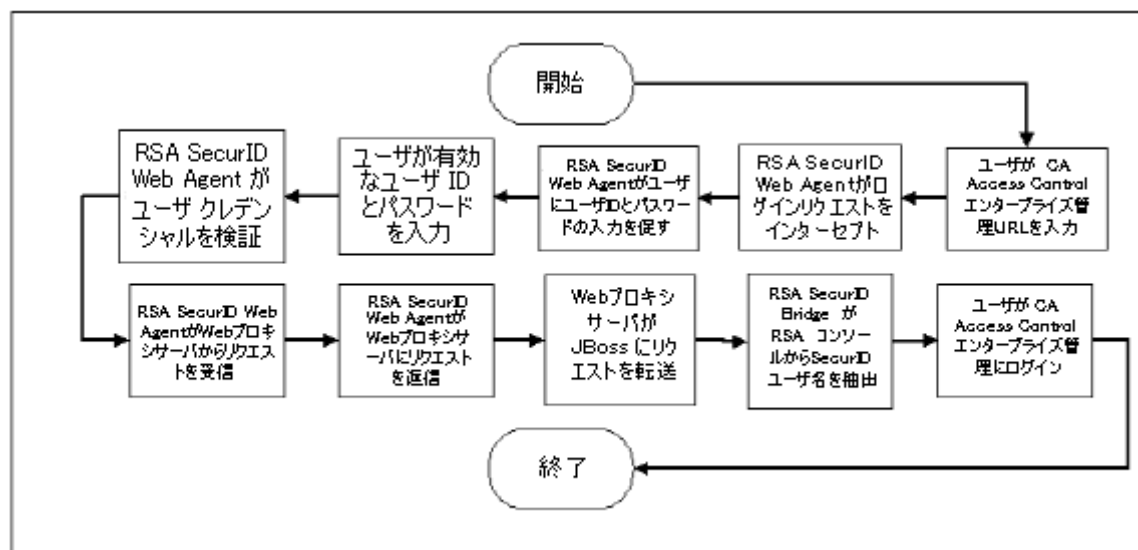
ユーザが CA Access Control エンタープライズ管理 へのログインを試行するたびに、RSA SecurID はユーザに対して、CA Access Control エンタープライズ管理 ユーザ アカウントの詳細ではなく有効な RSA SecurID クレデンシャルの入力を促すメッセージを表示します。認証が成功すると、RSA SecurID は CA Access Control エンタープライズ管理 へのログインをユーザに許可します。

注: RSA SecurID Web Agent および Authentication Manager の詳細については、[RSA SecurID](#) の Web サイトをご覧ください。

## RSA SecurID がユーザ ログインを認証する仕組み

エンタープライズ管理サーバを RSA SecurID と統合すると、ユーザが CA Access Control エンタープライズ管理 にログインするたびに、RSA SecurID がログイン リクエストを認証します。RSA SecurID がユーザ ログインを検証すると、ユーザは CA Access Control エンタープライズ管理 に自動的にログインできます。

以下の図は、RSA SecurID が CA Access Control エンタープライズ管理 へのユーザ ログインを認証する仕組みを示しています。



## リバースプロキシサーバとしての Web サーバの設定

ユーザが CA Access Control エンタープライズ管理 へのログインを試行すると、RSA SecurID はそのリクエストをインターセプトし、ユーザに対して有効な SecurID のユーザ名およびパスワードの入力を促すメッセージを表示します。インストールした Web サーバはリバースプロキシサーバとして動作します。このサーバは、エンタープライズ管理サーバ上の RSA Authentication Web Agent からログインリクエストを受信し、それを RSA Authentication Manager に転送します。

リバースプロキシは他のサーバのゲートウェイで、1つの Web サーバが他の Web サーバのコンテンツを提供するのを可能にします。

### 例: リバースプロキシサーバとしての Windows Server 2008 上での Internet Information Services 7.0 の設定

この例では、システム管理者である Steve はエンタープライズ管理サーバおよび Internet Information Services (IIS) 7.0 をアプリケーションリクエストルーティング (ARR) モジュールがインストールされている Windows Server 2008 にインストールしました。ARR モジュールによって、IIS はプロキシサーバとして機能します。

1. Steve は、Internet Information Services サーバ上で IIS プロキシ設定を有効にします。
  - a. [スタート] - [管理ツール] - [Internet Information Services (IIS) Manager] の順に選択します。

Internet Information Services (IIS) Manager が開きます。
  - b. 左ペインからホストを選択して操作ウィンドウを展開し、[アプリケーションリクエストルーティング キャッシュ] アイコンを選択します。

[アプリケーションリクエストルーティング キャッシュ] 管理コンソールが開きます。
  - c. 操作ウィンドウから [サーバプロキシ設定] を選択します。
  - d. [プロキシを有効] チェックボックスをオンにし、[適用] をクリックします。

Steve は IIS プロキシ設定を有効にしました。

2. Steve は、エンタープライズ管理サーバにリクエストを転送するように IIS を設定します。
  - a. [サイト] メニューを展開し、デフォルトの Web サイトを選択します。
  - b. [URL 書き換え] アイコンを強調し、操作メニューから [機能を開く] を選択します。

[URL 書き換え] 設定コンソールが開きます。
  - c. 操作メニューから [ルールの追加] を選択します。

[ルールの追加] ウィンドウが開きます。
  - d. [受信の規則] の下で [ブランク ルール] を選択し、[OK] をクリックします。

[受信の規則の編集] 設定ウィンドウが開きます。
  - e. ルール名を指定し、[パターン] メニューから [(iam.+)] を選択します。
  - f. [アクション] セクションまでスクロールし、[アクションの種類] メニューから [書き直す] を選択します。
  - g. 以下の形式で、[URL 書き換え] フィールドに CA Access Control エンタープライズ管理の URL を入力します。

`http://enterprise_host:8080/{R:0}`
  - h. [適用] をクリックして、ルールを作成します。

新しい受信ルールが作成されます。
  - i. [パターン] メニューの [(castyles.+)] を使用して、手順 c から h までを繰り返します。

Steve は、エンタープライズ管理サーバにリクエストを転送するように IIS を設定しました。

3. Steve は、Web サーバをセキュリティで保護するように RSA SecurID を設定します。
  - a. Internet Information Services (IIS) Manager コンソールで [既定の Web サイト] を選択し、[RSA SecurID] アイコンをダブルクリックします。

[RSA SecurID 設定] ウィンドウが開きます。
  - b. 以下のチェック ボックスをオンにします。
    - このサーバ上で RSA SecurID Web アクセス認証機能を有効にする
    - このリソースを保護する
  - c. 操作メニューから [適用] を選択する
4. Steve は、CA Access Control エンタープライズ管理用に Single Sign Off (SSO) を有効にするように、RSA Web Agent を設定します。
  - a. regedit ユーティリティを開き、以下の場所へ移動します。

HKEY\_LOCAL\_MACHINE\SOFTWARE\SDTI\RSAWebAgent
  - b. 「RSAUSERCustomHeader」という名前の下に、DWORD タイプのレジストリ キーを作成します。
  - c. レジストリ キー値を「1」に設定します。

Steve は Internet Information Services をリバースプロキシサーバとして設定しました。

## 例: Apache Web Server 2.2.6 を Red Hat Enterprise Linux 5.0 上でリバースプロキシサーバとして設定

この例で、システム管理者である Steve は、エンタープライズ管理サーバを Red Hat Enterprise Linux 5.0 上にインストールしました。ここで、Steve は Apache Web Server 2.2.6 をリバースプロキシサーバとしてインストールし設定する必要があります。

1. Steve は Apache Web Server 2.2.6 とプロキシモジュールをインストールし設定するために、以下の操作を行います。
  - a. プロキシモジュールをインストールするために、以下のようにインターフェースした Apache Web Server 2.2.6 を設定します。

```
tar -zxvf httpd_2.2.6.tar.gz
./configure --prefix=/usr/local/apache --enable-proxy --enable-proxy-http
make
make install
```

Apache Web Server 2.2.6 はプロキシモジュールと共にインストールされます。

2. Steve はリバースプロキシを設定するために、以下の操作を行います。
  - a. Apache Web Server の conf ディレクトリに移動します。
  - b. httpd.conf ファイルを開いて、編集します。
  - c. エントリの LoadModule リストを見つけて、以下のセクションを追加します。

```
# Used for proxy to the Enterprise Management Server
ProxyPass /iam http://196.168.1.1:8080/iam
ProxyPass /castylesr5.1.1 http://192.168.1.1:8080/castylesr5.1.1
ProxyPassReverse/iam http://192.168.1.1:8080/iam
```

- d. ファイルを保存して閉じます。
- e. Apache Web Server を再起動します。

Steve は、リバースプロキシサーバとして動作するように Apache Web Server 2.2.6 を設定しました。

3. Steve は、Cookie 検証用として Web ブラウザの IP アドレスを無視するように RSA Web Agent を設定します。

- a. RSA Web Agent インストールディレクトリに移動します。

```
/usr/local/apache/rsawebagent/
```

- b. RSA Web Agent 設定ユーティリティを実行します。
- c. リストから現在使用されている RSA サーバを選択します。
- d. 2 番目の設定画面を参照します。

- e. Cookie 検証用のブラウザ IP アドレスの無視が有効になっていることを確認します。

Steve は、Cookie 検証用として Web ブラウザの IP アドレスを無視するように RSA Web Agent を設定しました。

4. Steve は、CA Access Control エンタープライズ管理用に Single Sign Off (SSO) を有効にするように RSA Web Agent を設定します。

- a. Linux Web Agent ディストリビューションを開き、以下のファイルを見つけます。

```
rsacookieapi.tar
```

- b. 一時ディレクトリにファイルをコピーし、ファイルのコンテンツを抽出します。

- c. 以下のファイルを見つけます。

- RSACookieAPI.jar
- libsacookieapi.so

- d. 以下の場所に libsacookieapi.so ファイルをコピーします。ここで、*JBOSS\_HOME* は Steve が Jboss をインストールした場所を示します。

```
JBOSS_HOME/server/default/deploy/IdentityMinder.ear/library
```

- e. 以下の場所に RSACookieAPI.jar ファイルをコピーします。

```
JBOSS_HOME/server/default/deploy/IdentityMinder.ear/user_console.war/WEB-INF/lib/
```

Steve は、CA Access Control エンタープライズ管理用に SSO を有効にするように RSA Web Agent を設定しました。

# 第 5 章: 複数の LDAP サーバとの連携

---

このセクションには、以下のトピックが含まれています。

[概要 \(P. 59\)](#)

[複数の LDAP サーバを設定する方法 \(P. 60\)](#)

## 概要

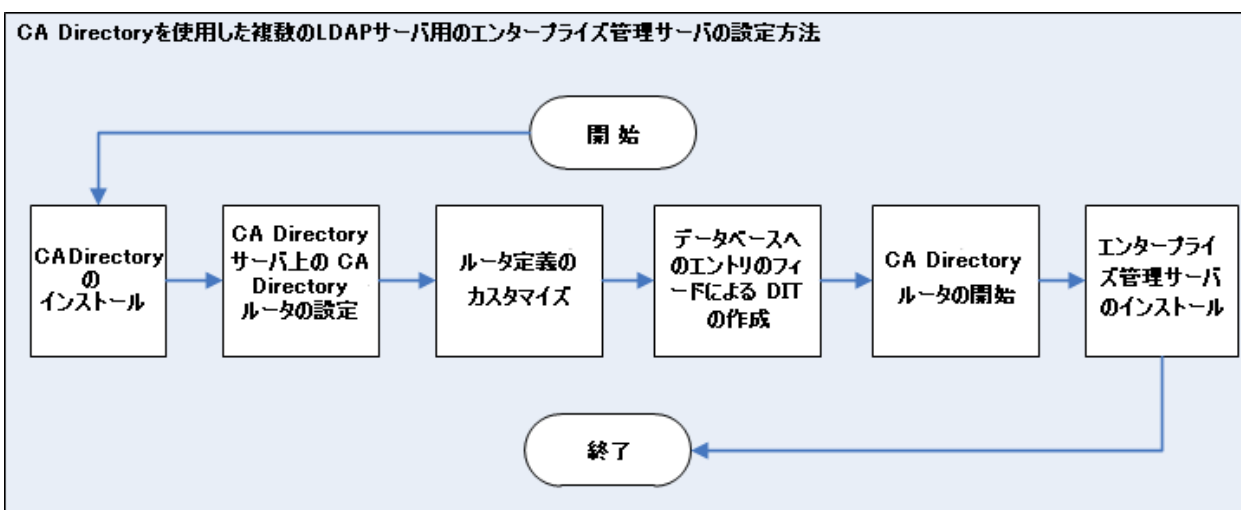
この章では、システムまたはデータベースの管理者を対象に、CA Directory を使用して複数の LDAP サーバと連携するよう CA Access Control エンタープライズ管理を設定する方法について説明します。複数の LDAP サーバと連携することにより、管理者は複数の LDAP ユーザストアを企業レベルの 1 つのユーザストアに統合することができます。

## 複数の LDAP サーバを設定する方法

CA Directory は、分散ディレクトリ バックボーンへの LDAP サーバの統合をサポートします。

CA Directory では、DXlink と呼ばれるユーティリティが提供され、これにより複数の LDAP ディレクトリ サーバに対する検索が可能になります。

以下の図は、CA Directory を使用して複数の LDAP サーバに対して CA Access Control エンタープライズ管理 を設定する方法を示しています。



CA Directory を使用して、複数の LDAP サーバ用にエンタープライズ管理サーバを設定するには、以下の手順を実行します。

1. CA Directory をインストールします
2. [CA Directory ルータを設定します](#) (P. 62)
3. [CA Directory ルータ定義をカスタマイズします](#) (P. 65)
4. [DIT 作成のため、データベースにエンティティを入力します](#) (P. 68)
5. CA Directory を開始します
6. Active Directory をユーザストアとしてエンタープライズ管理サーバをインストールします

**重要:** エンタープライズ管理サーバをインストールする際は以下を指定します。

- ホスト名 -- CA Directory ホスト名
- ポート番号 -- 25389
- ベース DN -- 環境内のすべての Active Directory サーバに共通の DN を指定します。適用しない場合はこのフィールドを空白にします。
- (Linux) 検索ルート -- 環境内のすべての Active Directory サーバに共通の DN を指定します。適用しない場合はこのフィールドを空白にします。
- 管理アカウント -- Active Directory ドメインの 1 つの管理アカウント

**注:** CA Access Control エンタープライズ管理 にログインする際は、使用している管理アカウントがメンバであるドメイン名を必ず指定してください。

## CA Directory ルータの設定

CA Directory は、Active Directory へのリクエストを、クライアント リクエストに定義されたサフィックスに基づいて、CA ControlMinder によって使用される Active Directory にルーティングします。CA Directory は、リクエストのルーティングに DXlink ユーティリティを使用します。

この手順を完了する前に、2 つの Active Directory ユーザストア（たとえば `acdir1` と `acdir2`）、および `dsarouter` という名前の CA Directory をインストールしました。

次の手順に従ってください:

1. CA Directory サーバから、コマンドプロンプト ウィンドウを開きます。
2. 以下のコマンドを実行します。

```
dxnewdsa -s 1 cadirhost-adrouter 25389
```

```
-s 1
```

データベース サイズに 1 MB を指定します

```
cadirhost-adrouter
```

ルータの名前を定義します

```
25389
```

ルータのポートを指定します

3. 以下のコマンドを使用してルータを停止します。

```
dxserver stop cadirhost-adrouter
```

4. 以下のコマンドを使用してルータをインストールします。

```
dxserver install cadirhost-adrouter
```

5. 以下のディレクトリに移動します（DXHOME はルータをインストールしたディレクトリの名前です）。

`DXHOME/config/knowledge`

6. 以下の手順に従って `cadirhost-router.dxc` ファイルを複製します。
  - a. 1 つ目のファイル名を `acdir1-dxlink.dxc` に変更します
  - b. 2 つ目のファイル名を `acdir2-dxlink.dxc` に変更します
  - c. `acdir1-dxlink.dxc` ファイルを以下のように編集します

```
set dsa "acdir1-dxlink" =
{
  prefix          = <dc "acdir1"><dc "com">
  dsa-name        = <cn "acdir1-dxlink">
  dsa-password    = "secret"
  ldap-dsa-name   = <dc "acdir1"><dc "com"><cn "users"><cn
"Administrator">
  ldap-dsa-password = "{CADIR}yKW2cVbG"
  address         = tcp "acdir1" port 389
  auth-levels     = clear-password
  trust-flags     = allow-check-password, no-server-credentials
  link-flags      = dsp-ldap, ms-ad
};
```

#### `ldap-dsa-name`

Active Directory にバインドするために使用される識別名（DN）を指定します。

#### `ldap-dsa-password`

DN の暗号化されたパスワードを定義します。

注: パスワードの暗号化には `dxpassword` ユーティリティを使用します。例: `dxpassword -P CADIR <password>`

#### `address`

Active Directory ドメイン コントローラのアドレスを指定します。

- d. `acdir2-dxlink.dxc` を以下のように編集します

```
set dsa "aclabcail-dxlink" =
{
  prefix          = <dc "acdir2"><dc "com">
  dsa-name        = <cn "acdir2-dxlink">
  dsa-password    = "secret"
  ldap-dsa-name   = <dc "acl"><dc "aclab"><cn "users"><cn "Administrator">
  ldap-dsa-password = "{CADIR}yKW2cVbG"
  address         = tcp "acdir2" port 389
  auth-levels     = clear-password
  trust-flags     = allow-check-password, no-server-credentials
  link-flags      = dsp-ldap, ms-ad
};
```

CA Directory ルータが設定されました。

## CA Directory ルータ定義のカスタマイズ

CA Directory ルータを設定したら、CA Directory ルータ定義をカスタマイズする必要があります。

次の手順に従ってください:

1. 以下のディレクトリに移動します (*DXHOME* は、CA Directory をインストールしたディレクトリです)。

*DXHOME*/config/limits

2. 以下の手順を実行します。

- a. *default.dxc* ファイルのコピーを作成し、元のファイルの名前を *dsarouter-adrouter.dxc* に変更します
- b. 読み取り専用フラグをファイルから削除します
- c. *dsarouter-adrouter.dxc* ファイルを開き、以下のフィールドを変更します

```
# size limits
set max-users = 255;
set max-local-ops = 100;
set max-op-size = 0;
```

```
# time limits
set max-bind-time = none;
set bind-idle-time = 3600;
set max-op-time = 600;
```

ファイルを保存して閉じます。

3. 以下のディレクトリに移動します

*DXHOME*/config/settings

4. 以下の手順を実行します。

- a. *default.dxc* ファイルのコピーを作成し、元のファイルの名前を *dsarouter-adrouter.dxc* に変更します
- b. 読み取り専用フラグをファイルから削除します
- c. *dsarouter-adrouter.dxc* ファイルを開き、以下のフィールドを変更します

```
# directory information base
set alias-integrity = true;
# distribution controls
set multi-casting = true;
set always-chain-down = false;
```

```
# security controls
set min-auth = clear-password;
set allow-binds = true;
set ssl-auth-bypass-entry-check = false;
# general controls
set op-attrs = true;
set transparent-routing = true;
```

ファイルを保存して閉じます

5. 以下のディレクトリに移動します

DXHOME/config/knowledge

6. dsarouter-adrouter.dxc ファイルを開くか作成し、auth-levels の文字列値 "anonymous" を削除して、クリアパスワードによるログインのみを有効にします。以下に例を示します。

```
set dsa "cadirhost-adrouter" =
{
prefix          = <>
dsa-name        = <cn "cadirhost-adrouter">
dsa-password    = "secret"
address         = tcp "cadirhost" port 25389
disp-psap      = DISP
snmp-port       = 25389
console-port    = 25390
auth-levels     = clear-password
```

ファイルを保存して閉じます。

**重要:** IPv4 および IPv6 アドレスの両方が定義されたサーバに CA Directory をインストールした場合、tcp の値には IPv6 と IPv4 のアドレスタイプを指定します。例: address = tcp "fe80::20d:56ff:fed4:8300%5" port 19389, tcp "192.168.1.1" port 19389

7. adrouter.dxa という名前のファイルを作成し、以下の行を追加し、ファイルを保存して閉じます。

```
source "dsarouter-adrouter.dxc";
source "acdir1-dxlink.dxc";
source "acdir2-dxlink.dxc";
```

8. 以下のディレクトリに移動します

DXHOME/config/logging

9. 以下の手順を実行します。
  - a. default.dxc ファイルのコピーを作成します
  - b. 元のファイルの名前を dsarouter-adrouter.dxc に変更します
  - c. 読み取り専用タグを削除します

10. 以下のディレクトリに移動します

DXHOME/config/servers

11. 以下の手順を実行します。
  - a. cadirhost-adrouter.dxi を編集し、以下の行を変更し、ファイルを保存して閉じます。

```
#
# Initialization file written by DXnewsda
#
# logging and tracing
source "../logging/cadirhost-adrouter.dxc";
# schema
clear schema;
source "../schema/default.dxc";
# knowledge
clear dsas;
source "../knowledge/adrouter.dxc";
# operational settings
source "../settings/cadirhost-adrouter.dxc";
# service limits
source "../limits/cadirhost-adrouter.dxc";
# access controls
clear access;
source "../access/default.dxc";
# ssl
source "../ssld/default.dxc";
# replication agreements (rarely used)
# source "../replication/";
# multiwrite DISP recovery
set multi-write-disp-recovery = false;
# grid configuration
set dxgrid-db-location = "data";
set dxgrid-db-size = 1;
set cache-index = all-attributes;
set lookup-cache = true;
```

注: cadirhost を CA Directory ホスト名で置き換えます。

CA Directory ルータ定義がカスタマイズされました。

## DIT を作成するための CA Directory データベースへの入力

Directory Informational Tree (DIT) を作成するために、CA Directory データベースにエンティティが入力されるようにすることができます。DIT によって組織階層を上から下へ参照することができます。

次の手順に従ってください:

1. CA Directory ルータをホストするサーバで、`input.ldif` という名前のファイルを作成し、以下のようにエンティティを追加します。

```
dn: dc=com
objectClass: domain
objectClass: top
dc: com

dn: dc=company,dc=com
objectClass: domain
objectClass: top
dc: company

dn: dc=demo
objectClass: domain
objectClass: top
dc: demo
```

2. ファイルを保存して閉じます。
3. コマンドプロンプト ウィンドウを開き、以下のコマンドを実行します。

```
dxloaddb cadirhost-adrouter input.ldif
```

4. 以下のコマンドを実行して CA Directory ルータを起動します。

```
dxserver start cadirhost-adrouter
```

**注:** `cadirhost` を CA Directory ホスト名で置き換えます。

DIT を作成するために CA Directory データベースにエンティティが入力されました。

## 第 6 章: CA SiteMinder との統合

---

このセクションには、以下のトピックが含まれています。

[概要 \(P. 69\)](#)

[CA SiteMinder で CA ControlMinder ユーザを認証する方法 \(P. 70\)](#)

[CA SiteMinder と統合する方法 \(P. 71\)](#)

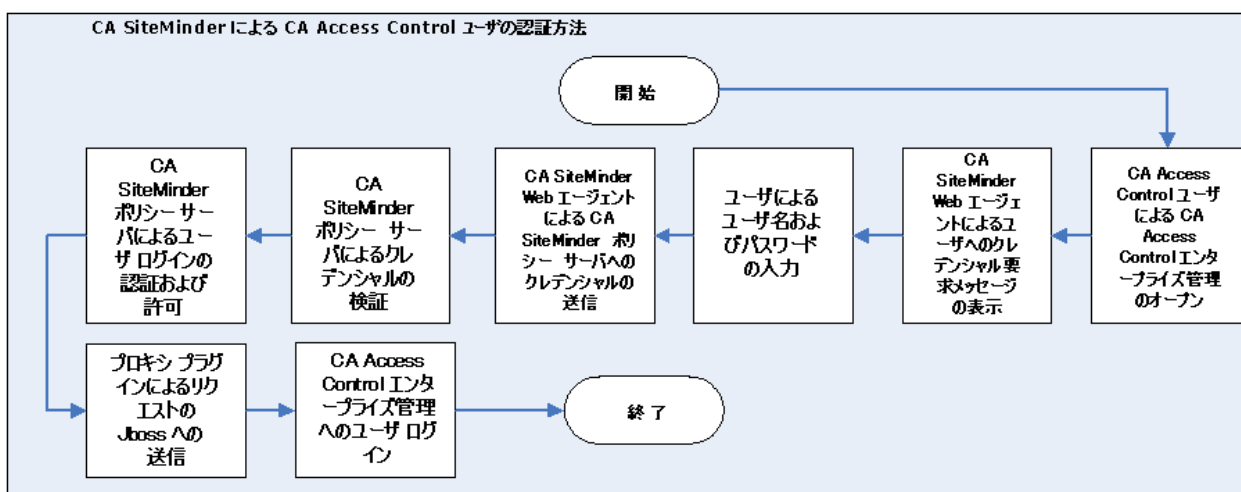
### 概要

この章では、システム、ネットワーク、またはセキュリティの管理者を対象に、CA SiteMinder との連携によって CA Access Control エンタープライズ管理を保護する方法について説明します。CA SiteMinder では、CA SiteMinder ディレクトリからユーザを認証し、CA ControlMinder ユーザのみが CA Access Control エンタープライズ管理へのログインを許可されるようにすることができます。CA SiteMinder を使用して CA Access Control エンタープライズ管理を保護することによって、管理者は CA SiteMinder の拡張ユーザ認証方式を使用できます。

## CA SiteMinder で CA ControlMinder ユーザを認証する方法

CA SiteMinder を使用して CA Access Control エンタープライズ管理 を保護すると、ユーザが CA Access Control エンタープライズ管理 にログインするたびに、CA SiteMinder はログイン リクエストを認証します。CA SiteMinder がログイン リクエストを許可したら、ユーザは CA Access Control エンタープライズ管理 へのアクセス権を獲得します。

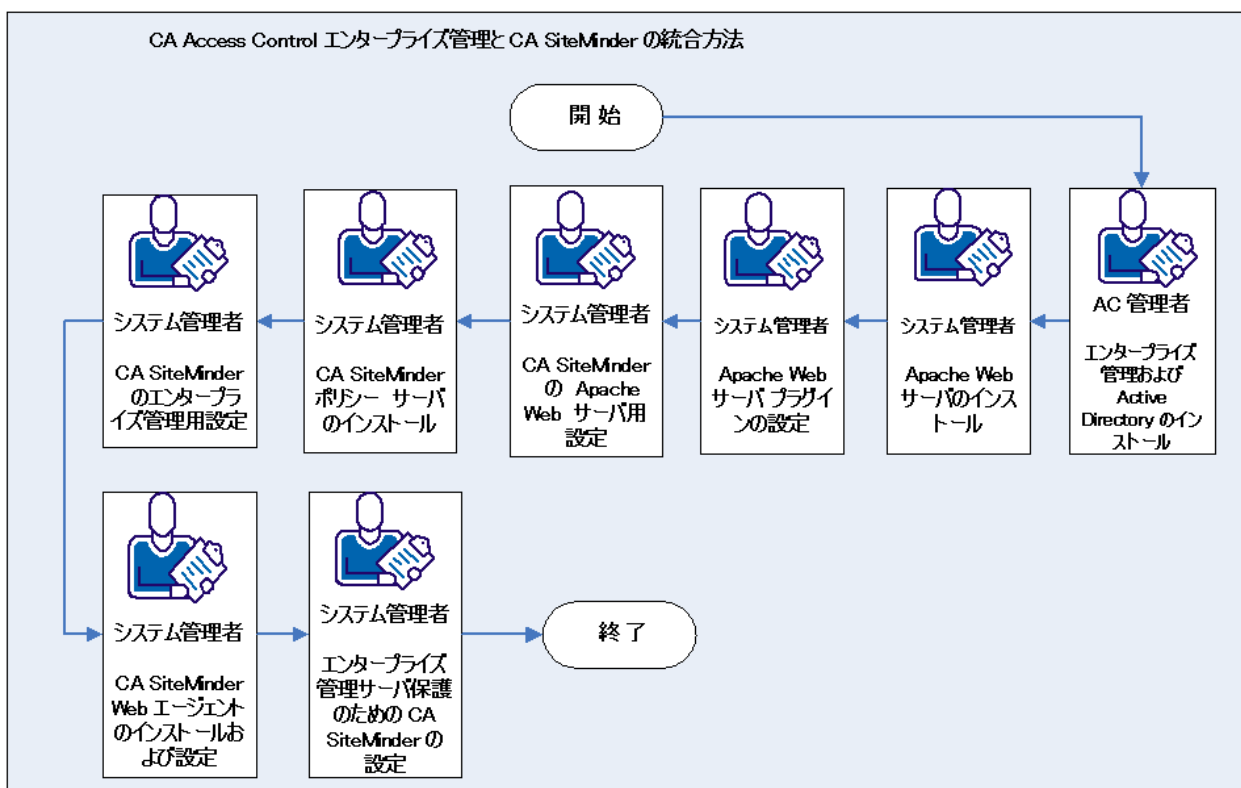
以下の図は、CA SiteMinder が、CA ControlMinder ユーザの CA Access Control エンタープライズ管理 へのログインを認証および許可する方法を示しています。



## CA SiteMinder と統合する方法

CA Access Control エンタープライズ管理を CA SiteMinder と統合することによって、CA SiteMinder の拡張ユーザ認証機能および許可機能を活用することができます。

以下の図は、システムまたはセキュリティの管理者が CA SiteMinder と CA Access Control エンタープライズ管理をどのように統合するかを示しています。



以下のプロセスは、CA SiteMinder と統合する方法を示しています。

1. エンタープライズ管理サーバをインストールします

Web ベースのすべてのアプリケーション、配布サーバ、DMS、および CA Access Control がインストールされます。

注: エンタープライズ管理サーバをインストールする前に、前提条件のインストールおよび設定によってコンピュータを準備します。

2. [Apache Web サーバをエンタープライズ管理サーバ上に設定します](#) (P. 73)
3. CA SiteMinder ポリシー サーバをインストールします
4. [エンタープライズ管理サーバ用に CA SiteMinder を設定します](#) (P. 77)
5. [CA SiteMinder Web エージェントを設定します](#) (P. 78)
6. [エンタープライズ管理サーバを保護するよう CA SiteMinder を設定します](#) (P. 79)
7. [ユーザの認証に CA SiteMinder を使用するようエンタープライズ管理サーバを設定します](#) (P. 82)

注: CA SiteMinder ポリシー サーバ、Web エージェント、および管理 UI の詳細については、CA SiteMinder のドキュメントを参照してください。

## 例: エンタープライズ管理サーバでの Apache Web サーバ プロキシ プラグインの設定

この例では、エンタープライズ管理サーバが Windows 2008 Server にインストールされます。また、Apache Web サーババージョン 2.2.19 がエンタープライズ管理サーバにインストールされ、SSL サポートが有効になっている必要があります。次に Apache Web サーバ プロキシ プラグインを設定します。以下の手順を実行します。

1. エンタープライズ管理サーバ上の JBoss アプリケーション サーバを停止します。

2. 以下のディレクトリに移動します

```
APACHE_HOME/conf
```

```
APACHE_HOME
```

Apache Web サーバがインストールされているディレクトリ

3. httpd.conf ファイルを編集し、プロキシ モジュールを有効にしてプロキシ設定を含めます。

- a. 以下の行のコメントを解除します。

```
LoadModule proxy_module modules/mod_proxy.so
```

```
LoadModule proxy_http_module modules/mod_proxy_http.so
```

- b. Global 設定セクションの最後に、以下の行を追加します。

```
Include conf/extra/httpd-proxy-entm.conf
```

4. 以下のディレクトリに移動します

```
APACHE_HOME/conf/extra
```

5. `httpd-proxy-entm.conf` という名前のファイルを作成し、以下のコンテンツを追加し、ファイルを保存して閉じます。

```
# Proxy to CA AC ENTM
<IfModule proxy_module>
  <IfModule proxy_http_module>
    # /iam section BEGIN
    <Proxy /iam>
      Order allow,deny
      Allow from all
    </Proxy>
    ProxyPass /iam http://acentmnode.example.com:8080/iam
    ProxyPassReverse /iam http://acentmnode.example.com:8080/iam
    ProxyPass /iam/ http://acentmnode.example.com:8080/iam/
    ProxyPassReverse /iam/ http://acentmnode.example.com:8080/iam/

    # /iam section END
    # /castylesr5.1.1 section BEGIN
    <Proxy /castylesr5.1.1>
      Order allow,deny
      Allow from all
    </Proxy>
    ProxyPass /castylesr5.1.1
    http://acentmnode.example.com:8080/castylesr5.1.1
    ProxyPassReverse /castylesr5.1.1
    http://acentmnode.example.com:8080/castylesr5.1.1
    ProxyPass /castylesr5.1.1/
    http://acentmnode.example.com:8080/castylesr5.1.1/
    ProxyPassReverse /castylesr5.1.1/
    http://acentmnode.example.com:8080/castylesr5.1.1/
    # /castylesr5.1.1 section END
  </IfModule>
</IfModule>
```

注: `acentmnode.example.com:port` を、エンタープライズ管理サーバがインストールされているサーバの実際のホスト名およびポートで置き換えます。

6. Apache Web サーバを再起動します。
7. JBoss アプリケーションサーバを再起動します。
8. エンタープライズ管理サーバを参照し、Apache Web サーバがリクエストを正常に転送することを確認します。以下の URL を使用します。

```
http://enterprise_host:port/iam/ac
```

Apache Web サーバプロキシプラグインがエンタープライズ管理サーバ上に設定されました。

## 例: Apache Web サーバ用の CA SiteMinder の設定

この例では、Apache Web サーバのプロキシプラグインをエンタープライズ管理サーバ上に設定した後、CA SiteMinder を Apache Web サーバに対して設定します。

1. CA SiteMinder 管理者インターフェースを使用して、以下を実行します。
  - a. [スタート] - [すべてのプログラム] - [CA] - [CA SiteMinder] - [CA SiteMinder Administrative UI] の順に選択します。  
CA SiteMinder 管理 UI が開き、ユーザ名とパスワードの入力が求められます。
  - b. CA SiteMinder 管理 UI にログインします。
  - c. [インフラストラクチャ] - [ホスト] - [ホスト設定] - [ホスト設定の作成] を選択し、ホスト設定タイプのオブジェクトのコピーを作成します。
  - d. DefaultHostSettings オブジェクトを選択して [OK] をクリックします。
  - e. 以下のフィールドに値を入力します。
    - 名前 -- webservernode-HCO
    - 説明 -- Web サーバ ホスト設定
  - f. 設定値フレームに移動し、[追加] をクリックして、CA SiteMinder ポリシー サーバのホスト名を以下のように入力します。  
ホスト: `policyserver.company.com`
  - g. [サブミット] をクリックします。  
ホスト設定オブジェクトが設定されました。

2. [インフラストラクチャ] - [エージェント] - [エージェント] - [エージェントの作成] を選択し、エージェント タイプの新規オブジェクトを作成します。
3. 以下のフィールドに入力して [サブミット] をクリックします。
  - 名前 -- webservers-agent
  - 説明 -- Web サーバ ノード Web エージェント
  - エージェント タイプの選択 -- SiteMinder
  - エージェント タイプ -- Web エージェント
  - 4.x エージェントのサポート -- オフWeb エージェント オブジェクトが設定されました。
4. [エージェント設定] - [エージェント設定の作成] を選択し、エージェント設定タイプのオブジェクトのコピーを作成します。
5. ApacheDefaultSettings を選択し、[OK] をクリックして以下の手順に従います。
  - a. 以下のフィールドに値を入力します。
    - **Name** -- webservernode-ACO
  - b. パラメータ リストで、#DefaultAgentName フィールドを編集し、名前の値から # 文字を削除します。
  - c. エージェント名を以下のように設定します。
    - **DefaultAgentName** -- webservers-agent
  - d. #LogoffUri を編集し、名前の値から # 文字を削除します。
  - e. 値を以下のように設定します。
    - **LogoffUri** -- /iam/logout.jsp

**注:** エージェント パラメータの詳細については、「CA SiteMinder エージェント設定ガイド」を参照してください。
6. [サブミット] をクリックします。  
エージェント設定オブジェクトが作成されました。

## 例: エンタープライズ管理サーバ用の CA SiteMinder の設定

この例では、エンタープライズ管理サーバに対して CA SiteMinder を設定します。

1. CA SiteMinder 管理者インターフェースを使用して、以下を実行します。
2. [スタート] - [すべてのプログラム] - [CA] - [CA SiteMinder] - [CA SiteMinder Administrative UI] の順に選択します。

CA SiteMinder 管理 UI が開き、ユーザ名とパスワードの入力が求められます。

3. CA SiteMinder 管理 UI にログインします。
4. [インフラストラクチャ] - [ホスト] - [ホスト設定] - [ホスト設定の作成] を選択し、ホスト設定タイプのオブジェクトのコピーを作成します。
5. DefaultHostSettings オブジェクトを選択して [OK] をクリックします。
6. 以下のフィールドに値を入力します。

- 名前 -- acentmnode-HCO
- 説明 -- ENTM ホスト設定

7. 設定値フレームに移動し、[追加] をクリックして、CA SiteMinder ポリシーサーバのホスト名を以下のように入力します。

ホスト: `policyserver.company.com`

8. [サブミット] をクリックします。

エージェントオブジェクトが設定されました。次に、CA SiteMinder Web エージェントをインストールおよび設定します。

## 例: CA SiteMinder Web エージェントの設定

この例で、システム管理者のステイブは **CA SiteMinder Web エージェント** をエンタープライズ管理サーバ上にインストールしました。ステイブは次に、以前に定義したホストおよびエージェントのオブジェクト設定を使用して、**Apache Web** サーバ用に **Web エージェント** を設定します。

1. 以下の手順を実行します。
  - a. 以下のディレクトリに移動します (*APACHE\_HOME* は、Apache Web サーバをインストールしたディレクトリです)。

```
APACHE_HOME/conf
```

- b. **WebAgent.conf** ファイルを以下のように編集し、**Web エージェント** を有効にします。

```
EnableWebAgent="YES"
```

- c. ファイルを保存して閉じます
2. **Apache Web** サーバを再起動します。

CA SiteMinder Web エージェントが設定されました。

## 例: エンタープライズ管理サーバを保護するための CA SiteMinder の設定

この例では、セッション内のエンタープライズ管理サーバログを保護するために CA SiteMinder を設定します。CA SiteMinder が保護するユーザストアに対して認証方式およびドメインポリシーを設定する必要があります。

1. 以下の手順を実行します。
  - a. [スタート] - [すべてのプログラム] - [CA] - [CA SiteMinder] - [CA SiteMinder Administrative UI] に移動します。

CA SiteMinder 管理 UI が開き、ユーザ名とパスワードの入力が求められます。
  - b. CA SiteMinder 管理者ユーザアカウントのクレデンシャルを入力します。
  - c. [インフラストラクチャ] - [ディレクトリ] - [ユーザディレクトリ] - [ユーザディレクトリの作成] を選択します。
  - d. [一般] フレームで以下のフィールドに入力します。
    - 名前 -- ac-dir
    - 説明 -- Access Control ユーザストア
  - e. ディレクトリのセットアップフレームに移動し、以下のフィールドに入力します。
    - ネームスペース -- LDAP
    - サーバ -- *directory\_hostname:port*
  - f. 管理者のクレデンシャルに移動し、以下のフィールドに入力します。
    - クレデンシャルが必要 -- オン
    - ユーザ名 -- バインドユーザの完全な DN
    - パスワード -- <パスワード>
    - パスワードの確認 -- <パスワード>
  - g. LDAP 設定フレームに移動し、以下のフィールドに入力します。
    - ルート -- searchroot
    - スコープ -- サブツリー
    - 開始 -- (&(sAMAccountName=

- 終了
  - )(objectclass=top)(objectclass=person)(objectclass=organizational person)(objectclass=user))
- h. ユーザ属性フレームに移動し、以下のフィールドに入力します。
  - ユニバーサル ID -- %USER\_ID% に対応する属性名
- 2. [サブミット] をクリックします。

CA SiteMinder によってユーザディレクトリ オブジェクトが作成されます。
- 3. [ユーザディレクトリの表示] - [ac-dir] - [内容の表示] を選択します。

ユーザストア エントリが表示されます。
- 4. [インフラストラクチャ] - [認証] - [認証方式] - [認証方式の作成] を選択し、以下のフィールドに入力します。
  - 名前 -- ac-basic-auth
  - 説明 -- CA Access Control エンタープライズ管理 基本認証
  - 認証方式タイプ - 基本テンプレート
  - 保護レベル -- 5
  - ライブラリ -- smauthdir
- 5. [サブミット] をクリックします。

CA SiteMinder によって認証方式オブジェクトが作成されます。

6. [ポリシー] - [ドメイン] - [ドメイン] - [ドメインの作成] を選択します。
7. ドメインの名前を指定します。
8. ユーザディレクトリ フレームに移動し、[追加] / [削除] をクリックします。
9. **ac-dir** を使用可能なメンバのリストから選択済みメンバのリストに移動させて、[OK] をクリックします。
10. [レルム] - [レルムの作成] を選択し、以下のフィールドに入力します。
  - 名前 -- **ac-realm**
  - エージェント -- **webserver-agent**
  - リソース フィルタ -- **/iam/**
  - デフォルト リソース保護 -- **保護**
  - 認証方式 -- **ac-basic-auth**
11. ルールフレームに移動し、[作成] を選択して以下のフィールドに入力します。
  - 名前 -- **ac-rule**
  - リソース -- **\***
  - アクセスを許可 -- **オン**
  - **Web** エージェントアクション -- **Get、Post**
12. [OK] を 2 回クリックします。
13. [ポリシー] - [作成] を選択し、以下のフィールドに入力します。
  - 名前 -- **ac-policy**
14. [ユーザ] タブに移動し、[すべて追加] を選択します。
15. [ルール] タブに移動し、[ルールの追加] をクリックし、**ac-rule** を選択して [OK] をクリックします。
16. [OK] および [サブミット] をクリックしてドメインを作成します。  
ドメインおよびレルム ポリシーが設定されました。

## 例: ユーザ認証に CA SiteMinder を使用するためのエンタープライズ管理サーバの設定

この例では、CA SiteMinder 統合に対してエンタープライズ管理サーバを設定します。

1. エンタープライズ管理サーバのホストで、以下の手順を実行します。
  - a. JBoss アプリケーション サーバを停止します。
  - b. 以下のディレクトリに移動します。ここで *JBOSS\_HOME* は、JBoss をインストールしたディレクトリです。

```
JBOSS_HOME/server/default/deploy/IdentityMinder.ear/user_console.war/WEB-INF
```

- c. `web.xml` ファイルを開き、`FrameworkAuthFilter` セクションを見つけます。
- d. 値を `false` に変更し、このファイルを保存して閉じます。以下に例を示します。

```
<filter>
  <filter-name>FrameworkAuthFilter</filter-name>

  <filter-class>com.netegrity.webapp.authentication.FrameworkLoginFilter</filter-class>
  <init-param>
    <param-name>Enable</param-name>
    <param-value>>false</param-value>
  </init-param>
</filter>
```

2. 以下のディレクトリに移動します

```
JBOSS_HOME/server/default/deploy/IdentityMinder.ear/policyserver.rar/META-INF
```

3. 以下の手順を実行します。
  - a. `ra.xml` ファイルを開き、以下のように値を `true` に変更して接続を有効にします。

```
<config-property>
  <config-property-name>Enabled</config-property-name>
  <config-property-type>java.lang.String</config-property-type>
  <config-property-value>>true</config-property-value>
</config-property>
```

- b. 以下のとおり、CA SiteMinder ポリシー サーバ設定に対応して FIPS モードを設定します。

```
<config-property>
  <config-property-name>FIPSMoDe</config-property-name>
  <config-property-type>java.lang.String</config-property-type>
  <config-property-value>false</config-property-value>
</config-property>
```

- c. CA SiteMinder ポリシー サーバのホスト名、IP アドレス、ポート番号を以下のように定義します。

```
<config-property>
  <config-property-name>ConnectionURL</config-property-name>
  <config-property-type>java.lang.String</config-property-type>

<config-property-value>policyservernode.example.com,44441,44442,44443</co
nfig-property-value>
</config-property>
```

- d. 管理者ユーザアカウント設定を以下のように定義します。

```
<config-property>
  <config-property-name>UserName</config-property-name>
  <config-property-type>java.lang.String</config-property-type>
  <config-property-value>siteminder</config-property-value>
</config-property>
```

- e. 以下のディレクトリにあるパスワード ツールを実行します。

```
/CA/AccessControlServer/IAMSuite/AccessControl/tools/PasswordTool
```

以下に例を示します。

```
pwdTools -FIPS -p <clear_text_password> -k
JBoss_HOME/server/default/deploy/IdentityMinder.ear/config/com/netegrity/
config/keys/FIPKey.dat
```

- f. AdminSecret を以下の暗号化コマンドの出力として以下のように定義します。

```
<config-property>
  <config-property-name>AdminSecret</config-property-name>
  <config-property-type>java.lang.String</config-property-type>

<config-property-value>{AES}:gSez2/BhDGzEKWvFmzca4w==</config-property-va
lue>
</config-property>
```

- g. AgentName を CA Access Control エンタープライズ管理 ノードエージェント名として定義します。

```
<config-property>
  <config-property-name>AgentName</config-property-name>
  <config-property-type>java.lang.String</config-property-type>
  <config-property-value>webserver-agent</config-property-value>
</config-property>
```

- h. 以下のパスワード ツール コマンドを使用して、CA Access Control エンタープライズ管理 の共有秘密鍵を暗号化します。

```
ACServerInstallDir/IAMSuite/AccessControl/tools/Passwordtool/pwdtools.bat
-FIPS -p <your_shared_secret> -k
JBoss_HOME/server/default/deploy/IdentityMinder.ear/config/com/netegrity/
config/keys/FIPSKey.dat
```

- i. AgentSecret を以下コマンドの暗号化された出力として定義します。

```
<config-property>
  <config-property-name>AgentSecret</config-property-name>
  <config-property-type>java.lang.String</config-property-type>

  <config-property-value>{AES}:gSez2/BhDGzEKWvFmzca4w==</config-property-value>
</config-property>
```

4. ファイルを保存して閉じます。  
5. 以下のディレクトリに移動します

```
JBoss_HOME/bin
```

6. run\_idm.bat を編集し、%PATH% 変数を JBoss インストールパスに設定します。例：

```
set
PATH=%PATH%;C:\jboss-4.2.3\server\default\deploy\IdentityMinder.ear\library;%
SystemRoot%\SYSTEM32;%SystemRoot%;%SystemRoot%\SYSTEM32\WBEM
```

7. ファイルを保存して閉じます。  
8. JBoss アプリケーション サーバを起動します。

CA SiteMinder 統合用にエンタープライズ管理サーバが設定されました。CA Access Control エンタープライズ管理 URL を参照し、CA SiteMinder によってログインセッションが保護されていることを確認できます。

# 第 7 章: CA ControlMinder REST API

---

このセクションには、以下のトピックが含まれています。

- [REST ベースの API \(P. 85\)](#)
- [スキーマの取得 \(P. 88\)](#)
- [アカウントの作成 \(P. 89\)](#)
- [アカウントの更新 \(P. 91\)](#)
- [アカウントの削除 \(P. 93\)](#)
- [アカウントの取得 \(P. 94\)](#)
- [アカウントの取得 \(P. 95\)](#)
- [アカウントのチェックイン \(P. 95\)](#)
- [アカウントのチェックアウト \(P. 96\)](#)
- [アカウントの \*\*break glass\*\* \(P. 97\)](#)
- [パスワードのリセット \(P. 98\)](#)
- [パスワードの自動リセット \(P. 99\)](#)
- [エンドポイントの作成 \(P. 100\)](#)
- [エンドポイントの更新 \(P. 102\)](#)
- [エンドポイントの削除 \(P. 103\)](#)
- [エンドポイントの取得 \(P. 103\)](#)
- [エンドポイントの取得 \(P. 104\)](#)
- [エンドポイントタイプの取得 \(P. 104\)](#)
- [アカウントリクエストの作成 \(P. 105\)](#)
- [アカウントリクエストの削除 \(P. 106\)](#)
- [リクエストするアカウントパスワードの取得 \(P. 107\)](#)
- [アカウントリクエストの取得 \(P. 108\)](#)

## REST ベースの API

REST (Representational State Transfer) は、URL でアクセス可能なオブジェクトの状態を作成および変更するために、ハイパーメディアの固有のプロパティに依存するソフトウェアのアーキテクチャスタイルの特徴を表します。

RESTful シナリオでは、ドキュメント (オブジェクトの状態を表す) がクライアントとサービスの間で交換されます。これは、どちらの側も 1 つの要求または応答に含まれているエンティティ以外については一切認識していないという前提で行われます。

REST-based API のスキーマを取得するには、以下の URL にアクセスし、空のページのソースを参照します。

`https://hostname:18443/iam/api/1.0/restapi/schemas`

**注:** スキーマの詳細については、このセクションの例を参照してください。

REST リクエストを使用して、カスタムまたはサードパーティプログラムと、エンタープライズ管理サーバユーザ インターフェースをバイパスする共有アカウント管理 データベースの間で通信できます。

## HTTP 動詞

可能な場合、CA ControlMinder REST API は以下の適切な HTTP 動詞を各アクションに使用します。

### GET

アカウント、エンドポイントおよびアカウント リクエストの取得に使用されます。

### POST

アカウント、エンドポイントおよびアカウント リクエストの作成に使用されます。

### PUT

アカウント、エンドポイントおよびアカウント リクエストの更新に使用されます。

### DELETE

アカウント、エンドポイントおよびアカウント リクエストの削除に使用されます。

## 例: HTTP 操作

サポートされた REST-based API コマンドのスキーマ例を以下に示します。

### ■ HTTP POST :

```
POST /iam/api/1.0/restapi/environments/ac/endpoints/endpointname/accounts
HTTP/1.1
Content-type: application/xml; charset=UTF-8
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Cache-Control: no-cache
Pragma: no-cache
Host: 10.112.196.244
Accept: text/html, image/gif, image/jpeg, *, q=.2, */*; q=.2
Connection: keep-alive
Content-Length: 79
```

以下の例は、アカウントを作成する HTTP POST 本文のコンテンツです。

```
<Account>
<Name>myaccount_name</Name>
<Disconnected>>true</Disconnected>
<Type>Shared</Type>
<Container>MS SQL Logins</Container>
<PasswordPolicy>default password policy</PasswordPolicy>
<PasswordState>CheckedIn</PasswordState>
<Exclusive>>false</Exclusive>
<ChangePasswordOnCheckOut>>false</ChangePasswordOnCheckOut>
<ChangePasswordOnCheckIn>>false</ChangePasswordOnCheckIn>
<LoginApplicationCheckoutOnly>>false</LoginApplicationCheckoutOnly>
<Owner ownerType="Group">my_group</Owner>
</Account>
```

### ■ HTTP GET :

```
GET /iam/api/1.0/restapi/environments/ac/endpoints/endpointname HTTP/1.1
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: 10.112.196.169:9998
```

### ■ HTTP PUT :

```
PUT /iam/api/1.0/restapi/environments/ac/endpoints/endpointname/accounts
HTTP/1.1
Content-type: application/xml; charset=UTF-8
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Cache-Control: no-cache
Pragma: no-cache
Host: 10.112.196.244
Accept: text/html, image/gif, image/jpeg, *, q=.2, */*; q=.2
Connection: keep-alive
Content-Length: 959
```

以下の例は、アカウントを更新する HTTP PUT 本文のコンテンツです。

```
<Account>
<Name>myaccount_name</Name>
<Disconnected>>true</Disconnected>
<Type>Shared</Type>
<Container>MS SQL Logins</Container>
<PasswordPolicy>default password policy</PasswordPolicy>
<PasswordState>CheckedIn</PasswordState>
<Exclusive>>false</Exclusive>
<ChangePasswordOnCheckOut>>false</ChangePasswordOnCheckOut>
<ChangePasswordOnCheckIn>>false</ChangePasswordOnCheckIn>
<LoginApplicationCheckoutOnly>>false</LoginApplicationCheckoutOnly>
<Owner ownerType="Group">my_group</Owner>
</Account>
```

- HTTP DELETE :

```
DELETE /iam/api/1.0/restapi/environments/ac/endpoints/endpointname HTTP/1.1
Content-type: application/xml; charset=UTF-8
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Cache-Control: no-cache
Pragma: no-cache
Host: 10.112.196.244
Accept: text/html, image/gif, image/jpeg, *, q=.2, */*; q=.2
Connection: keep-alive
```

## REST-based 認証

CA ControlMinder REST リクエストには、リクエスト情報の一部として認証情報が含まれます。CA ControlMinder は HTTP 基本認証方式をサポートします。たとえば、以下の基本認証を使用できます。

```
Authorization: Basic
c3VwZXJhZG1pbjpkZWZhdWx0c3VwZXJhZG1pbjpkZWZhdWx0
```

上記の例は、ユーザ "superadmin" およびパスワード "default" の Base 64 エンコーディングを表しています。

## スキーマの取得

アカウント リクエスト スキーマを取得するには、以下の URL に HTTP GET リクエストを送信します。

```
https://<host_name>:18443/iam/api/1.0/restapi/schemas
```

host\_name

ホスト名を指定します。

## アカウントの作成

アカウントを作成するには、以下の URL に HTTP POST リクエストを送信します。

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts
```

**host\_name**

ホスト名を指定します。

**endpoint\_name**

エンドポイント名を指定します。

以下の例は、アカウントを作成する HTTP 本文コンテンツを示しています。

```
<Account>
<Name>myaccount_name</Name>
<Disconnected>>true</Disconnected>
<Type>Shared</Type>
<Container>MS SQL Logins</Container>
<PasswordPolicy>default password policy</PasswordPolicy>
<PasswordState>CheckedIn</PasswordState>
<Exclusive>>false</Exclusive>
<ChangePasswordOnCheckOut>>false</ChangePasswordOnCheckOut>
<ChangePasswordOnCheckIn>>false</ChangePasswordOnCheckIn>
<LoginApplicationCheckoutOnly>>false</LoginApplicationCheckoutOnly>
<Owner ownerType="Group">my_group</Owner>
</Account>
```

**Name**

アカウント名を指定します。

**Disconnected**

アカウントが接続解除されるかどうかを指定します。

**Type**

アカウントのタイプを指定します。

### Container

コンテナを指定します。

### PasswordPolicy

アカウントに対して実装されるパスワードポリシーを指定します。

### PasswordState

アカウントのパスワード状態を指定します。

### Exclusive

アカウントが排他的かどうかを指定します。

### ChangePasswordOnCheckOut

アカウントのチェックアウト時にパスワードが変更されるかどうかを指定します。

### ChangePasswordOnCheckIn

アカウントのチェックイン時にパスワードが変更されるかどうかを指定します。

### LoginApplicationCheckoutOnly

ログインアプリケーションがアカウントをチェックアウトするかどうかを指定します。

### Owner

所有者のタイプを指定します。

## アカウントの更新

アカウントを更新するには、以下の URL に HTTP PUT リクエストを送信します。

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>
```

**host\_name**

ホスト名を指定します。

**endpoint\_name**

エンドポイント名を指定します。

**account\_name**

アカウント名を指定します。

以下の例は、アカウントを更新する HTTP 本文コンテンツを示しています。

```
<Account>
<Name>myaccount_name</Name>
<Disconnected>>true</Disconnected>
<Type>Shared</Type>
<Container>MS SQL Logins</Container>
<PasswordPolicy>default password policy</PasswordPolicy>
<PasswordState>CheckedIn</PasswordState>
<Exclusive>>false</Exclusive>
<ChangePasswordOnCheckOut>>false</ChangePasswordOnCheckOut>
<ChangePasswordOnCheckIn>>false</ChangePasswordOnCheckIn>
<LoginApplicationCheckoutOnly>>false</LoginApplicationCheckoutOnly>
<Owner ownerType="Group">my_group</Owner>
</Account>
```

**Name**

アカウント名を指定します。

**Disconnected**

アカウントが接続解除されるかどうかを指定します。

### Type

アカウントのタイプを指定します。

### Container

コンテナを指定します。

### PasswordPolicy

アカウントに対して実装されるパスワードポリシーを指定します。

### PasswordState

アカウントのパスワード状態を指定します。

### Exclusive

アカウントが排他的かどうかを指定します。

### ChangePasswordOnCheckOut

アカウントのチェックアウト時にパスワードが変更されるかどうかを指定します。

### ChangePasswordOnCheckIn

アカウントのチェックイン時にパスワードが変更されるかどうかを指定します。

### LoginApplicationCheckoutOnly

ログインアプリケーションがアカウントをチェックアウトするかどうかを指定します。

### Owner

所有者のタイプを指定します。

## アカウントの削除

アカウントを削除するには、以下の URL に HTTP DELETE リクエストを送信します。

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>
```

**host\_name**

ホスト名を指定します。

**endpoint\_name**

エンドポイント名を指定します。

**account\_name**

アカウント名を指定します。

## アカウントの取得

特定のアカウントを取得するには、**GET** コマンドを使用します。

**注:** アカウントがチェックアウトされている場合、パスワードを表示できません。

アカウントを取得するには、以下の URL に HTTP GET リクエストを送信します。

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>
```

アカウントの取得中に、アカウント コンテナ クエリ パラメータを使用して、エンドポイントをサポートするためのコンテナを指定します。

**Active Directory** などのデフォルト以外のアカウント コンテナがあるアカウントを取得するには、以下の URL に HTTP GET リクエストを送信します。

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>
```

**host\_name**

ホスト名を指定します。

**endpoint\_name**

エンドポイント名を指定します。

**account\_name**

アカウント名を指定します。

## アカウントの取得

エンドポイント上の特権アカウントを取得するには、以下の URL に HTTP GET リクエストを送信します。

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts
```

**host\_name**

ホスト名を指定します。

**endpoint\_name**

エンドポイント名を指定します。

## アカウントのチェックイン

アカウントをチェックインするには、以下の URL に HTTP PUT リクエストを送信します。

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>
```

**host\_name**

ホスト名を指定します。

**endpoint\_name**

エンドポイント名を指定します。

**account\_name**

アカウント名を指定します。

以下の例は、アカウントをチェックインする HTTP 本文コンテンツを示しています。

```
<Account>
```

```
<PasswordState>Checked In</PasswordState>
```

```
</Account>
```

## アカウントのチェックアウト

アカウントをチェックアウトするには、以下の URL に HTTP PUT リクエストを送信します。

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>
```

**host\_name**

ホスト名を指定します。

**endpoint\_name**

エンドポイント名を指定します。

**account\_name**

アカウント名を指定します。

以下の例は、アカウントをチェックアウトする HTTP 本文コンテンツを示しています。

```
<Account>
```

```
<PasswordState>Checked Out</PasswordState>
```

```
</Account>
```

## アカウントの break glass

管理権限がないアカウントへの即時アクセスが必要な場合、ユーザは `break glass` チェックアウトを実行します。

アカウントの `break glass` を行うには、以下の URL に HTTP リクエストを送信します。

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>?breakglass-accounts=true
```

`host_name`

ホスト名を指定します。

`endpoint_name`

エンドポイント名を指定します。

`account_name`

アカウント名を指定します。

以下の例は、アカウントの `break glass` を行う HTTP 本文コンテンツを示しています。

```
<Account>
```

```
<PasswordState justification="my justification">BreakGlass</PasswordState>
```

```
</Account>
```

**注:** Break Glass 特権アクセス ロールを持つユーザのみが、`break glass` プロセスを実行できます。

## パスワードのリセット

パスワードを手動でリセットするには、以下の URL に HTTP PUT リクエストを送信します。

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>
```

**host\_name**

ホスト名を指定します。

**endpoint\_name**

エンドポイント名を指定します。

**account\_name**

アカウント名を指定します。

以下の例では、パスワードをリセットする HTTP 本文コンテンツを示しています。

```
<Account>
```

```
<Password auto="false">password</Password>
```

```
</Account>
```

## パスワードの自動リセット

パスワードをアカウントに自動的にリセットするには、以下の URL に HTTP PUT リクエストを送信します。

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>
```

**host\_name**

ホスト名を指定します。

**endpoint\_name**

エンドポイント名を指定します。

**account\_name**

アカウント名を指定します。

以下の例では、パスワードを自動的にリセットする HTTP 本文コンテンツを示しています。

```
<Account>
```

```
<Password auto="true"/>
```

```
</Account>
```

## エンドポイントの作成

エンドポイントを作成するには、以下の URL に HTTP POST リクエストを送信します。

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints
```

**host\_name**

ホスト名を指定します。

以下の例は、エンドポイントを作成する HTTP 本文コンテンツを示しています。

```
<Endpoint>
  <Name>endpoint_name</Name>
  <EndpointType>MS SQL Server</EndpointType>
  <EndpointTypeProperties>
    <UserLogin>user1</UserLogin>
    <URL>URL Value</URL>
    <Host>Endpoint_Host_Address</Host>
    <Password>User_Password</Password>
  </EndpointTypeProperties>
  <AdministrativeAdvanced>>false</AdministrativeAdvanced>
```

</Endpoint>

**Name**

エンドポイント名を指定します。

**EndpointType**

エンドポイントのタイプを指定します。

**UserLogin**

エンドポイントのユーザ ログインを指定します。

**URL**

エンドポイントの URL 値を指定します。

**Host**

エンドポイント ホスト アドレスを指定します。

**Password**

**UserLogin** タグで指定されるエンドポイント ユーザのパスワードを指定します。

**AdministrativeAdvanced**

エンドポイントが高度な管理で有効かどうかを指定します。

**注:** *EndpointTypeProperties* タグは動的で、*EndpointType* タグに対する入力によって確定されます。動的エンドポイントタイププロパティのプロパティスキーマの取得方法の詳細については、トピック「[エンドポイントタイプの取得 \(P. 104\)](#)」を参照してください。

## エンドポイントの更新

エンドポイントを更新するには、以下の URL に HTTP PUT リクエストを送信します。

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints
```

**host\_name**

ホスト名を指定します。

以下の例は、エンドポイントを更新する HTTP 本文コンテンツを示しています。

```
<Endpoint>
  <Name>endpoint_name</Name>
  <EndpointType>Endpoint_type</EndpointType>
  <EndpointTypeProperties>
    <UserLogin>user1</UserLogin>
    <URL>URL Value</URL>
    <Host>Endpoint_Host_Address</Host>
    <Password>User_Password</Password>
  </EndpointTypeProperties>
  <AdministrativeAdvanced>false</AdministrativeAdvanced>
</Endpoint>
```

**Name**

エンドポイント名を指定します。

**EndpointType**

エンドポイントのタイプを指定します。

**UserLogin**

エンドポイントのユーザ ログインを指定します。

**URL**

エンドポイントの URL 値を指定します。

**Host**

エンドポイント ホスト アドレスを指定します。

**Password**

UserLogin タグで指定されるエンドポイント ユーザのパスワードを指定します。

**AdministrativeAdvanced**

エンドポイントが高度な管理で有効かどうかを指定します。

## エンドポイントの削除

エンドポイントを削除するには、以下の URL に HTTP DELETE リクエストを送信します。

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>
```

**host\_name**

ホスト名を指定します。

**endpoint\_name**

エンドポイント名を指定します。

## エンドポイントの取得

すべてのエンドポイントを取得するには、以下の URL に HTTP GET リクエストを送信します。

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>
```

**host\_name**

ホスト名を指定します。

**endpoint\_name**

エンドポイント名を指定します。

## エンドポイントの取得

エンドポイントをすべて取得するには、`get endpoints` コマンドを使用します。

すべてのエンドポイントを取得するには、以下の URL に HTTP GET リクエストを送信します。

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints
```

`host_name`

ホスト名を指定します。

## エンドポイントタイプの取得

エンドポイントタイプをすべて取得するには、`get endpoint types` コマンドを使用します。

すべてのエンドポイントタイプを取得するには、以下の URL に HTTP GET リクエストを送信します。

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoint-types
```

`EndpointTypeProperties` タグは動的で、`EndpointType` タグに対して指定された入力によって決定されます。プロパティスキーマを取得するには、以下の URL を使用します。

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoint-types/<host_name>/properties-schema
```

`host_name`

ホスト名を指定します。

## アカウントリクエストの作成

アカウントリクエストを作成するには、以下の URL に HTTP POST リクエストを送信します。

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>/accountrequest
```

**host\_name**

ホスト名を指定します。

**endpoint\_name**

エンドポイント名を指定します。

**account\_name**

アカウント名を指定します。

以下の例は、アカウントリクエストを作成する HTTP 本文コンテンツを示しています。

```
<AccountRequest>
  <StartTime>Start_Time</StartTime>
  <ValidUntilTime>Valid_Until_Time</ValidUntilTime>
  <User>
    <Name>user1</Name>
  </User>
  <Approver>
    <User>
      <Name>superadmin</Name>
    </User>
  </Approver>
  <Justification>user1 requests</Justification>
</AccountRequest>
```

**StartTime**

依頼者ユーザが共有アカウントリクエストタスクを実行できる開始時間を指定します。

日付を以下の形式で入力します。

yyyy-mm-ddThh:mm:sec

**ValidUntilTime**

それ以降ユーザが共有アカウントリクエストタスクを実行できなくなる、有効な時間を指定します。

日付を以下の形式で入力します。

yyyy-mm-ddThh:mm:ss

### Name

依頼者のユーザ名を指定します。

<承認者> <ユーザ>名前

承認者のユーザ名を指定します。

### Justification

正当化のコメントを指定します。

## アカウントリクエストの削除

アカウントリクエストを削除するには、以下の URL に HTTP DELETE リクエストを送信します。

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>/accountrequest/<account_request_name>
```

host\_name

ホスト名を指定します。

endpoint\_name

エンドポイント名を指定します。

account\_name

アカウント名を指定します。

account\_request\_name

アカウントリクエスト名を指定します。

## リクエストするアカウント パスワードの取得

ユーザがリクエストできるアカウント パスワードをすべて取得するには、以下の URL に HTTP GET リクエストを送信します。

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts?to-request=true
```

**host\_name**

ホスト名を指定します。

**endpoint\_name**

エンドポイント名を指定します。

## アカウントリクエストの取得

特定のアカウントリクエスト、たとえば **exc-113** を取得するには、以下の URL に HTTP GET リクエストを送信します。

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>/accountrequests/exc-113
```

アカウントリクエスト（特権アカウント (**account\_name**) に対するアクセス権がある）をすべて取得するには、以下の URL に HTTP GET リクエストを送信します。

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>/accountrequests
```

環境全体のアカウントリクエストをすべて取得するには、以下の URL に HTTP GET リクエストを送信します。

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints?display=accountrequests
```

**host\_name**

ホスト名を指定します。

**endpoint\_name**

エンドポイント名を指定します。

**account\_name**

アカウント名を指定します。