CA Identity Manager™

実装ガイド

12.6.4

ca technologies

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 CloudMinder™ Identity Management
- CA ディレクトリ
- CA Identity Manager ™
- CA Identity Governance（旧 CA GovernanceMinder）
- CA SiteMinder®
- CA User Activity Reporting
- CA AuthMinder ™

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: アイデンティティとアクセスの管理

このセクションには、以下のトピックが含まれています。

ユーザ管理とアプリケーション アクセス

典型的な IT （Information Technology）部門では、ユーザ アカウントのメンテナンス要求が常に発生します。 IT 管理者は、忘れたパスワードのリセット、新規アカウントの作成、消耗品や事務機器の提供など、ユーザの緊急ニーズに対処する必要があります。

同時に、アプリケーションに対するさまざまなアクセス レベルをユーザに提供する必要もあります。たとえば、部門管理者が発注書を作成し、財務アプリケーションのアカウントを必要とすることがあります。

IT に関する要求の拡大に対応するため、CA Identity Manager では、ユーザとそのプリケーション アクセスを管理するための、以下のような統合された方法を提供します。

- ロールによる権限の割り当て。 具体的な内容は次のとおりです。
  - 管理者によるユーザ アカウントの作成とメンテナンスを可能にするロール
  - 既存ユーザに追加アカウントをプロビジョニングするロール（ただし、プロビジョニング のサポートが必要）
- ユーザおよびアプリケーション アクセスの管理の委任
- アカウントを自己管理するためのセルフ サービス オプション
- ビジネス アプリケーションと CA Identity Manager の統合
- CA Identity Manager をカスタマイズおよび拡張するオプション

ロール ベース権限

ユーザにロールを割り当てることにより、権限を割り当てます。 ロールに含まれるタスクには、ユーザの作成タスクなどの CA Identity Manager 内のアプリケーション機能、発注書の作成機能などのアプリケーション内の機能に相当する機能、または SAP アカウントなどのユーザ アカウントを付与するアカウント テンプレートが含まれます。 ユーザにロールが割り当てられると、対応する権限が付与されます。

CA Identity Manager では、以下のタイプのロールを提供します。

- ユーザ管理ロール。 *管理ロール*と呼ばれます。

  管理ロールには、ユーザ コンソール に表示される任意のタスクを含めることができます。
- アカウント割り当てロール。 *プロビジョニング ロール*と呼ばれます。
- アプリケーション機能ロール。 *アクセス ロール*と呼ばれます。

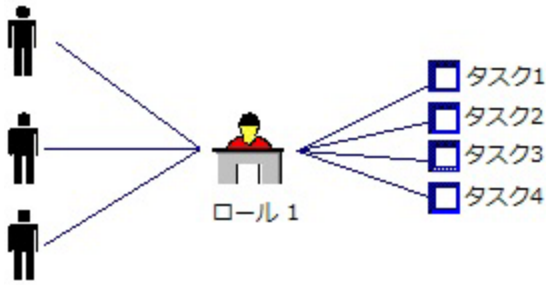
ロールからタスクまたはアカウント テンプレートを削除すると、ユーザはそのタスクの実行、エンドポイント アカウントの使用、またはアプリケーション機能の使用ができなくなります。

管理ロール

管理ロールは、ユーザが CA Identity Manager で何を実行できるかを制御します。 システム管理者は、ロールをユーザに割り当てます。そのロールは、ユーザが実行できるタスクのセットを定義します。 ユーザは、パスワードの変更や職位の更新といった、ユーザ アカウントに対する管理 *タスク*を実行できます。

これらのタスクに対しては、ユーザによって異なるレベルのアクセス権があります。 たとえば、従業員ロールには、ユーザの名前や住所を変更する権限を付与するタスクが含まれ、人事マネージャ ロールには、ユーザの職位および給与を変更するタスクが含まれます。

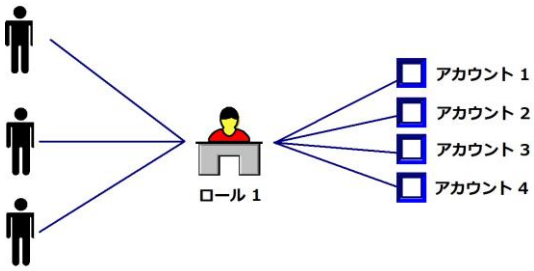
以下の図では、4 つのタスクが 1 つの管理ロールに統合され、3 ユーザに割り当てられていることを示します。



プロビジョニング ロール

電子メール システムなど、追加アプリケーションのアカウントへのアクセスをユーザに付与するには、プロビジョニング ロールを割り当てます。プロビジョニング ロールにはアカウント テンプレートが含まれています。アカウント テンプレートは、あるタイプのアカウントに存在する属性を定義します。 たとえば、Exchange アカウント用のアカウント テンプレートは、メールボックスのサイズなど属性を定義します。の アカウント テンプレートでは、CA Identity Manager ユーザ属性とアカウントのマッピング方法も定義できます。

以下の図では、4 つのアカウントが 1 つのプロビジョニング ロールに統合され、3 ユーザに割り当てられていることを示します。プロビジョニング ロールをユーザに割り当てると、各ユーザは 4 つのアカウントを受信します。



アクセス ロール

アクセス ロールは、CA Identity Manager または他のアプリケーションにおける権限付与の追加的な方法を提供します。たとえば、アクセス ロールを使用して以下の処理を実行できます。

- ユーザ属性に間接的なアクセス権を付与する
- 複合式を作成する
- 権限を決定するために他のアプリケーションで使用される、ユーザ プロファイルの属性を設定する

アクセス ロールは、ユーザまたはユーザのグループに一連のビジネス変化を適用するという点でアイデンティティ ポリシーに似ています。ただし、アクセス ロールを使用してビジネス変化を適用すると、アクセス ロールのメンバを表示して、この変化の適用先のユーザを確認できます。

ほとんどの場合、アクセス ロールはタスクと関連付けられていません。

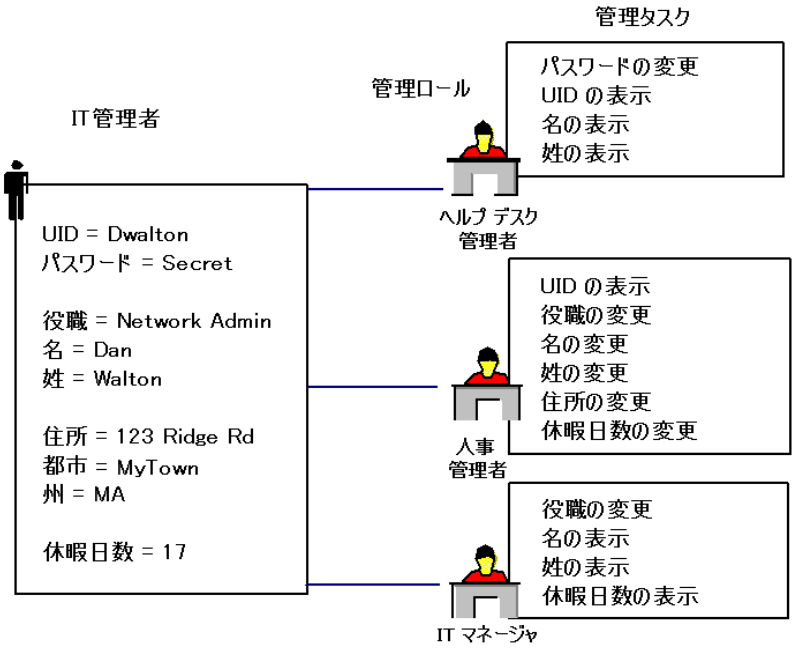
注: CA Identity Manager が CA SiteMinder と統合されると、アクセス ロールは CA SiteMinder によって保護されるアプリケーションへのアクセスも提供できます。この場合、アクセス ロールにはアクセス タスクが含まれます。詳細については、*「設定ガイド」*の SiteMinder 統合についての章を参照してください。

ユーザー アカウント管理の管理ロール

CA Identity Manager では、管理ロールによって、ユーザ ストア オブジェクト（ユーザ、グループ、組織）を管理できます。 また、管理ロールを使用すると、ユーザ ストア オブジェクトの管理に使用するロールとタスクも管理できます。たとえば、管理ロールを使用して、ユーザのプロファイル属性を変更したり、ユーザに自分のアカウントを管理するオプションを提供したり、ワークフローを使用するタスクを承認できます。

属性レベルでのプロファイル管理

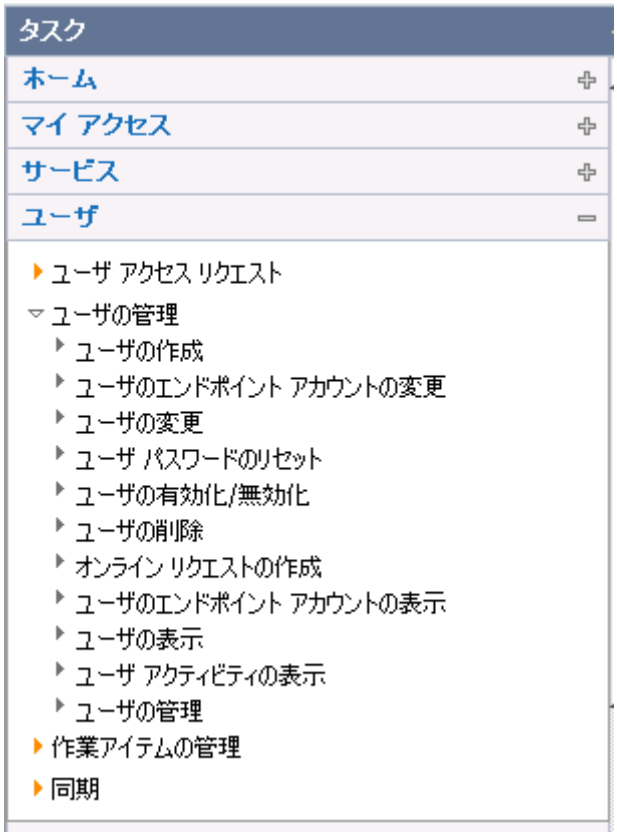
さまざまなプロファイル属性の読み取りまたは書き込みを必要とするさまざまな管理者の管理ロールを作成できます。たとえば、会社にユーザ プロファイルを操作する数名の従業員がおり、各自がさまざまな属性にアクセスする場合があります。 以下の図は、3 つのロールとそれらの関連タスクを示しています。 ロールごとに、プロファイル属性へのアクセス権が異なります。



この例では、3 つのロールで、同じユーザ（Dan Walton）のさまざまな属性を管理できます。

- ヘルプ デスク管理者はユーザ名とアドレスを表示し、ユーザ パスワードをリセットします。
- 人事管理者は、ユーザ ID、ユーザ名、アドレス、役職、および休暇日数を変更します。
- IT マネージャは、ユーザの役職を変更し、ユーザの名前とその休暇日数を表示します。

CA Identity Manager へのログイン時のロールに関わらず、CA Identity Manager アカウントに割り当てられた管理ロールに基づいて、カテゴリと呼ばれる一連のタブが表示されます。 タブをクリックすると、そのカテゴリで実行できるタスクが表示されます（下図参照）。



表示されるカテゴリとそのカテゴリのタスクは、ユーザの管理ロールによって決まります。

管理タスクのワークフロー承認

ビジネス プロセスの自動化を促すため、ワークフロー プロセスを生成する管理タスクを設計できます。 *ワークフロー プロセス*は、会社で頻繁に繰り返され、十分に定義された手順を自動化します。 CA Identity Manager には WorkPoint ワークフロー エンジンが含まれています。

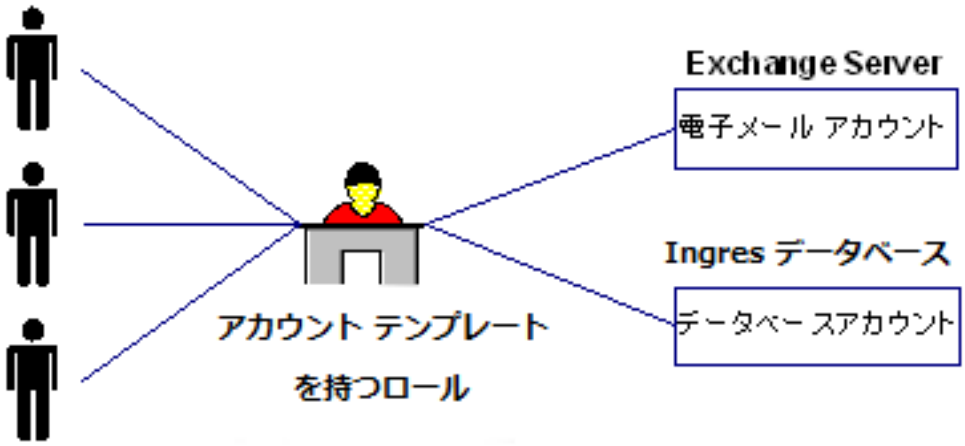
ワークフロー プロセスは、管理タスクに含まれた CA Identity Manager イベントによってトリガされます。 たとえば、「ユーザの作成」タスクには、「CreateUserEvent」と「AddToGroupEvent」と呼ばれるイベントが含まれています。イベントが発生すると、ワークフロー エンジンは、以下のことができます。

- 承認の要求 - CA Identity Manager がユーザ ストアを更新する前に、承認者はイベント（ユーザ プロファイルの変更など）を承認する必要があります。 承認者とは、特定タスクの承認者ロールを持つ管理者です。
- 通知の送信 - ワークフロー エンジンは、プロセスのさまざまな段階で（ユーザによるイベント開始時、イベントの承認時など）イベントのステータスをユーザに通知できます。
- ワーク リストの生成 - ワーク リストは、特定ユーザが実行する必要のあるタスクを指定します。管理者のワーク リストは、ワークフロー エンジンが自動的に更新します。

共通イベントについては、CA Identity Manager と共に提供されるワークフロー プロセスを使用できます。 あるいは、カスタム ワークフロー プロセスを作成することもできます。

追加アカウント用プロビジョニング ロール

CA Identity Manager では、プロビジョニング ロールを使用して、ユーザに追加アカウントを提供できます。プロビジョニング ロールには、アカウント テンプレートが含まれています。このテンプレートでは、電子メール サーバなど管理対象エンドポイントに存在するアカウントが定義されます。 CA Identity Manager にユーザができると、それらのユーザの一部にプロビジョニング ロールを割り当てることができます。 ユーザは、ロールのテンプレートによって定義されたアカウントを受け取ります。



アカウント テンプレートでは、アカウントの特性が定義されます。 たとえば、Exchange アカウントのアカウント テンプレートで、メールボックスのサイズを定義することがあります。アカウント テンプレートでは、ユーザ属性とアカウントのマッピング方法も定義できます。

プロビジョニング ロールを使用するには、CA Identity Manager サーバと共にプロビジョニング サーバをインストールします。 次に、ユーザ コンソール でアカウント テンプレートを作成します。

パスワード管理

CA Identity Manager は、以下のユーザ パスワード管理機能を備えています。

- パスワード ポリシー: これらのポリシーでは、パスワードの有効期限、構成、および使用方法を管理するルールと制限を適用することで、ユーザ パスワードを管理します。

  注: 高度なパスワード ポリシーの場合は、SiteMinder との統合を設定します。詳細については、「インストール ガイド」を参照してください。

- パスワード マネージャ : パスワード マネージャ ロールを持つ管理者は、ユーザがヘルプ デスクに連絡してくると、パスワードをリセットできます。

- セルフサービス パスワード管理 : CA Identity Manager には、ユーザによるパスワードの自己管理を可能にするいくつかのセルフサービス タスクがあります。 以下のタスクが実行できます。

  - 自己登録 - ユーザは企業の Web サイトで登録する際にパスワードを指定します。

  - マイ パスワードの変更 - ユーザは、IT 担当者やヘルプデスク担当者からのサポートなしで、自分のパスワードを変更できます。

  - 忘れたパスワード - ユーザは、CA Identity Manager による身元の確認後、忘れたパスワードをリセットまたは取得できます。

  - 忘れたユーザ ID - ユーザは、CA Identity Manager による身元の確認後、忘れたユーザ ID を取得できます。

- パスワード同期（プロビジョニングと併用の場合のみ） : パスワードの変更が、CA Identity Manager と、エンドポイントと呼ばれるターゲット システム上のアカウントで同期されます。新しいパスワードは、CA Identity Manager パスワード ポリシーに照らして検証されます。

ユーザ用セルフ サービス オプション

さらに IT 作業負荷を軽減するため、CA Identity Manager には、新規ユーザを登録し、忘れたパスワードを提供する機能が含まれています。 これらの機能は、管理者の関与を必要としません。ユーザは、ログイン アカウントのいらない*パブリック コンソール*から CA Identity Manager にアクセスできます。このコンソールでは、サイトに自己登録したり、忘れたパスワードを思い出すための情報を要求できます。

IT 管理者の時間を節約するため、CA Identity Manager ユーザは自分のアカウントを管理できます。 ユーザは、自己管理ロールを持っているので、以下のことができます。

- 個人情報のメンテナンス
- 自分のパスワードの変更
- 自己登録グループへの参加

カスタマイズと拡張性

以下の CA Identity Manager の特長をカスタマイズします。

- CA Identity Manager に対してユーザ ストアの構造を記述する CA Identity Manager ディレクトリ。
- ユーザ インターフェースの外観および機能。
- 各タスク画面のフィールドとレイアウトを決定するユーザ入力画面。
- 正規表現、JavaScript、または Java 実装の使用によるユーザ データ エントリの検証。
- 自動ワークフロー プロセスを定義するワークフロー。 WorkPoint Process Designer で承認者とアクションをリンクすることで、プロセスを作成または変更します。
- タスクのステータスをユーザに通知する電子メール メッセージ。
- サードパーティ アプリケーションで CA Identity Manager TEWS（Task Execution Web Service）に送信できるタスク サブミット。 TEWS はリモート タスク要求を処理します。 リモート タスク要求は WSDL 標準に準拠します。

以下の API を使用すると、CA Identity Manager の機能を拡張できます。

- 論理属性 API - ユーザ ディレクトリでの物理的な保存形式とは異なる形式で属性を表示できます。
- ビジネス ロジック タスク ハンドラ API - データの妥当性検証または変換操作時にカスタム ビジネス ロジックを実行できます。
- ワークフロー API - ワークフロー プロセス内のカスタム スクリプトに情報を提供します。スクリプトは、情報を評価し、ワークフロー プロセス パスを適宜決定します。
- 参加者リゾルバ API - ワークフロー アクティビティを承認する権限を持つ参加者のリストを指定できます。
- イベント リスナ API - 特定の CA Identity Manager のイベントまたはイベント グループをリスンするカスタム イベント リスナを作成できます。イベントが発生すると、イベント リスナはカスタム ビジネス ロジックを実行できます。
- 通知ルール API - 電子メール通知を受信するユーザを決定できます。
- 電子メール テンプレート API - 電子メール通知にイベント固有の情報を含めます。

注: CA Identity Manager API の詳細については、「Java のプログラミング ガイド」を参照してください。

CA Identity Manager にプロビジョニングが含まれる場合は、以下のようにプロビジョニング機能も拡張できます。

- カスタム コネクタ - プロビジョニング サーバとエンドポイント システム間の通信を可能にします。 コネクタを構成するコードには GUI プラグイン、サーバ プラグイン、およびエージェント プラグインを含めることができます。

  動的コネクタは Connector Xpress で生成できます。また、カスタムの静的コネクタは Java または C++ で開発できます。

  注: 詳細については、「Connector Xpress ガイド」を参照してください。
- プログラム出口 - プロビジョニング サーバのプロセス フローからカスタム コードを参照できます。

注: プロビジョニング機能の拡張の詳細については、「*Programming Guide for Provisioning*」を参照してください。このガイドは、Legacy Components メディアから利用できます。

CA Identity Governance の統合

CA Identity Governance は、ロール モデルを迅速かつ正確に開発し、メンテナンスし、分析することを可能にするアイデンティティ ライフサイクル管理製品です。また、集中管理されたアイデンティティ コンプライアンス ポリシー制御と、コンプライアンスとセキュリティの要求を満たすプロセスの自動化を可能にします。CA Identity Governance を使用すると、以下を実行できるようになります。

- CA Identity Manager ユーザ権限がビジネス コンプライアンス ポリシーに従って付与されているかどうかの検証
- CA Identity Manager ユーザ、ロール、およびアカウントの作成または変更時における推奨されたロールおよびコンプライアンス チェックの取得
- 組織に存在するロールの確認、組織に適合するロール モデルの確立、および CA Identity Manager 内の必要なロール モデルの再作成
- ビジネスの成長に合わせたロール モデルの分析と保守

CA Identity Manager は、以下の 2 つの方法で CA Identity Governance と統合します。

- CA Identity Manager の CA Identity Governance コネクタ

  CA Identity Manager と CA Identity Governance の間で権限データを自動的に同期する特別なタイプのコネクタ。 このコネクタを使用して、CA Identity Manager から CA Identity Governance へのデータのインポート、または CA Identity Governance から CA Identity Manager へのデータのエクスポートを行うことができます。

- スマート プロビジョニング

  CA Identity Manager が CA Identity Governance と統合している場合は、日常のアイデンティティ管理操作をサポートするため、ロールおよびコンプライアンス情報（ロール モデルで入手可能）の使用を可能にする追加機能を設定できます。CA Identity Manager で変更を行うと、CA Identity Governance のロール モデルが動的に更新されます。

注: CA Identity Manager と CA Identity Governance の統合の詳細については、CA Identity Governance マニュアル選択メニューにある「CA Identity Manager 統合ガイド」を参照してください。

CA User Activity Reporting との統合

CA Identity Manager r12.6 以降、CA Enterprise Log Manager は、CA UAR （CA User Activity Reporting） と呼ばれます。

CA UAR は CEG （CA Common Event Grammar）を使用して、さまざまなシステムで生成されるイベントを標準形式にマップし、まだマップされていないイベントも含め、すべてのイベントをレビューおよび分析用に保存します。 さらに、CA UAR は、各種の情報およびイベントを検索するため、設定可能なデータベース クエリおよび/またはレポートを使用して、収集データの管理およびレポート用の大量のソリューションを提供します。

CA UAR は、管理対象でないシステムと CA Identity Manager の範囲および制御外のシステムに対するより良く、広く、深い洞察を提供します。また、アイデンティティのより詳細な調査も可能にします。

CA Identity Manager との統合により、CA Identity Manager ユーザ コンソールを使用して、CA UAR のアイデンティティ中心のレポートおよび/または動的クエリ を CA UAR ユーザ コンソールに表示できます。 このユーザ コンソールから、特定の アイデンティティをさらに詳細に調査しながら、既存の CA Identity Manager/ CA UAR レポートおよび/またはクエリの表示および変更方法を設定することができます。

CA UAR レポート

以下の CA UAR レポートは、デフォルトで CA UAR ロール定義と共に提供されます。

タスク	呼び出されるレポート
システム ユーザ別全イベント	CA Identity Manager - ユーザ ID でフィルタリングされたシステムの全イベント
アカウント管理（ホスト別）	アカウント管理（ホスト別）
アカウント作成（アカウント別）	アカウント作成（アカウント別）
アカウント削除（アカウント別）	アカウント削除（アカウント別）
アカウント ロックアウト（アカウント別）	アカウント ロックアウト（アカウント別）
認証プロセス アクティビティ（ホスト別）	CA Identity Manager - プロセス アクティビティ（ホスト別）
パスワード ポリシーの変更アクティビティ	CA Identity Manager - ポリシー変更アクティビティ

第 2 章: ビジネス ニーズへの対応

このセクションには、以下のトピックが含まれています。

ビジネス変更の処理

アイデンティティ ポリシーの使用により、一定のアイデンティティ管理タスクの処理を自動化できます。 アイデンティティ ポリシーは、ユーザが特定の条件やルールを満たすと発生する一連のビジネス変更です。アイデンティティ ポリシー セットを使用して以下の処理を実行できます。

- ロールやグループ メンバシップの割り当て、リソースの割り当て、ユーザ プロファイル属性の変更といった、特定のアイデンティティ管理タスクを自動化する。
- 職務の分離を適用する。 (P. 28) たとえば、アイデンティティ ポリシー セットを作成し、Check Signer ロールのメンバが Check Approver ロールを所有することを禁止して社内の人間が $10,000 を超える小切手を書くことを制限することができます。
- コンプライアンスを適用する。 たとえば、特定の役職に就いており給与が $100,000 を超えるユーザを監査できます。

  コンプライアンスを適用するアイデンティティ ポリシーは、*コンプライアンス ポリシー*と呼ばれます。

アイデンティティ ポリシーに関連付けられるビジネス変化には以下のものがあります。

- プロビジョニング ロールを含むロールの割り当てまたは取り消し（CA Identity Manager がプロビジョニングを含む場合）
- グループ メンバシップの割り当てまたは取り消し
- ユーザ プロファイルの属性の更新

たとえば、ある企業では、副社長は全員カントリー クラブ メンバー グループに所属しており、給与承認者ロールを所有していることを記述するアイデンティティ ポリシーを作成する場合があります。ユーザの役職が副社長に変わり、そのユーザがアイデンティティ ポリシーに同期されると、CA Identity Manager は、そのユーザを適切なグループおよびロールに追加します。副社長が CEO に昇進すると、副社長アイデンティティ ポリシーの条件を満たさなくなります。よって、このポリシーで適用されていた変更は取り消され、CEO ポリシーに基づいた新しい変更が適用されます。

アイデンティティ ポリシーに基づいて発生する変更アクションには、ワークフロー制御下で監査できるイベントが含まれます。 前の例では、給与承認者ロールによって、所属するメンバに重要な権限が付与されます。 給与承認者ロールを保護するために、企業は、ロールの割り当て前に一連の承認を必要とするワークフロー プロセスを作成し、さらにロールの割り当てを監査するように CA Identity Manager を設定できます。

アイデンティティ ポリシーの管理を簡略化するため、アイデンティティ ポリシーはアイデンティティ ポリシー セットとしてグループ化されます。 たとえば、副社長ポリシーと CEO ポリシーを、幹部権限アイデンティティ ポリシー セットの一部とすることができます。

ビジネス ポリシーへのコンプライアンス

コンプライアンスとは、企業とその従業員がビジネス ポリシーに準拠していることを確認する広範な手順を含んだコーポレート ガバナンスです。これらのコンプライアンス手順には通常、アプリケーションやシステムへの資格の割り当てに対する監査、自動化、および文書化が含まれます。

CA Identity Manager には、このようなコンプライアンス管理をサポートする以下の機能が含まれます。

- **スマート プロビジョニング**

  スマート プロビジョニングは、CA Identity Manager が CA Identity Governance と統合している場合に、プロビジョニング ロールの割り当てを簡略化する機能の集まりです。 この機能には、以下が含まれます。

  - サジェストされたプロビジョニング ロール

    CA Identity Manager は、管理者にユーザへの割り当てが適切なプロビジョニング ロールのリストを提供します。このプロビジョニング ロールのリストは、管理者が入力した基準に基づいて、CA Identity Governance によって決定されます。

    サジェストされたプロビジョニング ロールによって、ユーザは、会社のロール モデルを保持しつつ、適切な権限を持つことができます。

- コンプライアンス メッセージおよびパターン メッセージ

  CA Identity Manager 管理者は、変更をコミットする前に、CA Identity Governance 内のロール モデルに対して提案された変更を検証できます。コミットする前に変更を検証することにより、各操作に定義したロール モデルを維持できます。

  ユーザは、プロビジョニング ロールに対する提案済みの変更（ロールの割り当てまたは削除）の検証およびユーザ属性に対する変更の検証を行うことができます。

  CA Identity Manager では、以下の 2 種類のポリシー検証を実行します。

  - コンプライアンス

    提案済みの変更は、それが CA Identity Governance 内の明示的な事前定義済みビジネス ポリシーに違反しているかどうか確認するために、CA Identity Governance のロール モデルと照合して検証されます。

  - パターン

    CA Identity Manager は、提案された変更と CA Identity Governance ロール モデルを比較し、提案された変更によって変更対象が「パターン外」となるかどうかを確認します。また、変更がロール モデル内で確立されたパターンを大きく変えないことも確認します。

    ユーザが特定のタスクを遂行する場合に、このような検証を自動で実行するか、ユーザが手動で開始できるようにするかを CA Identity Manager で設定できます。

CA Identity Governance に CA Identity Manager データに基づいて確立されたロール モデルがあると、CA Identity Manager 環境にスマート プロビジョニングを実装できます。

注: 詳細については、「管理ガイド」を参照してください。

- **アイデンティティ ポリシー**

  ユーザが他の権限をもっている場合に特定の権限を持つことを禁止するコンプライアンス ポリシー（アイデンティティ ポリシー (P. 23)の 1 種）を作成できます。 たとえば、小切手を承認できるユーザが、小切手を発行することを禁止できます。

  コンプライアンス ポリシーでは、使用環境における義務を分離する必要があります。

- **コンプライアンス レポート**

  CA Identity Manager には、環境内のユーザのコンプライアンス ステータスを表示するサンプル レポートが組み込まれています。これらのレポートを使用すれば、ビジネス ポリシーに準拠しないユーザを確認できます。

コンプライアンス レポート

CA Identity Manager には、法人企業ポリシーへのコンプライアンスの監視に使用できるサンプル レポートが含まれています（下表参照）。

レポート	Description
ロール メンバ	レポート データベース内のロールを表示し、それらのロールのメンバをリストします。
ロール	レポート データベースの各ロールに関する以下の情報が表示されます。 ■ ロールに関連付けられているタスク ■ メンバ ポリシーとロール メンバ ■ 管理者ポリシーとロール管理者 ■ 所有者ポリシーとロールの所有者
タスク ロール	レポート データベース内のタスクと、それらのタスクが関連付けられているロールを表示します。
ユーザ ロール	レポートデータベース内のユーザを表示し、各ユーザのロールをリストします。
非標準アカウントの傾向	孤立アカウント、システム アカウント、および例外アカウントに関する非標準アカウント の傾向を表示します。
非標準アカウント	すべての孤立アカウント、システム アカウント、および例外アカウントを表示します。
孤立アカウント	プロビジョニング サーバ内にグローバル ユーザがないエンドポイント アカウントをすべて表示します。
ポリシー	アイデンティティ ポリシーをすべて表示します。

レポート	Description
ユーザのプロファイル	ユーザに関する以下の情報が表示されます。 ■ Name ■ User ID ■ ユーザがメンバまたは管理者であるグループ ■ ユーザがメンバ、管理者、または所有者であるロール
エンドポイント アカウント	エンドポイントごとのアカウントを表示します (表示するエンドポイントは選択できます）。
ロール管理者	ロールとロールの管理者を表示します。
ロール所有者	ロールとロールの所有者を表示します。
スナップショット	エクスポートされたスナップショットをすべて表示します。
ユーザ アカウント	ユーザとそのアカウントのリストを表示します。
ユーザ権限	ユーザのロール、グループ、およびアカウントを表示します。
ユーザ ポリシー同期ステータス	ポリシーごとのユーザ ステータス（どのポリシーを割り当てるか、割り当て解除するか、または再割り当てするか）を表示します。

注: レポートの詳細については、「管理ガイド」を参照してください。

職務の分離要件の適用

職務分掌（SOD）要件が適用されると、利害の対立または不正の原因となる可能性のある権限は取得できなくなります。 CA Identity Manager では、SOD をサポートするため、以下の機能を提供します。

- **禁止アイデンティティ ポリシー**

  タスクがサブミットされる前に実行されるこれらのポリシーにより、管理者は権限の割り当てやプロファイル属性の変更を行う前にポリシー違反を確認することができます。 違反がある場合、管理者はタスクをサブミットする前に違反をクリアできます。

  たとえば企業は、ユーザ マネージャ ロールを持つユーザが同時にユーザ承認者ロールも持つことを禁止する禁止アイデンティティ ポリシーを作成できます。 管理者が［ユーザの変更］タスクを使用してユーザ マネージャにユーザ承認者ロールを与えた場合、CA Identity Manager から違反に関するメッセージが表示されます。 管理者はロールの割り当てを変更し、タスクをサブミットする前に違反をクリアできます。

- **スマート プロビジョニングによるポリシー検証**

  CA Identity Manager 管理者は、変更をコミットする前に、CA Identity Governance で プロビジョニング ロールおよびユーザ属性の変更案を BPR（Business Policy Rules）に照らして検証できます。 BPR は権限のさまざまな制約を表します。 たとえば、ある BPR では、メンバの下請け会社への備品の発注を許可する調達部門のロールをもつユーザが、下請け会社に支払いを行うロールをもつことを禁じています。 システム管理者、ビジネス マネージャ、監査担当者、またはロール エンジニアが CA Identity Governance で BPR を作成します。

  注: BPR の詳細については、「*CA Identity GovernanceSage DNA User Guide*」を参照してください。

注: 禁止アイデンティティ ポリシーとスマート プロビジョニングの詳細については、「CA Identity Manager 管理ガイド」を参照してください。

ユーザ ストア内のデータの変換

場合によっては、データがユーザ ストアに格納される前に、CA Identity Manager でデータを変換することをお勧めします。 たとえば、入力された形式とは異なる形式で情報を保存したり、一定のタイプの情報が存在する場合に変更を適用したりすることをお勧めします。

CA Identity Manager には、以下のデータの変換機能が含まれています。

- アイデンティティ ポリシー
- ロジカル アトリビュート ハンドラ

注: アイデンティティ ポリシーとロジカル アトリビュート ハンドラで、カスタム ビジネス ロジックを実装することもできます。

ロジカル アトリビュート ハンドラ

ロジカル アトリビュート ハンドラはカスタム Java コードです。このハンドラは、CA Identity Manager タスク画面で使用されるユーザ属性値を変換します。 ロジカル アトリビュート ハンドラを使用すると、タスク画面で物理属性を表示する形式をコントロールできます。また、ロジカル アトリビュート ハンドラを使用して、タスク画面で表示値（コストなど）を 1 つ以上の物理属性（単価、数量など）に変換し、ユーザ ストアに格納することもできます。

注: ロジカル アトリビュート ハンドラの詳細については、「Java のプログラミング ガイド」を参照してください。

カスタム ビジネス ロジックの適用

CA Identity Manager をカスタマイズして自社に必要なビジネス ロジックを実装することができます。CA Identity Manager には、以下のカスタム ビジネス ロジック実装オプションがあります。

- アイデンティティ ポリシー - アイデンティティ ポリシーを使用すると、ユーザがある条件またはルールを満たしたときに発生する一連のビジネス変更を定義できます。たとえば、アイデンティティ ポリシーで、一定のアイデンティティ管理タスクを自動化できます。これらのアイデンティティ管理タスクには、ロールの割り当てやビジネス ルールの適用などが含まれます（たとえば、20,000 ドルを超える小切手には署名や承認を禁止するなど）。

  注: アイデンティティ ポリシーの詳細については、「*管理ガイド*」を参照してください。

- ロジカル アトリビュート ハンドラ - これらのハンドラと CA Identity Manager タスク画面を関連付けることで、属性値の表示および変更をコントロールできます。

  詳細については、「*Programming Guide for Java*」を参照してください。

- ビジネス ロジック タスク ハンドラ - CA Identity Manager タスク用のデータ妥当性検証時に、以下のようにカスタム ビジネス ロジックを実行できます。
  - カスタム ビジネス ルールの適用 - たとえば、1 人の管理者には 5 つを超えるグループの管理を許可できません。
  - カスタマ固有のタスク画面フィールドの検証 - たとえば、［従業員 ID］フィールドの値は、マスタ人事データベースに存在する必要があります。

  ビジネス ロジック タスク ハンドラは、Java または JavaScript で実装できます。

  注: 詳細については、「Java のプログラミング ガイド」を参照してください。

- ワークフロー - カスタム プロセス定義を作成できます。それらの定義は CA Identity Manager イベントと関連付けられます。

注: ビジネス ロジック タスク ハンドラまたはワークフロー プロセスにビジネス ロジックを実装するかどうかを決定する前に、以下のセクションを参照してください。

- ビジネス ロジック タスク ハンドラ考慮事項 (P. 31)
- ワークフロー プロセス考慮事項 (P. 31)

ビジネス ロジック タスク ハンドラ考慮事項

ビジネス ロジック タスク ハンドラは、タスクの同期処理段階でビジネス ロジックの妥当性検査を実行します。この同期処理は、イベント生成に先立って発生します。 このハンドラでは、以下のことができます。

- タスク レベルでの検証の実行。たとえば、グループ メンバをそのオフィスの場所に基づいて追加または削除できます。オフィスの場所はユーザ プロファイル画面で指定されます。
- タスクのサブミットの禁止（検証が失敗した場合）。
- タスク画面のすべての情報の自動変換。これにより、それらの情報をビジネス ポリシーに準拠させてからタスクをサブミットできます。

注: ビジネス ロジック タスク ハンドラでは、完了に長時間かかるアクティビティを実装しないでください。 実行時間の長いアクティビティは、タスクのサブミットを遅らせ、ユーザとの対話が発生する同期段階には適しません。 代わりに、タスクの非同期段階で実行されるワークフロー プロセスを使用してください。

ワークフロー プロセス考慮事項

ワークフロー プロセスは、タスクの非同期段階で呼び出され、個々のイベントと関連付けられます。 ワークフロー プロセスでは、以下のことができます。

- 個々のイベント データに基づく承認アクティビティの実行
- 実行時間の長いカスタム ビジネス ロジック アクティビティの実行

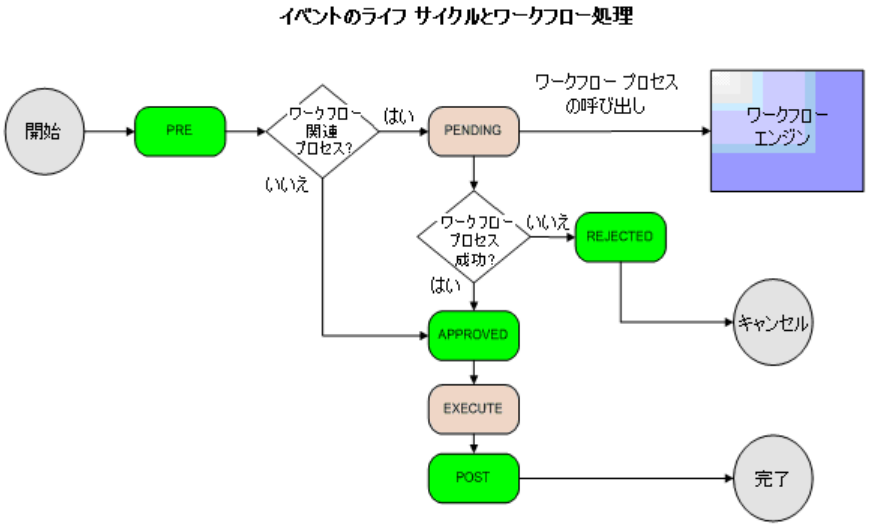
ワークフロー API では、ワークフロー アクティビティからタスク レベルのデータを取得できますが、通常は、ワークフローにおけるその特定イベントのコンテキストで操作を行います。

ビジネス変更の承認

ワークフローは 1 つ以上の手順で構成されるプロセスを記述します。これらは、一定のビジネス目的（採用手順の実行、外部システムからのユーザのクレジット スコアの取得など）を達成するため、実行する必要のある手順です。 通常、ワークフロー プロセスの手順の 1 つに、ビジネス変更の承認または拒否が含まれています。

CA Identity Manager では、ワークフロー プロセスはイベント（タスク処理時に発生するアクション）と関連付けられています。イベントがそのライフサイクルにおいて保留中状態に入ると、CA Identity Manager は関連するワークフロー プロセスを呼び出し、プロセスが完了するまでイベントの実行を一時停止します。プロセス完了後、CA Identity Manager は、ワークフロー プロセスの結果に基づいてイベントを実行または拒否します。

このシーケンスを以下の図に示します。



CA Identity Manager には、ワークフロー プロセスの作成および管理のための InSession WorkPoint ワークフロー エンジンがあります。

注: 詳細については、「管理ガイド」を参照してください。

第 3 章: CA Identity Manager アーキテクチャ

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 Identity Manager コンポーネント

CA Identity Manager の実装には、以下のコンポーネントの一部またはすべてが含まれます。

- サーバ
- ユーザ ストア
- データベース
- コネクタ

サーバ

CA Identity Manager の実装には、必要とする機能に応じて、1 種類以上のサーバが含まれています。

CA Identity Manager サーバ（必須）

CA Identity Manager 内のタスクを実行します。J2EE CA Identity Manager アプリケーションは管理コンソールとユーザ コンソールを含んでいます。

CA Identity Manager プロビジョニング サーバ

エンドポイント システムのアカウントを管理します。

CA Identity Manager インストールでアカウント プロビジョニングがサポートされる場合は、このサーバが必要です。

注: プロビジョニング サーバをインストールする前に、リモートで（またはデモ環境の場合のみローカルで）CA CA Directory サーバにプロビジョニング ディレクトリをインストールしておく必要があります。

SiteMinder ポリシー サーバ

CA Identity Manager に高度な認証を提供し、SiteMinder 機能（パスワード サービスやシングル サインオンなど）へのアクセスを提供します。

このサーバはオプションです。

ユーザ ストアとプロビジョニング ディレクトリ

CA Identity Manager は 2 つのユーザ ストアを調整します。

- *CA Identity Manager ユーザ ストア*（CA Identity Manager によってメンテナンスされるユーザ ストア）。通常、これは会社が管理する必要のあるユーザ ID を格納している既存ストアです。

  このユーザ ストアは、LDAP ディレクトリまたはリレーショナル データベースのいずれかです。

  管理コンソールで、CA Identity Manager ディレクトリ オブジェクトを作成することで、ユーザ ストアに接続し、CA Identity Manager によってメンテナンスされるユーザ ストア オブジェクトを記述します。

- *プロビジョニング ディレクトリ*（プロビジョニング サーバによってメンテナンスされるユーザ ストア）。

  プロビジョニング ディレクトリは、CA Directory のインスタンスであり、グローバル ユーザを含みます。グローバル ユーザは、プロビジョニング ディレクトリのユーザをエンドポイント（Microsoft Exchange、Active Directory、SAP など）のアカウントと関連付けます。

  一部の CA Identity Manager ユーザにのみ、グローバル ユーザが対応しています。 CA Identity Manager ユーザがプロビジョニング ロールを受け取ると、プロビジョニング サーバがグローバル ユーザを作成します。

別個のユーザ ストアとプロビジョニング ディレクトリ

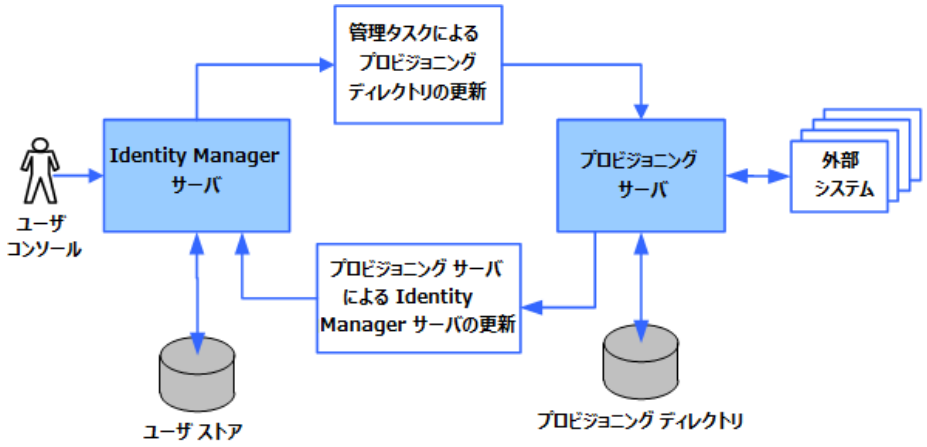
以下の図は、個別のユーザ ストアおよびプロビジョニング ディレクトリを示しています。これは、CA Identity Manager の新規インストールに対してサポートされているシナリオです。 この図の説明は、以下のとおりです。

- CA Identity Manager 管理者が管理タスクを使用してユーザ ストア内のユーザを編集すると、その変更はプロビジョニング ディレクトリに影響します

  この変更は、プロビジョニング サーバへのコネクタを持つエンドポイント（電子メール サーバなど）も更新する場合があります。

  プロビジョニング サーバ（またはプロビジョニング サーバへのコネクタを含むエンドポイント）で行われた変更は、CA Identity Manager ユーザ ストアおよびプロビジョニング ディレクトリを更新します。

たとえば、人事アプリケーションなどのエンドポイントでユーザの電子メール アドレスが更新される場合があります。



データベース

CA Identity Manager は、データ ソースを使用して CA Identity Manager 機能のサポートに必要な情報が格納されているデータベースに接続します。これらのデータベースは、データベースの単一物理インスタンスか、または別々のインスタンスに存在できます。

オブジェクト データベース（必須）

CA Identity Manager 設定情報が含まれています。

タスク永続性データベース（必須）

CA Identity Manager アクティビティおよびその関連イベントの情報を長期的にメンテナンスします。このため、CA Identity Manager サーバを再起動しても、CA Identity Manager アクティビティが正確に追跡されます。

アーカイブ データベース（必須）

タスク永続性データベースからデータをアーカイブします。

ワークフロー データベース

ワークフロー プロセス定義、ジョブ、スクリプト、およびワークフローエンジンで必要とされるその他のデータを格納します。

監査データベース

CA Identity Manager 環境で行われた操作の履歴を提供します。

注: CA Identity Manager によって監査データベースに格納する情報の量とタイプを設定できます。 詳細については、*「設定ガイド」*を参照してください。

レポート データベース

スナップショット データを保存します。スナップショット データは、スナップショット作成時における CA Identity Manager 内のオブジェクトの現状を反映します。 この情報からレポートを生成して、ユーザとロールなどオブジェクト間の関係を表示できます。

インストーラを使用すると、CA Identity Manager が CA Identity Manager データベースと呼ばれる単一のデータベースへの接続を設定します。このデータベースには、各データベース タイプのテーブルが含まれます。

注: タスク永続性、ワークフロー、監査、またはレポーティングのデータ ストアを別個のデータベース内に作成し、そのデータ ストアに接続するように CA Identity Manager を設定できます。 詳細については、「インストール ガイド」を参照してください。

コネクタ コンポーネント

コネクタは、エンドポイントに対するソフトウェア インタフェースです。プロビジョニング サーバは、コネクタを使用してエンドポイントと通信します。コネクタは、プロビジョニング サーバのアクションをエンドポイントでの変更に変換します（たとえば、Microsoft Exchange エンドポイントでの新規電子メール アカウントの作成など）。

エンドポイントの例としては、UNIX ワークステーション、Windows PC、または Microsoft Exchange （電子メール用）などのアプリケーションがあります。

コネクタ サーバ

コネクタ サーバは、コネクタを管理するプロビジョニング サーバのコンポーネントです。 コネクタ サーバは、プロビジョニング サーバ システムまたはリモート システムにインストールできます。

コネクタ サーバは、複数のエンドポイントを対象として動作します。 たとえば、多くの UNIX ワークステーション エンドポイントがある場合、1 つのコネクタ サーバで、UNIX アカウントを管理するすべてのコネクタを操作する場合があります。そして、もう 1 つのコネクタ サーバで、Windows アカウントを要求するすべてのコネクタを操作します。

分散コネクタ サーバでは、複数のコネクタ サーバが動作します。この方式では、あるコネクタ サーバがビジーになると負荷分散を行い、コネクタ サーバがダウンした場合に高い可用性を提供します。

コネクタ サーバには、次の 2 タイプがあります。

- CA IAM コネクタ サーバ（CA IAM CS）は、Java で書かれたコネクタを管理します
- C++ コネクタ サーバ（CCS）は、C++ で書かれたコネクタを管理します

C++ コネクタ サーバ

*C++ コネクタ サーバ*は C++ コネクタを管理するコネクタ サーバです。このコネクタ サーバは、プロビジョニング サーバまたはリモート システムにインストールできます。C++ コネクタ サーバは、オブジェクト指向のアプリケーション フレームワークを提供します。このフレームワークによって、C++ コネクタ サーバとエンドポイント間の通信を担当するコネクタの開発が簡略化します。

CA IAM CS

CA IAM CS は、Java コネクタのホスティング、ルーティング、および管理を処理するサーバ コンポーネントです。 CA IAM CS は、C++ コネクタ サーバの代替となる Java コネクタ サーバです。 CA IAM CS は、アーキテクチャと機能において C++ コネクタ サーバと同様です。ただし、C++ API の代わりに Java API 搭載しているので、CA IAM CS を使用すればコネクタを Java で実装できます。 さらに、CA IAM CS は、コード駆動型でなく、データ駆動型なので、コネクタ自体ではなくコンテナ（または CA IAM CS）によって、より多くの機能に対応できます。

プロビジョニング サーバは、ユーザのプロビジョニングを処理すると、次に、（C++ コネクタ サーバ または CA IAM CS を使用して）エンドポイント アカウントおよびグループの管理をコネクタに委任します。

コネクタとエージェント

CA Identity Manager コネクタは、より広範なプロビジョニング サーバ アーキテクチャの一部として実行され、環境内で管理されているシステムと通信します。 コネクタはネイティブ エンドポイント タイプのシステム技術へのゲートウェイとして機能します。 たとえば、ADS（Active Directory Services）を実行しているマシンは、プロビジョニング サーバが通信できるコネクタ サーバに ADS コネクタがインストールされている場合のみ管理できます。 コネクタは、システムに常駐するオブジェクトを管理します。 管理対象オブジェクトには、アカウント、グループ、およびオプションとしてエンドポイント タイプ固有のオブジェクトなどがあります。

コネクタはコネクタ サーバにインストールされ、一部のコンポーネントはプロビジョニング サーバ（たとえば、サーバ プラグイン）またはプロビジョニング マネージャ（ユーザ インターフェース プラグイン）にインストールされます。

一部のコネクタは、通信サイクルを完了するためには管理するシステム上にエージェントを必要とします。その場合、それらはプロビジョニング インストーラを使用してインストールできます。 エージェントは、以下のカテゴリに分類できます。

リモート エージェント

管理対象のエンドポイント システムにインストールされます。

環境エージェント

CA ACF2、CA Top Secret、RACF などのシステムにインストールされます。

一定のコンポーネントは、以下の C++ コネクタ サーバ ベースのオプションを含め、UNIX および Windows 上で動作します。

- UNIX （ETC, NIS）
- ACC（Access Control）

  注: UNIX ACC コネクタは UNIX ACC エンドポイントのみを管理できます。Windows ACC コネクタは Windows ACC エンドポイントの管理に必要ですが、UNIX ACC エンドポイントも管理できます。
- CA-ACF2
- RACF
- CA Top Secret

他の C++ コネクタ サーバ ベースのコネクタは、CSF（Connector Server Framework）に依存することにより、Solaris プロビジョニング サーバからアクセスできます。CSF を使用すると、Solaris 上のプロビジョニング サーバが Windows で実行されるコネクタと通信できます。

注: これらのコネクタを使用するには、CSF が Windows で 実行されている必要があります。

Connector Xpress

Connector Xpress は、動的コネクタの管理、エンドポイントへの動的コネクタのマッピング、およびエンドポイントのルーティング ルールの確立のための CA Identity Manager ユーティリティです。 Connector Xpress を使用すると、SQL データベースおよび LDAP ディレクトリのプロビジョニングと管理ができるように動的コネクタを設定できます。

Connector Xpress では、プロビジョニング マネージャによって管理されるコネクタを作成する際に一般的に必要な技術的専門知識がなくても、カスタム コネクタを作成し、展開することができます。

さらに、Connector Xpress を使用して、コネクタ サーバ設定（Java と C++ の両方）をセットアップし、編集し、削除することができます。

Connector Xpress への主要入力はエンドポイント システムのネイティブ スキーマです。 たとえば、Connector Xpress を使用すると、RDBMS に接続し、データベースの SQL スキーマを取得できます。 ID 管理とプロビジョニングに関連するネイティブ スキーマの一部からマッピングを構築する場合も Connector Xpress を使用できます。 マッピングには、プロビジョニング レイヤでネイティブ スキーマの要素が表現される方法が記述されます。

Connector Xpress は、動的コネクタに対して、ターゲット システムへのランタイム マッピングを記述するメタデータを生成します。

Connector Xpress の出力は、マッピングの完了時に生成されるメタデータ ドキュメントです。 メタデータは、CA IAM CS に対してコネクタの構造を記述する XML ファイルです。

メタデータは、プロビジョニング サーバのクラスと属性、およびそれらがネイティブ スキーマにどのようにマップされるかを記述します。

メタデータは 1 つ以上のプロビジョニング サーバで動的エンドポイント タイプの作成に使用されます。

注: Connector Xpress の使用の詳細については、*CA Identity Manager マニュアル選択メニュー*から「Connector Xpress ガイド」を参照してください。

追加コンポーネント

CA Identity Manager には、CA Identity Manager 機能をサポートする追加のコンポーネントが含まれています。 これらのコンポーネントの一部は CA Identity Manager と共にインストールされますが、別途インストールが必要なコンポーネントもあります。

WorkPoint ワークフロー

WorkPoint ワークフロー エンジンおよび WorkPoint Designer は、CA Identity Manager をインストールすると自動的にインストールされます。

これらのコンポーネントを使用すると、CA Identity Manager タスクをワークフローの制御下に置き、既存のワークフロー プロセス定義を変更したり、新しい定義を作成したりできます。

注: ワークフローの詳細については、「管理ガイド」を参照してください。

プロビジョニング マネージャ

CA Identity Manager プロビジョニング マネージャは、グラフィカル インターフェースを介してプロビジョニング サーバを管理します。このプロビジョニング マネージャは、プロビジョニング サーバ オプションの管理など、管理タスクに使用されます。 場合によっては、プロビジョニング マネージャで、CA Identity Manager ユーザ コンソールでは管理できない一定のエンドポイント属性を管理することがあります。

プロビジョニング マネージャは CA Identity Manager 管理ツールの一部としてインストールされます。

注: このアプリケーションは Windows システムでのみ実行されます。

プロビジョニング マネージャの詳細については、「*Provisioning Reference Guide*」を参照してください。

IAM レポート サーバ

CA Identity Manager は、CA Identity Manager 環境のステータスの監視に使用できるレポートを生成します。 CA Identity Manager で提供されるレポートを使用するには、CA Identity Manager に組み込まれている IAM レポート サーバをインストールします。

IAM レポート サーバは、Business Objects Enterprise XI で作動します。 既存の BO サーバがある場合は、IAM レポート サーバの代わりに、その BO サーバを使用して CA Identity Manager レポートを生成してください。

注: インストール手順については、「実装ガイド」を参照してください。

CA Identity Manager のサンプル インストール

CA Identity Manager では、ユーザの ID と、エンドポイント システムのアプリケーションおよびアカウントに対するユーザ アクセスを制御できます。必要とする機能に基づいて、インストールする CA Identity Manager コンポーネントを選択します。

すべての CA Identity Manager インストールで、CA Identity Manager サーバはアプリケーション サーバにインストールされます。 その他の必要なコンポーネントは CA Identity Manager インストーラを使用してインストールします。

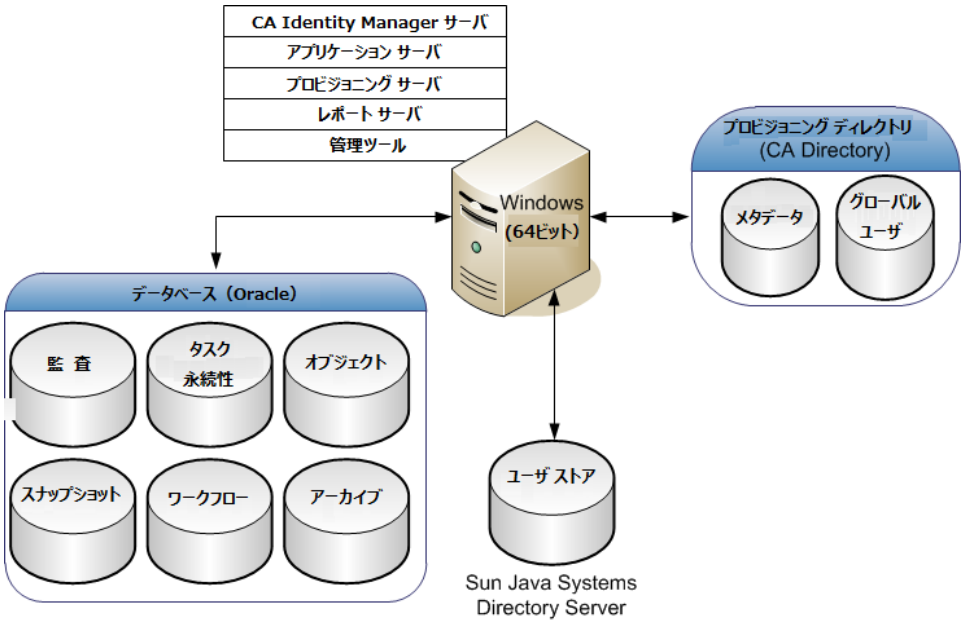
以降のセクションでは、高レベルでの CA Identity Manager の実装例を示します。

プロビジョニング コンポーネントを含むインストール

CA Identity Manager プロビジョニングでは、さまざまなエンドポイント システムにアカウントをプロビジョニングするプロビジョニング サーバに接続する環境を作成できます。 CA Identity Manager で作成するユーザにはプロビジョニング ロールを割り当てることができます。プロビジョニング ロールは、エンドポイント システム上で受信するアカウントを定義するアカウント テンプレートを持つロールです。アカウントは、電子メール アカウントなど、追加リソースへのアクセスをユーザに提供します。

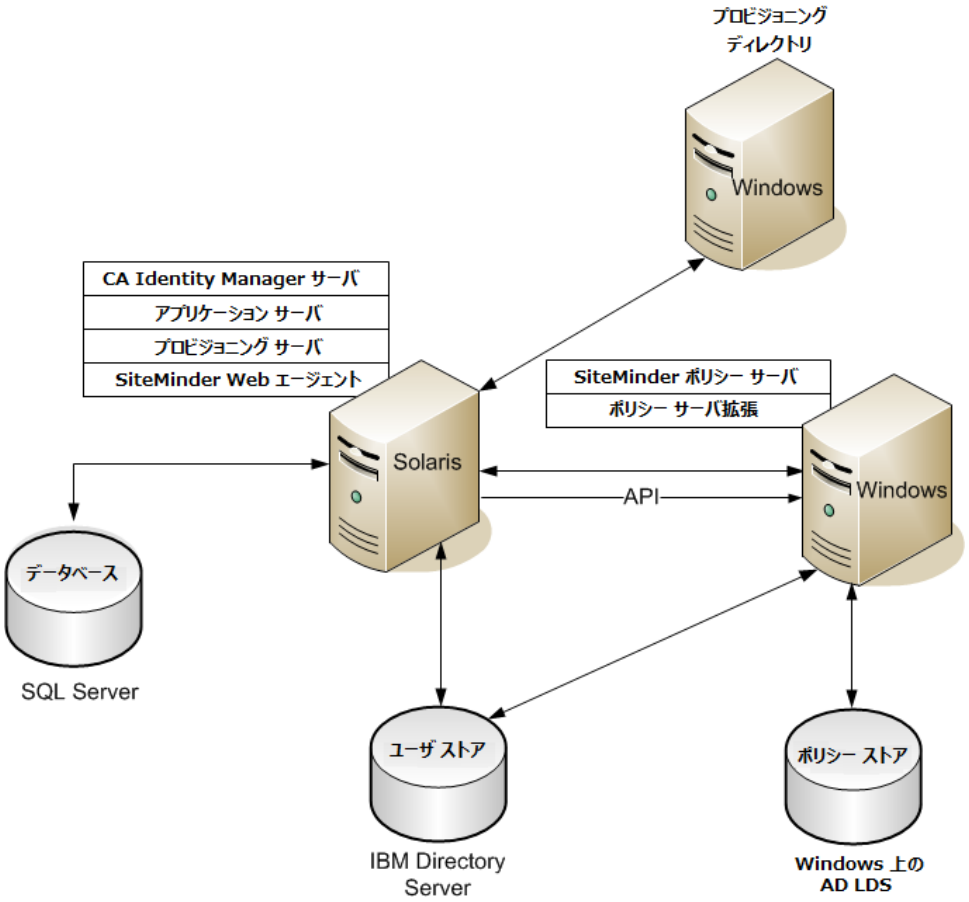
プロビジョニング ロールをユーザに割り当てると、そのユーザは、プロビジョニング ロールのアカウント テンプレートで定義されたアカウントを受け取ります。アカウント テンプレートでは、ユーザ属性とアカウントのマッピング方法も定義できます。アカウントは、アカウント テンプレートで定義された管理対象エンドポイントで作成されます。

以下の図は、プロビジョニングを含む CA Identity Manager インストールの一例です。



SiteMinder ポリシー サーバを含むインストール

SiteMinder ポリシー サーバは、CA Identity Manager 環境に高度な認証および保護を提供します。以下の図は、SiteMinder ポリシー サーバを含む CA Identity Manager インストールの一例です。



SiteMinder を含む CA Identity Manager 実装には、基本インストールまたはプロビジョニングを含むインストールのすべてのコンポーネントに加えて、以下の追加コンポーネントが含まれます。

SiteMinder Web エージェント

SiteMinder ポリシー サーバと連携して、ユーザ コンソールを保護します。 この Web エージェントは、CA Identity Manager サーバと共にシステムにインストールされます。

SiteMinder ポリシー サーバ

CA Identity Manager 用の高度な認証や許可に加えて、パスワード サービスやシングル サインオンなどの機能も提供します。

SiteMinder ポリシー サーバの拡張

SiteMinder ポリシー サーバによる CA Identity Manager のサポートを可能にします。CA Identity Manager 実装において、各 SiteMinder ポリシー サーバ システムに拡張機能をインストールします。

SiteMinder ポリシー ストア

SiteMinder が Web リソースへのアクセスの管理に必要とする情報を保存します。

CA Identity Manager が SiteMinder と統合すると、ポリシー ストアに CA Identity Manager ディレクトリおよび環境に関する情報も含まれるので、SiteMinder が高度な認証を提供できるようになります。

注: これらのコンポーネントは、例のように、さまざまなプラットフォームにインストールされます。ただし、他のプラットフォームを選択することもできます。CA Identity Manager データベースは Microsoft SQL Server にあります。ユーザ ストアは IBM ディレクトリ サーバにあります。 SiteMinder ポリシー ストアは Windows 上の AD LDS にあります。

第 4 章: 実装計画

CA Identity Manager の実装を計画するには、CA Identity Manager によるユーザ管理の方法とビジネス目的の達成に必要な機能を決定します。検討する質問は以下のとおりです。

- ユーザはどのように管理するか。
- アカウントのプロビジョニングは必要か。
- 何がカスタム ビジネス要件か。また、それら要件は実装すべきか。

これらに対して行う決定に基づいて、環境に最適な CA Identity Manager の実装方法を決定できます。

このセクションには、以下のトピックが含まれています。

管理対象の決定

管理したい対象を決定すると、インストールするコンポーネントの決定に役立ちます。 CA Identity Manager を使用すると、以下を管理できます。

- ユーザ ID
- エンドポイント システムのアカウントに対するアクセス

ユーザ ID

ユーザ ID は、従業員、契約業者、サプライヤなど、会社が管理する必要のある人々を表します。

ユーザ ID を管理するには、CA Identity Manager サーバと管理ツールしかインストールする必要がありません。

ユーザ管理サポートを設定する方法

CA Identity Manager では、管理ロールでユーザを管理します。管理ロールは管理者が実行できる CA Identity Manager タスクを決定します。

注: CA Identity Manager でユーザ管理を実装する前に、必要な機能を決定し、その機能を段階的に実装する計画を開発する (P. 63)必要があります。

ユーザ管理サポートを設定するには、以下の高レベル手順を完了します。

1. CA Identity Manager サーバと管理ツールをインストールします。

   管理対象ユーザにアカウントをプロビジョニングする必要がある場合は、プロビジョニング (P. 49)のサポートもインストールする必要があります。

   注: 手順については、「インストール ガイド」を参照してください。

2. CA Identity Manager 管理コンソールで以下を作成します。

   - **CA Identity Manager ディレクトリ**

     CA Identity Manager にユーザ ストアを記述します。 マニュアル選択メニューの内容は以下のとおりです。

     - ユーザ ストアへのポインタ。ユーザ ストアは、ユーザ、グループ、組織などの管理対象オブジェクトを格納します。
     - メタデータ。管理対象オブジェクトがどのようにディレクトリに格納され、どのように CA Identity Manager で表現されるかを記述します。

   - **CA Identity Manager 環境**

     管理ネームスペースを提供します。このネームスペースにより、CA Identity Manager 管理者はユーザ、グループ、組織などのオブジェクトを一連の関連するロールおよびタスクと共に管理できます。 CA Identity Manager 環境は、ディレクトリの管理およびグラフ表現を制御します。

   CA Identity Manager ディレクトリおよび環境の詳細については、「設定ガイド」を参照してください。

3. ビジネス要件に適合するように、デフォルト管理ロールおよびタスクを変更します。

   典型的なロール変更には、既存の管理ロールからのデフォルト タスクの追加や削除、デフォルト ロールに基づいた新規管理ロールの作成などがあります。

典型的なタスク変更には、管理したい情報のみを含むようにデフォルトのユーザ プロファイル タブをカスタマイズすることが含まれます (デフォルト プロファイル タブには、ユーザに対して定義されたすべての属性が含まれています)。

デフォルトの管理ロールおよびタスクの変更については、「*ユーザ コンソール デザイン ガイド*」を参照してください。

4. ユーザ管理タスクを実行するユーザに管理ロールを割り当てます。

他のアプリケーションからのアカウントのプロビジョニング

プロビジョニングを実装する決定は、管理する必要のある情報のタイプによって左右されます。 中央のユーザ ディレクトリを管理し、他のシステムのユーザ アカウントは管理したくない場合は、プロビジョニングを必要としません。 さまざまなシステムのユーザ アカウントを管理したい場合は、プロビジョニング サポートを実装する必要があります。

プロビジョニング機能はプロビジョニング サーバを介して提供され、プロビジョニング サーバは CA Identity Manager に統合されています。 プロビジョニング サーバは、以下のアカウント プロビジョニング機能を提供します。

- エンドポイント管理
- アカウントの同期
- アカウント テンプレート
- 検索および関連付け機能

注: プロビジョニング情報はプロビジョニング ディレクトリに格納されます。CA Identity Manager が別のタイプのディレクトリでユーザをメンテナンスする場合、展開には CA Identity Manager ユーザ ストアとプロビジョニング ディレクトリが含まれます。

エンドポイント管理

アカウントをプロビジョニングするには、CA Identity Manager ユーザ コンソールでエンドポイントを定義し管理します。*エンドポイント*はユーザがアクセスを必要とするシステムです。エンドポイントの例には、Oracle データベース、UNIX NIS サーバ、Windows サーバ、Microsoft Exchange サーバなどがあります。 アカウントを作成し、管理対象エンドポイントにおけるユーザ機能を決定するには、*アカウント テンプレート* (50P.)を使用します。

注: エンドポイントの定義および管理には、プロビジョニング マネージャも使用できます。ほとんどのエンドポイント管理タスクにユーザ コンソールを使用することを推奨しますが、一部のタスクではプロビジョニング マネージャを必要とします。これらのタスクには、エンドポイント属性の管理や、アカウント以外のエンドポイント オブジェクトの管理などがあります。 プロビジョニング マネージャの詳細については、「*Provisioning Reference*」を参照してください。

アカウントの同期

複数の管理対象エンドポイントにわたってユーザ アカウントを同期できます。アカウント同期が有効になっていると、プロビジョニング サーバでユーザ プロファイルに行われた変更が、そのユーザのアカウントのあるエンドポイントすべてに伝達されます。

注: CA Identity Manager タスクの［プロファイル］タブでアカウント同期の設定を指定してください。CA ARCserve Backup アカウント同期の設定の詳細については、「管理ガイド」を参照してください。

アカウント テンプレート

アカウント テンプレートは、管理対象エンドポイントでユーザを表す方法を定義します。 たとえば、Exchange アカウントのテンプレートでは、ユーザの電子メール アドレスの形式を定義できます（たとえば、<first initial><last name>@mycompany.com）。

アカウント テンプレートは、管理対象のシステム内でユーザが持つ権限も決定します。 たとえば、電子メール アドレスの形式の定義に加えて、Exchange アカウントのテンプレートは、メールボックス サイズも制限する場合があります。

アカウント テンプレートは、ユーザ コンソールで作成および管理します。

検索および関連付け機能

検索および関連付けの機能では、管理対象システムでの変更を検出および同期することで、エンドポイント管理を簡略化します。

検索機能では、エンドポイントでアカウントなどのオブジェクトを検索し、それらのオブジェクトへの参照をプロビジョニング ディレクトリに格納します。検索機能を使用すると、管理対象となる新規オブジェクトを検出できます。たとえば、LDAP ディレクトリでアカウントをプロビジョニングし、そのディレクトリに新しい組織を追加する場合は、検索機能を使用して、それらの新組織をアカウント テンプレートで使用できるようにします。

関連付け機能では、管理対象エンドポイントのアカウントをプロビジョニング ディレクトリ内のグローバル ユーザと関連付けます。エンドポイントでアカウントが変更されたら、関連付け機能でそれらの変更をグローバル ユーザ アカウントと同期できます。

注: 検索および関連付け機能の詳細については、「管理ガイド」を参照してください。

プロビジョニングのサポートを設定する方法

プロビジョニングの実装を決定したら、以下の高レベル手順を完了します。

1. CA Identity Manager サーバのインストーラを使用して、CA Identity Manager サーバ、プロビジョニング サーバ、プロビジョニング ディレクトリ初期化、および管理ツールをインストールします。

   注: CA Identity Manager コンポーネントのインストールの詳細については、「インストール ガイド」を参照してください。

2. CA Identity Manager サーバに接続するようにプロビジョニング マネージャを設定します。

3. CA Identity Manager 管理コンソールでプロビジョニングを設定します。

   a. プロビジョニングを有効にします。

   b. 以下を完了することで、プロビジョニングの環境を設定します。

      - カスタム ロール定義のインポート
      - インバウンド管理者の設定
      - プロビジョニング サーバへの環境の接続

   注: 詳細については、「設定ガイド」を参照してください。

4. ユーザ コンソールでエンドポイントを作成します。

   これにより、CA Identity Manager でエンドポイントを管理できるようになります。

   注: エンドポイント管理の詳細については、「管理ガイド」を参照してください。

5. エンドポイントを検索および関連付けます。

   エンドポイントを検索すると、CA Identity Manager がエンドポイント内でオブジェクトを検出し、それらのインスタンスをプロビジョニング ディレクトリに格納します。 このアクションにより、アカウントおよびエンドポイントで検出された他のオブジェクトがプロビジョニング ディレクトリに追加されます。

   エンドポイント上のアカウントを関連付けると、CA Identity Manager により、それらのアカウントがプロビジョニング ディレクトリ内のグローバル ユーザに関連付けされます。関連付け機能で存在しないグローバル ユーザを作成するかどうか、または関連付け機能で一致するグローバル ユーザのないアカウントを［デフォルト ユーザ］のグローバル ユーザに関連付けるかどうかを選択できます。

6. アカウント テンプレートの使用により、エンドポイント アカウントを作成し、メンテナンスします。これらのテンプレートには、アカウントの作成に使用される属性が含まれています。

7. アカウント テンプレートをプロビジョニング ロールと関連付けます。

   ユーザにプロビジョニング ロールを割り当てると、CA Identity Manager がそれらのユーザに関連するエンドポイントでアカウントを作成します。

   注: アカウント テンプレートとプロビジョニング ロールについては、「管理ガイド」を参照してください。

監査要件の決定

CA Identity Manager には、CA Identity Manager 環境でアクティビティを監視できる監査機能が含まれています。

この情報は監査データベースに格納されます。監査データベースに格納される情報の量とタイプは設定可能です。

［サブミット済みタスクの表示］と呼ばれるタスクにより、ユーザ コンソールで監査データを表示します。 このタスクを使用すると、管理者がシステムで発生するタスクを検索および表示できます。管理者は高レベルのタスク情報を表示したり、タスクおよびイベントの詳細を表示できます。

CA Identity Manager 監査の考慮事項

監査データから、CA Identity Manager 環境で行われた操作の履歴レコードが生成されます。 CA Identity Manager でデータを監査するには、以下が必要です。

- 監査データベース
- 監査設定ファイル

監査データベース

CA Identity Manager インストーラを使用すると、CA Identity Manager が CA Identity Manager データベースと呼ばれる単一のデータベースへの接続を設定し、監査用データベース テーブルに接続するためのデータ ソースを作成します。

注: CA Identity Manager データベースには、タスク永続性、ワークフロー、レポーティングなど、その他の CA Identity Manager 機能によって使用されるデータも含まれます。拡張性のため、監査用に別個のデータベース インスタンスを新たに作成できます。

注: 監査データベースの詳細については、「インストール ガイド」を参照してください。

監査設定

監査設定は監査設定ファイルで設定します。 監査設定ファイルは、CA Identity Manager が監査する情報の量とタイプを決定します。監査設定ファイルの設定によって、以下を行うことができます。

- CA Identity Manager 環境に関する監査を有効にします。
- 管理タスクによって生成された CA Identity Manager のイベントの一部またはすべての監査を有効にします。
- イベントの完了時またはキャンセル時など、特定の状態でのイベント情報を記録します。
- イベントに含まれる属性に関する情報をログ記録します。 たとえば、ModifyUserEvent イベント時に変更された属性をログ記録できます。
- 属性ログ記録の監査レベルを設定します。

注: 監査の設定の詳細については、「設定ガイド」を参照してください。

CA Audit 考慮事項

CA Audit は監査管理システムです。このシステムを使用すると、監査、レポーティング、コンプライアンスの検証、およびイベント モニタリングのセキュリティ関連データを収集し、格納することができます。

CA Audit を統合するには、CA Identity Manager サーバのインストール時に iRecorder コンポーネントをインストールします。 iRecorder は CA Identity Manager からイベントを取得します。 iRecorder は、CA Audit ポリシー マネージャのポリシーに基づき、イベントを無視するか、またはイベントを CA Audit にルーティングします。

ユーザ ストア要件の決定

CA Identity Manager 実装は、ユーザ ID を格納するユーザ ストアを含む必要があります。これらのユーザ ID は CA Identity Manager によってメンテナンスされます。通常、このユーザ ストアは、企業がユーザ（従業員や顧客など）に関する情報の格納に使用する既存のユーザ ストアです。

実装にプロビジョニングが含まれる場合、CA Identity Manager ではグローバル ユーザを含むプロビジョニング ディレクトリも必要とします。これらのグローバル ユーザは、エンドポイント（Microsoft Exchange、Active Directory、Oracle など）のアカウントに関連付けられます。

複数ユーザストアの管理

企業は複数のユーザ ストアをメンテナンスする場合があります。 各ユーザ ストアでは、ユーザ ID を使用して、さまざまな企業リソースにアクセスできます。 複数のユーザ ストアを管理するには、以下の方法のいずれかを使用できます。

- CA Identity Manager でプロビジョニング ディレクトリを直接管理し、プロビジョニング サーバでさまざまなユーザ ストア内のユーザおよびアカウントを間接的に管理します。

  このアプローチでは、以下が可能です。

  - 1 つの場所から、各種の企業リソースに割り当てることのできるユーザを一元管理します
  - 企業のリソース間で共通のセキュリティおよびビジネス ルールを実装します。 これには、以下を含めることがあります。
    - ロール ベースのアクセス制御
    - 委任管理

- 管理する企業アイデンティティのタイプに基づいてカスタマイズされるタスクおよび画面
- ルール ベースのアイデンティティ管理のためのアイデンティティ ポリシー
- カスタマイズと拡張性

注: これらの機能については、「管理ガイド」を参照してください。

- 各ユーザ ストアを管理する別個の CA Identity Manager 環境を作成します。

  この方法では、情報が環境間で共有されません。

インストールするコンポーネントの選択

以下の表では、実装したい機能をサポートするためにインストールするコンポーネントをリストしています。

注: これらのコンポーネントをインストールする手順については、「インストール ガイド」を参照してください。

行いたい処理	インストールするコンポーネント
既存の企業ユーザ ストアのユーザ ID を管理します。	■ CA Identity Manager サーバ
エンドポイント システムでアカウントをプロビジョニングします。	■ プロビジョニング サーバ ■ プロビジョニング ディレクトリ ■ プロビジョニング マネージャ ■ コネクタ ■ コネクタ サーバ **注**: コネクタをインストールする手順については、インストールしたいコネクタ タイプの「コネクタ ガイド」を参照してください。

行いたい処理	インストールするコンポーネント
以下の機能の 1 つ以上を実装します。 ■ 高度な認証 ■ 高度なパスワード ポリシー ■ 異なるユーザ セットに対する異なるコンソール スキン ■ ユーザに関するロケール基本設定の設定	■ SiteMinder ポリシー サーバ ■ ポリシー ストア ■ SiteMinder Web エージェント ■ ポリシー サーバへの CA Identity Manager の拡張 **注**: SiteMinder ポリシー サーバおよびポリシー ストアをインストールする手順については、「*CA SiteMinder Web Access Manager Policy Server Installation Guide* 」を参照してください。Web エージェントをインストールする手順については、「*CA SiteMinder Web Access Manager Web Agent Installation Guide* 」を参照してください
CA Identity Manager アクティビティに関するレポートの生成	IAM レポート サーバ

ハードウェア要件の決定

CA Identity Manager インストールに必要なハードウェアは、実装する機能および展開のサイズによって異なります。

以降のセクションでは、典型的な CA Identity Manager の実装とそれらに必要なハードウェアについて説明します。

展開のタイプ

CA Identity Manager の展開に必要なハードウェアを計画する際には、実装したい機能と展開の初期サイズを考慮します。 以下のカテゴリのいずれかを使用して、展開のサイズを見積もってください。

注: 選択する展開タイプによって、プロビジョニング ディレクトリで使用される DxGrid ファイルのサイズが決まります。 展開タイプは、CA Identity Manager サーバのインストール時に指定します。

デモンストレーション

デモンストレーションまたは開発環境での基本的テストで使用される単一サーバ展開。 デモンストレーション展開では、プロビジョニングされたアカウントを最大 10,000 までサポートします。

注: この実装タイプでは、運用環境での実装はサポートされません。

基本

ほとんどの中小規模実装に適した可用性の高い実装。 基本実装では、プロビジョニングされたアカウントを最大 400,000 までサポートします。

このタイプの実装では、CA Identity Manager アプリケーションおよびそのコンポーネントを実行するための 2 つのサーバと、CA Identity Manager データベースおよびユーザ ストアを実行するための 2 つのサーバを必要とします。

中規模

中規模の実装に適した可用性の高い実装。 中規模展開では、プロビジョニングされたアカウントを最大 600,000 までサポートします。

大規模

ユーザの追加とトランザクション数の増加に対応するため、追加サーバ クラスタを含める可用性の高い実装。 大規模展開では、600,000 を超えるプロビジョニングされたアカウントをサポートします。

注: 可用性の高い実装の詳細については、「インストール ガイド」を参照してください。

プロビジョニングの追加要件

CA Identity Manager にプロビジョニングを組み込む場合は、CA Identity Manager の基本実装に必要なコンポーネントに加えて、以下の追加のコンポーネントが必要です。

- プロビジョニング サーバ

  CA Identity Manager サーバと同じマシンにインストールできます。

- プロビジョニング ディレクトリ初期化

  重要: The Provisioning Directory Initialization must be installed on CA Directory.

- プロビジョニング マネージャ

  プロビジョニング サーバにアクセスできる任意の Windows マシンにインストールできます。

注: 開発環境では、これらのコンポーネントは、基本インストール コンポーネントもインストールされている 1 台のマシンにインストールできます。

SiteMinder 統合の追加要件

CA Identity Manager を SiteMinder と統合する場合、実装には CA Identity Manager の基本インストールのコンポーネントに加えて、以下の追加のコンポーネントを含める必要があります。

- **ポリシー サーバ**

  ポリシー管理、認証、許可、および監査の各サービスを提供します。

  ポリシー サーバが CA Identity Manager 専用の場合は、CA Identity Manager サーバと同じマシンにポリシー サーバをインストールできます。ポリシー サーバが他のアプリケーションを保護する場合は、パフォーマンスを最高にするため、ポリシー サーバを別個のマシンにインストールすることを推奨します。

- **ポリシー ストア**

  すべてのポリシー サーバ データを格納します。 ポリシー ストアの設定は、サポートされている LDAP またはリレーショナル データベース内で行うことができます。 可用性の高い実装では、ポリシー ストアを別個のサーバにインストールすることを推奨します。

- **ポリシー サーバの拡張**

  SiteMinder ポリシー サーバによる CA Identity Manager のサポートを可能にします。 CA Identity Manager 実装内の各 SiteMinder ポリシー サーバ システムにこれらの拡張をインストールしてください。

- **SiteMinder Web エージェント**

  SiteMinder ポリシー サーバと共に動作して、ユーザ コンソールを保護します。CA Identity Manager サーバのあるシステムにインストールされます。

ユーザをインポートする方法の選択

既存のユーザ ストアへユーザをインポートする必要がある場合は、ビジネス要件に基づいて方法を選択してください。

以降のセクションでは、ユーザ インポートのオプションについて説明します。

新規ユーザ ストアにユーザをインポートする方法

ユーザ データを格納する方法を決定したら、あるストアから別のストアにユーザをインポートする必要がある場合があります。 実装に応じて、さまざまなユーザのインポート方法を使用できます。

注: 新規ユーザ ストアにユーザをインポートした後で、アイデンティティ ポリシー (P. 61)を使用して、インポートしたユーザに変更を適用できます。

CA Identity Manager によるユーザのインポート

CA Identity Manager では、下記の方法で、CA Identity Manager が直接管理するユーザ ストアにユーザを追加します。

方法	機能	制限事項
Bulk Loader	ユーザ コンソールの［Bulk Loader］タスクを使用してフィーダ ファイルをアップロードできます。フィーダ ファイルを使用すると、多くの管理対象オブジェクトを同時に操作できます。 Bulk Loader 方式の利点は、多数の管理対象オブジェクトの操作プロセスを 1 つの情報（フィーダ）ファイルを使用して自動化できることです。［Bulk Loader］タスクをワークフロー プロセスにマッピングすることもできます。	Bulk Loader を使用している場合、インポート中のユーザの数によっては、メモリ不足の例外メッセージが表示されることがあります。 この問題に対処するには、JVM メモリの設定を増大してください。
TEWS（Task Execution Web Service）によるリモート タスク呼び出し	［ユーザの作成］タスクを含め、Web サービスに有効な任意の CA Identity Manager タスクを実行できます。 タスクが［ユーザの同期］に設定されている場合、CA Identity Manager は適用可能なあらゆるアイデンティティ ポリシーを実行します。	Web サービス モデルのパフォーマンス特性がバルク インポート操作の高スループット要件にうまく適合しない場合があります
IM API	■ Java クライアントによるユーザの作成用に直接呼び出せるユーザ ベースの API を提供します ■ 最高のスループット機能を提供します。	■ タスク サーバが提供する監査とセキュリティのメカニズムをバイパスします。 ■ アイデンティティ ポリシーの実行をサポートしません。

注: Bulk Loader の詳細については、「管理ガイド」を参照してください。TEWS および IM API の詳細については、「Java のプログラミング ガイド」を参照してください。

インポートされたユーザに対するアイデンティティ ポリシーの実行

*アイデンティティ ポリシー*とは、ユーザが特定の条件やルールを満たした場合に発生する一連のビジネス変更です。 これらの変更には、ロール（プロビジョニング ディレクトリのユーザのプロビジョニング ロールを含む）の割り当てまたは取り消し、グループ メンバシップの割り当てまたは取り消し、ユーザ プロファイル内の属性の更新などがあります。

アイデンティティ ポリシーを使用すると、新規ユーザ ストアへのユーザ アカウントのインポート後に、それらのユーザ アカウントに変更を適用できます。

このセクションでは、1 ステップまたは 2 ステップでインポートされたユーザのアイデンティティ ポリシーを実行する方法について説明します。

1 ステップ アプローチ

以下のインポート方法を使用すると、1 つのステップで、新規ユーザ ストアにインポートするユーザに対してアイデンティティ ポリシーを実行できます。

- ユーザ コンソールの［Bulk Loader］
- TEWS による［ユーザの作成］タスクの実行
- インバウンド同期

2 ステップ アプローチ

2 ステップ アプローチでは、まず、ユーザをインポートし、次に、それらのユーザに対してアイデンティティ ポリシーを実行します。この方法を使用できるのは、［プロビジョニング サーバ］で CA Identity Manager ユーザを管理する場合です。この方法は、インポート要件によっては、より多くの柔軟性を提供する場合があります。

1. インポート ツールの 1 つを使用して、プロビジョニング ディレクトリにユーザを追加します。
2. インポートしたユーザの各々に対して、TEWS を介して CA Identity Manager の［ユーザの同期］タスクを呼び出します。

プロビジョニング サーバによるユーザのインポート

プロビジョニング サーバには、プロビジョニング ディレクトリでのユーザの追加および管理用のバルク インポート オプションが含まれています。以下の表では、プロビジョニング ディレクトリにユーザをインポートする方法を説明します。

方法	機能	制限事項
バッチ ユーティリティ（etautil）	プロビジョニング ディレクトリでオブジェクトを管理することを可能にするコマンド ライン インターフェース ユーティリティ。	■ 現在は Windows システムにしか対応していません。
検索および関連付け	■ プロビジョニング サーバが既知のエンドポイントで管理できる新規オブジェクトを検出します（ユーザも含む）。 ■ エンドポイントおよびプロビジョニング サーバに存在するオブジェクト インスタンスに関連付け機能を提供します。 追加情報については、「検索および関連付け機能」を参照してください。	■ 現在サポートされているコネクタの場合、デフォルトで、検索および関連付けの機能を利用できます。この機能はカスタム コネクタで拡張できます。 ■ 関連付けオプションは、多数のユーザで動作すると、拡張性に影響する場合があります。このインポート オプションを選択する場合は、必ずパフォーマンスと拡張性に対する影響を評価してください。

グローバル ユーザと CA Identity Manager ユーザ ストアの同期

プロビジョニング サーバにユーザをインポートしたら、以下の方法でそれらのユーザを CA Identity Manager ユーザ ストアに追加できます。

- **インバウンド同期**

  インバウンド同期によって、プロビジョニング ディレクトリで発生した変更の最新情報が CA Identity Manager ユーザに通知されます。 プロビジョニング ディレクトリでの変更には、プロビジョニング マネージャやプロビジョニング サーバへのコネクタを持つシステムを使用して行われた変更などがあります。

  インバウンド同期を使用してユーザをインポートする際には、以下の点に注意します。

  - CA Identity Manager 管理コンソールで、インバウンド リクエストからの属性を CA Identity Manager タスク内の属性にマップする方法をカスタマイズできます。

    注: 詳細については、「管理ガイド」を参照してください。

  - どのプロビジョニング サーバの変更が企業ユーザ ストアとの同期を必要とするか考慮してください。 多数の変更を同期すると、パフォーマンスと拡張性に影響を与える場合があります。

- **プロビジョニング ロールとアカウント テンプレート**

  プロビジョニング サーバは、プロビジョニング ロールおよびアカウント テンプレートを使用して、CA Identity Manager ユーザ ストア内のアカウントを管理できます。 このためには、CA Identity Manager ユーザ ストアをポイントする管理対象エンドポイントが取得されており、適切なアカウント テンプレートおよびロールが存在する必要があります。 この場合、「プロビジョニング サーバによるユーザのインポート」で説明されているオプションの 1 つによって作成されたグローバル ユーザに、CA Identity Manager ユーザ ストア内のユーザ アカウントを作成するプロビジョニング ロールを割り当てることができます。

展開計画の開発

大規模な実装を計画する際には、CA Identity Manager の機能を段階的に展開する必要があります。 以下の展開順序を使用すると、CA Identity Manager から大きな価値をすばやく取得し、時間経過と共に変化する実装のニーズを評価し、最高のパフォーマンスと拡張性を提供する環境を注意深く構築することができます。

- セルフ サービスとパスワード管理
- アイデンティティ ポリシー

- ワークフロー承認
- ユーザ、グループ、および組織の各オブジェクトの委任管理
- ロール管理の委任管理

各展開段階の後で、必ずパフォーマンスを評価し、調整を行ってから、次の段階に進みます。 「CA Identity Manager の最適化 (P. 73)」には、パフォーマンス、調整、および拡張性に関する情報が示されています。

セルフ サービスおよびパスワード管理の展開

以下の理由により、他の CA Identity Manager 機能を展開する前にセルフ サービスのタスクおよびパスワード管理を展開します。

- セルフ サービス タスクおよびパスワード管理は展開しやすく、大きな価値を迅速にもたらします。
- これらは、委任された管理モデルから独立した機能であり、変化するビジネス ニーズに応じて再設定できます。
- これらの機能は、通常、CA Identity Manager によって定期的に処理される最高ボリュームのタスクを生成します。 このため、これらの機能を使用すると、追加機能の展開前に実装の拡張性をテストすることができます。

セルフ サービス タスクを展開するには、以下の手順を完了します。

1. 自己登録タスクを設定します。

   これはパブリック タスクであり、インストール時に、デフォルトで有効になります。 このタスクを設定するには、デフォルトの自己登録タスクのフィールドを必要に応じて追加または削除します。

2. 自己管理マネージャ ロールを展開します。

   このロールのメンバ ルールは、すべてのユーザに適用されるように設定するか、またはロールを新規ユーザに自動的に割り当てるメンバ ルールを含む必要があります。 たとえば、すべての常勤スタッフに自己管理マネージャ ロールを割り当てるメンバ ルールを作成できます。 ユーザが自己登録すると、CA Identity Manager は、（ロジカル アトリビュート ハンドラまたはビジネス タスク ハンドラの使用により）従業員タイプを常勤に設定できます。 ユーザはメンバ ルールの基準を満たすと、自己管理マネージャのロールを自動的に受け取ります。

   注: 自己管理マネージャ ロールのメンバ ルールを設定する際には、管理者によるロール メンバの追加や削除を許さないでください。 ロールは自動的に割り当てられるので、管理者が明示的にロールを割り当てる必要はありません。

パスワード管理機能を展開するには、以下の手順を完了します。

1. ［忘れたパスワード］タスクなど、パスワード管理のパブリック タスクを設定します。
2. パスワードの作成方法と有効期限を決定するパスワード ポリシーを作成します。
3. パスワード マネージャ ロールを展開します。これにより、ロール メンバによるユーザ パスワードのリセットが可能になります。

注: ロール、タスク、およびパスワード管理については、「管理ガイド」を参照してください。

アイデンティティ ポリシーの展開

アイデンティティ ポリシーは、ユーザが特定の条件やルールを満たすと発生する一連のビジネス変更です。 完全な委任モデルを展開する前に、アイデンティティ ポリシーを使用してビジネス駆動の権限付与を提供できます。 たとえば、セールス マネージャ プロビジョニング ロールを割り当てるアイデンティティ ポリシーを作成できます。このポリシーは、セールス アプリケーションへのアクセス権をセールス マネージャという役職を持つすべてのユーザに与えます。 販売員は、セールス マネージャに昇進すると、管理者の関与を待たずに、職務の遂行に必要なすべてのシステムへのアクセス権を自動的に受け取ります。

アイデンティティ ポリシーを展開するには、以下の手順を完了します。

1. ユーザ プロファイル属性への変更によってトリガされるアイデンティティ ポリシーを設定します。
2. 少数の管理者が、ユーザ タスク（［ユーザの作成］や［ユーザの変更］など）を使用して、アイデンティティ ポリシーをトリガする属性を変更できるようにユーザ マネージャ ロールを設定します。

   ユーザ マネージャのメンバ ポリシーにスコープ ルールを必ず設定して、ロール メンバが管理できるユーザ セットを決定します

アイデンティティ ポリシーを展開する際には、以下の点に注意してください。

- ワークフロー承認を必要とし*ない*権限を付与するアイデンティティ ポリシーを最初に作成することを検討します。 これにより、ワークフロー プロセス、承認形式、および承認者モデルを定義しなくても、アイデンティティ ポリシーの展開が可能になります。
- アイデンティティ ポリシーを作成する前に、どの方法が最適な解決策となるかを判別するため、データ妥当性検証ルール、論理属性、ビジネス ロジック タスク ハンドラ、ワークフロー プロセスなど、CA Identity Manager でビジネス ルールを実装する他の方法に精通しておく必要があります。

  注: これらの方法の詳細については、「管理ガイド」と「Java のプログラミング ガイド」を参照してください。
- アイデンティティ ポリシーは CA Identity Manager で権限を割り当てる効率的な方法です。ただし、それらは著しくパフォーマンスに影響する (P. 89)場合があります。
- ユーザ タスクの初期展開では、［ロール］タブなど、関係タブの削除または非表示を検討してください。これらのタブは、アイデンティティ ポリシーが管理する権限と同じ権限を管理します。 これは、許可されていない権限を付与するリスクを防ぎ、不適切に構築されたロールがパフォーマンスに影響する可能性をなくします。

注: アイデンティティ ポリシーの詳細については、「管理ガイド」を参照してください。

ワークフロー承認の展開

ワークフロー承認を使用すると、CA Identity Manager 実装にセキュリティと自動化の追加レベルを追加できます。

ワークフロー承認の展開には、以下のタスクが必要です。

1. 承認を必要とするイベントまたはタスクを決定します。
2. ワークフロー プロセスごとに、参加者と呼ばれる承認者のセットを定義します。

   注: すべての参加者は、参加者リゾルバによって動的に決定されます。 良好なパフォーマンスを維持するため、参加者数を 30 名までに制限します。
3. 承認形式を設定します。
4. 必要な場合は、カスタム ワークフロー プロセスを定義します。

環境およびタスク レベルのワークフロー承認

CA Identity Manager は、2 タイプの承認（環境レベルの承認とタスク レベルの承認）をサポートします。 環境レベルの承認は、イベントのすべてのインスタンスに対して、それらに関連付けられたタスクと関わりなく、定義されます。 タスク レベルの承認は、特定タスクに関連付けられた特定イベントに対して定義されます。 タスク レベルの承認は環境レベルの承認より優先されます。

ほとんどの承認は環境レベルで定義されます。これは、あるイベントに対して、そのイベントに関連付けられたタスクに関わらず、同じワークフロー アクティビティが発生するようにするためです。ただし、以下の状況では、タスク レベルのワークフローを実装することを考慮してください。

- 特化したタスクで、承認を必要としないイベントを生成する特定のビジネス変更を実行する場合。
- アイデンティティ ポリシーによってトリガされる変更アクションで、ワークフロー承認を必要としないイベントを生成する場合。
- 特定のワークフロー プロセスをタスクに固有な変更と関連付ける柔軟性が必要な場合。

トランザクション ボリュームの増大に伴い、環境レベルの承認で大量の処理およびシステム リソースが必要となる場合があります。 このため、最終的にパフォーマンスと拡張性の問題が発生する可能性があります。 これらの問題は、タスク レベルの承認を適宜使用することで、軽減ないし除去される場合があります。

ユーザ、グループ、および組織の委任管理の展開

委任管理では、さまざまな CA Identity Manager ユーザにロールの変更、割り当て、および使用の機能を実行させることで、ユーザとユーザの権限を管理します。

注: CA Identity Manager 実装のパフォーマンスおよび拡張性を良好にするには、委任モデルを注意深く構築する必要があります。

委任はスコープ ルールによって適用されます。スコープ ルールは管理ロールのメンバおよび管理ポリシーで定義されます。 スコープ ルールは、ロール メンバがロールを使用できるオブジェクトを決定します。 たとえば、スコープ ルールで、ユーザ マネージャが、他の部門ではなく、自分の部門のユーザを管理できるようにします。

通常、スコープ ルールは、ユーザ ストアの論理構造を反映します。 たとえば、階層 LDAP ユーザ ストアでは、スコープが組織で定義される場合があります。 リレーショナル データベースでは、スコープを部門 ID などの属性を使用して定義できます。

ユーザ、グループ、および組織の委任管理を展開する際には、以下の点に注意してください。

- ユーザ関連タスクで、［管理ロール］タブおよび［プロビジョニング ロール］タブなど、関係タブへのアクセスを制限します。これらの関係タブは、［ユーザの作成］や［ユーザの変更］などのデフォルト ユーザ タスクに含まれています。それらのタブをデフォルト タスクから削除し、少数の管理ロールに関連する特化したタスクでのみ使用することを考慮してください。
- CA Identity Manager は各スコープ ルールを動的に評価し、スコープ情報はキャッシュされません。 良好なパフォーマンスを確保するため、単純なディレクトリ クエリを含むスコープ ルールを作成することを考慮してください。
- 管理者が管理できるオブジェクトが CA Identity Manager から返る時間を確定することで、スコープ ルールのパフォーマンスを評価します。

ロールの委任管理の展開

ロールの委任管理は、CA Identity Manager で最も大きな権限を付与し、パフォーマンスに最大の影響 (P. 74)を与えることができます。 これらの理由により、ロールの委任管理は、他のすべての機能を展開した後で展開するように考慮してください。

ロールの委任管理を展開する際には、以下の点に注意します。

- 環境を保護し、良好なパフォーマンスを保証するため、管理ロール、管理ロール メンバ、および管理ロール管理者の数を制限します。
- ロールの委任管理を展開したら、パフォーマンスと拡張性のテストを行います。 必要に応じて環境を最適化します。

第 5 章: 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。

SiteMinder および CA Identity Manager

CA Identity Manager が CASiteMinder と統合される場合、CA SiteMinder は CA Identity Manager 環境に以下の機能を追加できます。

高度な認証

CA Identity Manager には、デフォルトで CA Identity Manager 環境用のネイティブ認証が含まれます。 CA Identity Manager 管理者は、CA Identity Manager 環境にログインするために、有効なユーザ名およびパスワードを入力します。 CA Identity Manager は、CA Identity Manager が管理するユーザ ストアに対する名前およびパスワードを認証します。

CA Identity Manager が CASiteMinder と統合される場合、CA Identity Manager は、環境を保護するために CA SiteMinder 基本認証を使用します。 ユーザが CA Identity Manager 環境を作成する場合、ポリシー ドメインおよび認証方式がその環境を保護するために CA SiteMinder で作成されます。

CA Identity Manager が CASiteMinder と統合される場合は、管理コンソールを保護するために SiteMinder 認証も使用できます。

アクセス ロールおよびタスク

アクセス ロールにより、CA Identity Manager 管理者が CA SiteMinder が保護するアプリケーションで権限を割り当てることができます。 これらのアクセス ロールは、財務アプリケーションでの発注書の生成など、ビジネス アプリケーションでユーザが実行できる単一のアクションを表します。

ディレクトリマッピング

管理者は、管理者の認証に対して使用されるものとは別のユーザ ストアにそのプロファイルが存在するユーザを管理する必要がある場合があります。CA Identity Manager 環境にログインするときに、管理者は、あるディレクトリと使用して認証され、管理者にユーザを管理する権限を与えるために別のディレクトリを使用して認証されます。

CA Identity Manager が CA SiteMinder と統合される場合、認証と認可用に別のディレクトリを使用するように CA Identity Manager 環境を設定できます。

異なるユーザ セットのスキン

スキンにより、ユーザ コンソールの外観が変更されます。 CA Identity Manager が CASiteMinder と統合される場合、異なるユーザ セットが異なるスキンを参照できるようになります。 この変更を実行するには、スキンをユーザのセットと関連付けるために SiteMinder レスポンスを使用します。 レスポンスは、ユーザのセットに関連付けられる、ポリシーのルールと組み合わされます。 ルールが実行される場合、ユーザ コンソールを構築するために、スキンに関する情報を CA Identity Manager に渡すようにレスポンスをトリガします。

注: 詳細については、「*ユーザ コンソール デザイン ガイド*」を参照してください。

ローカライズされた環境のロケール基本設定

CA Identity Manager が CASiteMinder と統合される場合、imlanguage HTTP ヘッダを使用して、ユーザにロケール基本設定を定義できます。SiteMinder ポリシー サーバで、SiteMinder レスポンス内でこのヘッダを設定し、ヘッダの値としてユーザ属性を指定します。 この imlanguage ヘッダはユーザに対する優先度が最も高いロケール基本設定として機能します。

注: 詳細については、「*ユーザ コンソール デザイン ガイド*」を参照してください。

詳細情報:

SiteMinder ポリシー サーバを含むインストール (P. 44)

SiteMinder 認証

CA Identity Manager には以下のコンソールが含まれています。これらのコンソールは保護する必要があります。

ユーザ コンソール

CA Identity Manager 管理者が CA Identity Manager 環境でタスクを実行することを可能にします。

管理コンソール

CA Identity Manager 管理者が CA Identity Manager ディレクトリ、プロビジョニング ディレクトリ、および CA Identity Manager 環境を作成および設定することを可能にします。

CA Identity Manager にはネイティブ認証が含まれています。デフォルトでは、ネイティブ認証がユーザ コンソールを保護します。管理コンソールはデフォルトでは保護されません。ただし、管理コンソールを保護するように CA Identity Manager を設定できます。 管理コンソールの保護には、CA SiteMinder も使用できます。

ユーザ コンソールに、証明書またはキー認証など、他のタイプの認証を設定するには、CA Identity Manager を SiteMinder と統合する必要があります。

注: 詳細については、「設定ガイド」を参照してください。

第 6 章: CA Identity Manager の最適化

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 Identity Manager のパフォーマンス

CA Identity Manager のパフォーマンスは、さまざまな機能およびコンポーネントの個々のパフォーマンスによって左右されます。

CA Identity Manager 環境では、以下の機能を最適化できます。

- ロール
- タスク
- グループ メンバシップおよび管理
- アイデンティティ ポリシー

さらにパフォーマンスを向上するには、以下のコンポーネントも調整できます。

- ユーザ ストア
- プロビジョニング コンポーネント
- ランタイム コンポーネント（タスク永続性データベースなどのデータベースや、アプリケーション サーバ設定を含む）

最適なパフォーマンスを保証するには、以降のセクションのガイドラインを使用して、CA Identity Manager 機能を設定します。 次に、パフォーマンスを測定し、必要に応じてコンポーネントを調整します。コンポーネントは一緒に動作するので、環境に最適な調整の設定を見つけるまで、数回繰り返すことが必要な場合があります。

ロールの最適化

CA Identity Manager には 3 タイプのロールが含まれています。

- 管理ロール

  ユーザが ユーザ コンソール内で持つ権限を決定します。

  ユーザが CA Identity Manager 環境にログインすると、そのユーザのアカウントには 1 つ以上の管理ロールがあります。 各管理ロールには、ユーザがその CA Identity Manager 環境で完了できる［ユーザの作成］などのタスクが含まれています。 ユーザの管理ロールがユーザ コンソールの表示を決定します。したがって、ユーザは、そのロールに関連付けられたタスクのみを見ることになります。

- プロビジョニング ロール

  電子メール システムなど、管理対象エンドポイントのアカウントをユーザに付与します。

- アクセス ロール

  CA Identity Manager における権限を付与する追加手段を提供します。

ロールには、以下を決定するポリシーが含まれます。

- ロールを使用できるユーザ（管理ロールとアクセス ロールの場合のみ）と、ロールを使用できる場所。
- ロール メンバおよび管理者を管理できるユーザ。
- ロール定義を変更できるユーザ。

ロールおよびロールに関連する権限の評価は、CA Identity Manager のパフォーマンスに大きな影響を与える場合があります。

ロール評価によるログイン時のパフォーマンスへの影響

CA Identity Manager ユーザがユーザ コンソールへのログインを試みると、以下のアクションが発生します。

1. CA Identity Manager は、ユーザ名とパスワードなどクレデンシャルの入力をユーザに促します。
2. ユーザのクレデンシャルは、以下のいずれかの方法で認証されます。
   - CA Identity Manager ネイティブ認証
   - SiteMinder 認証（CA Identity Manager 実装に SiteMinder が含まれている場合）

3. CA Identity Manager は、環境内のすべての管理ロールのすべてのメンバ ポリシーを評価して、どの管理ロールをユーザに適用するか決定します。

   注: この評価は、所定のユーザに対して 1 回のみ行われます。最初の評価後、CA Identity Manager は結果をキャッシュします。 CA Identity Manager は、ユーザまたはメンバ ポリシーのセットが変更されるまでキャッシュされた情報を使用します。変更が行われると、CA Identity Manager はキャッシュ内の情報を更新します。

4. CA Identity Manager ユーザ コンソールには、ユーザがそのロールに基づいて見ることのできるカテゴリが表示されます。

このプロセスは、ユーザ コンソールにログインするユーザごとに発生します。CA Identity Manager 環境に多数のロール (非効率なメンバ ポリシー) が含まれている場合は、ロール メンバシップの評価がパフォーマンスに著しく影響する可能性があります。その場合は、ユーザ コンソールへのログイン時の初期画面の表示が遅くなる場合があります。

注: ユーザがパブリック タスクにアクセスして自己登録したり、忘れたパスワードを要求する際には、CA Identity Manager がメンバ ポリシーを評価する必要はありません。 これらの場合、CA Identity Manager は、完全なユーザ コンソールを表示しないので、ユーザのロール リストを必要としません。

ロール オブジェクトとパフォーマンス

各ロールをサポートするため、CA Identity Manager は、ロール設定に応じて、CA Identity Manager オブジェクト ストア (P. 35)に多数のオブジェクトを作成します。

CA Identity Manager は、ロールごとに 1 つのベース オブジェクトを作成します。ベース オブジェクトに加えて、CA Identity Manager は、ポリシーごとに 1 つのオブジェクトを作成します。

多数のロール オブジェクトは、オブジェクト ストア検索とポリシー評価のパフォーマンスに影響する場合があります。

オブジェクト ストアのパフォーマンス

CA Identity Manager は、ユーザおよび権限の管理に必要な情報をオブジェクト ストアに格納します。 オブジェクト ストア内に多くのロール オブジェクトがあると、以下の問題が発生する場合があります。

- CA Identity Manager タスク画面での管理対象オブジェクトの検索が長くかかる場合があります。

  検索に対する影響を減らすには、検索で使用される属性にインデックスを付けます (P. 94)。

- ロール管理タスクの実行が遅くなる場合があります。

  大きなオブジェクト ストアによって影響を受けるロール管理タスクの例を以下に示します。

  - CA Identity Manager がオブジェクト ストア内でロール名が一意であることを確認する必要があるため、［管理ロールの作成］タスクの動作が遅くなります。
  - ［管理ロールの削除］タスクは、ロールをサポートするために作成されたオブジェクトをすべて削除する必要があります。そして、オブジェクト キャッシュは更新される必要があります。

- CA Identity Manager によるロール ポリシーの評価に時間がかかります。

CA Identity Manager は、オブジェクト ストアの情報をキャッシュすることで、パフォーマンスを改善します。

ロール ポリシー評価の最適化

管理ロールごとに、以下の 3 タイプのポリシーを作成できます。

- メンバ ポリシー

  ロールを受信するユーザを決定するメンバ ルールと、ロール メンバが管理できるオブジェクトを決定するスコープ ルールを定義します。

- 管理ポリシー

  管理ルール、スコープ ルールおよびロール用管理者権限を定義します。

- 所有者ポリシー

  ロールを変更できるユーザを定義します。

CA Identity Manager がロール ポリシーを評価するする際のパフォーマンスを最適化したい場合は、以下を考慮してください。

- CA Identity Manager 環境内の管理ロールの数を制限します。
- ポリシー ルール作成のガイドライン (P. 77)に従います。
- ユーザ ストアを調整します。
- CA Identity Manager に SiteMinder が含まれている場合は、ポリシー ストアを調整します。

ポリシー ルール作成のガイドライン

ロール ポリシー評価の全体的パフォーマンスを決定する主な要因の 1 つは、任意の単一ポリシー ルールの評価にかかる時間です。 ポリシー ルール評価時間を改善するには、ポリシー作成時に、以下の点に注意します。

- 可能な場合は、複雑な表現でポリシー ルールを作成することにより、CA Identity Manager によって作成されるポリシー オブジェクトの数と実行されるユーザ ストア検索の数を制限します。

  複雑な表現を含む単一のルールは、単純な表現を含む複数のルールより効率的です。

- 可能な場合は、最も効率的で最も拡張性のあるタイプのポリシー ルールを選択します。
- ポリシー ルールのインメモリ評価オプションを有効にします。

  インメモリ評価オプションは、ユーザ ストアから評価対象のユーザに関する情報を取得し、メモリにそのユーザの表現を格納することにより、ポリシー評価時間を著しく減らします。 CA Identity Manager は、インメモリ表現を使用して、属性値をポリシー ルールと照合します。

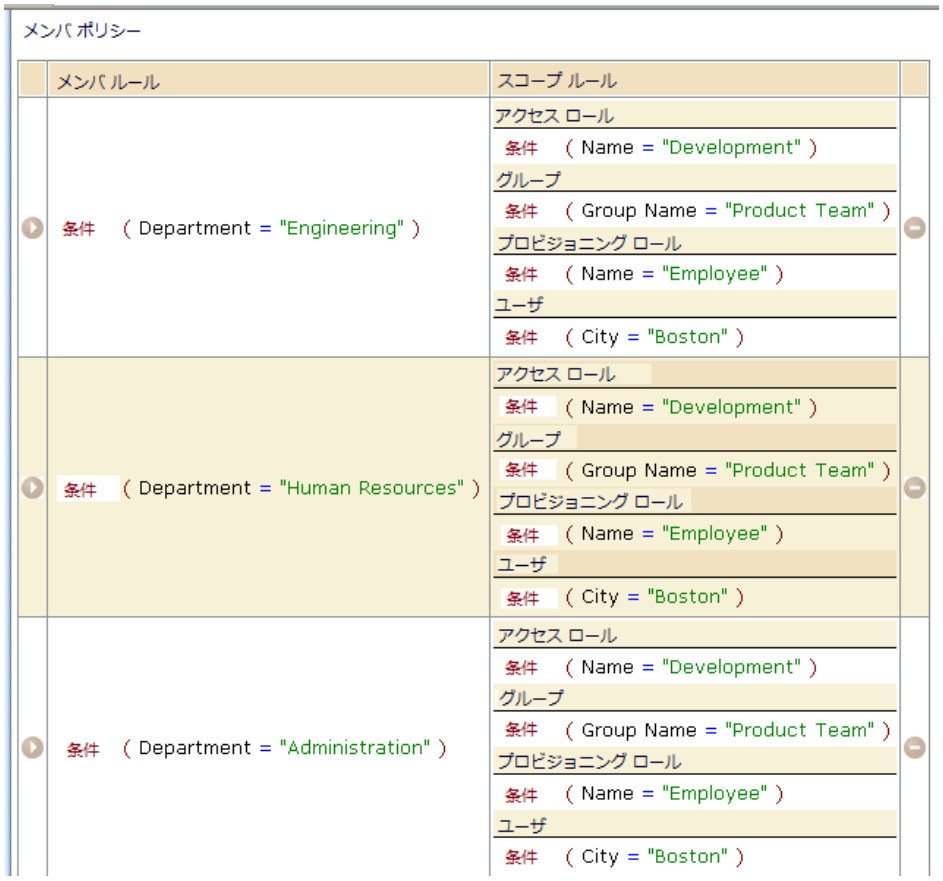
  注: : インメモリ評価オプションの詳細については、「設定ガイド」を参照してください。

- ユーザ ストアを調整します。
- CA Identity Manager 実装に SiteMinder が含まれている場合は、ポリシー ストアを調整します。

ポリシー オブジェクトとユーザ ストア検索の制限

ロール ポリシーのルールごとに、オブジェクト ストア内の 1 セットのオブジェクトを必要とします。CA Identity Manager はルールを評価すると、これらのオブジェクトをロードし、必要なユーザ ストア検索を実行します。

以下の例は、3 つのメンバ ルールを含むメンバ ポリシーを示しています。各ルールには 4 つのスコープ ルールが含まれています。

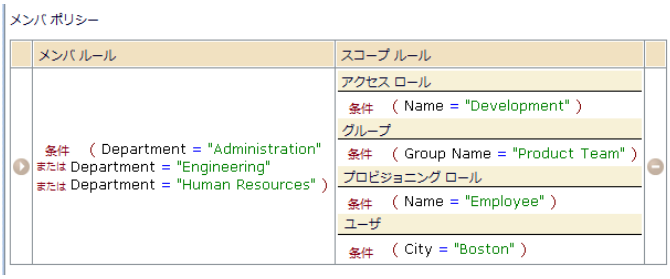


この例では、CA Identity Manager は、メンバ ポリシーの評価および適用時にオブジェクトを作成し、以下の表に記述されているユーザ ストア検索を実行します。

ルール	ポリシー オブジェクト	可能性のあるユーザ ストア検索
■ メンバ ルール： where (Department = "Administration") ■ ユーザ スコープ： City = "Boston" ■ グループ スコープ： Group Name = "Product Team" ■ プロビジョニング ロール スコープ： Name = "Employee" ■ アクセス タスク スコープ： Name = "Development"	5	5 （ルール定義オブジェクトごとに 1 回）
■ メンバ ルール： where (Department = "Engineering") ■ ユーザ スコープ： City = "Boston" ■ グループ スコープ： Group Name = "Product Team" ■ プロビジョニング ロール スコープ： Name = "Employee" ■ アクセス タスク スコープ： Name = "Development"	5	5
■ メンバ ルール： where (Department = "Human Resources") ■ ユーザ スコープ： City = "Boston" ■ グループ スコープ： Group Name = "Product Team" ■ プロビジョニング ロール スコープ： Name = "Employee" ■ アクセス タスク スコープ： Name = "Development"	5	5

この例では、CA Identity Manager は 15 個のオブジェクトを作成し、15 回のディレクトリ検索を実行して、メンバシップとスコープを決定します。

ポリシー オブジェクトの数と CA Identity Manager が実行するユーザ ストア検索の回数を制限するには、ルールを組み合わせて複雑な表現を作成します。以下の例では、最初の例と同じ権限を 1 つのメンバ ルールとして指定します。



この例では、CA Identity Manager は 10 個のポリシー オブジェクトしか作成せず、ユーザ ストア検索は 5 回しか実行しません。

ルール	ポリシー オブジェクト	可能性のあるユーザ ストア検索
■ メンバ ルール： where (Department = "Administration") OR where (Department = "Engineering") OR where (Department = "Human Resources") ■ ユーザ スコープ： City = "Boston" ■ グループ スコープ： Group Name = "Product Team" ■ プロビジョニング ロール スコープ： Name = "Employee" ■ アクセス タスク スコープ： Name = "Development"	5	5

拡張性のあるポリシー ルール タイプの選択

ポリシー ルールの数に加えて、ポリシー ルールのタイプもパフォーマンスに影響する場合があります。 通常、ポリシー ルールは、ユーザ ストアの構造と権限の決定方法に基づいて構築されます。 たとえば、グループ メンバシップ、組織、またはユーザ属性に基づいてポリシー ルールを作成できます。 ただし、ポリシー ルールを構築する方法が複数存在する場合は、以下の表に記載されたパフォーマンス ガイドラインを検討してから、構築すべきルールのタイプを決めてください。

注: 以下の表のポリシー ルール タイプは、パフォーマンスの順（最も効率的なルール タイプから開始）にリストされています。

ポリシー ルール タイプ	パフォーマンスに関するメモ
組織	■ 最良の全体的パフォーマンス ■ LDAP ディレクトリは検索不要です。 CA Identity Manager は、評価対象ユーザの DN とポリシー ルール内の組織の DN を使用します。
ロール	■ CA Identity Manager はオブジェクト ストアのキャッシュにロール オブジェクトの情報と以前の評価を格納します。 ■ ほとんどの場合、組織ポリシー ルールと同じくらい良いパフォーマンスになります。
ユーザ属性	■ 最良のユーザ ストア検索パフォーマンスを提供し、多数のユーザ群に最も影響されません。 ■ インメモリ評価を有効にして、パフォーマンスを大幅に向上できます。
グループ メンバシップ	■ パフォーマンスは、グループのサイズとユーザ ストアのタイプによって左右されます。

タスクの最適化

CA Identity Manager では、ユーザ コンソールで表示されるタスクは、そのユーザの特定の権限によって異なります。タスクを表示および実行するには、CA Identity Manager は複数のセキュリティ評価を実行する必要があります。そして、それらの評価が CA Identity Manager 環境内のすべてのユーザに適用されると、パフォーマンスに重大な影響を及ぼす場合があります。

CA Identity Manager は、以下のアクションが発生すると、セキュリティ評価を実行します。

- ユーザがユーザ コンソールにログインする

  この場合、CA Identity Manager は、ユーザのロールを評価して、そのユーザがユーザ コンソールでアクセスできるタスクを決定する必要があります。

- ユーザがタスクを呼び出す

  タスクが呼び出されると、CA Identity Manager は、ユーザがそのタスクで管理できるオブジェクトを決定する必要があります。

- ユーザが関係タブにアクセスする

  関係タブとは、ユーザがタスクの対象と権限セットの間の一対多数の関係を表示または管理できるタブです。 関係タブの一例として［管理ロール］タブがあり、このタブでは、ユーザのロールが表示されます。

- ユーザが関係タブにオブジェクトを追加する

  たとえば、あるユーザが［管理ロール］タブで別のユーザにロールを追加すると、CA Identity Manager は追加のセキュリティ チェックを実行します。

タスク パフォーマンスは、以下の要因に影響されます。

- タスク スコープ。管理者がタスクを使用できるスコープを決定します。
- 関係タブ。オブジェクトと他のオブジェクトとの関係を表示します。

タスク スコープ評価とパフォーマンス

管理者が、ユーザ、グループ、組織、タスク、ロールなど、管理対象オブジェクトの検索を含む管理タスクを使用すると、CA Identity Manager はタスク スコープ ルールを評価し、適用します。これらのルールは、タスク用に選択されるオブジェクトのリストを表示するために CA Identity Manager がかける時間の量に著しく影響する場合があります。

注: メンバ ポリシー、管理ポリシー、および所有者ポリシーの評価と異なり、スコープ ルール評価に関する情報はキャッシュに保存されません。

タスク スコープは、以下の要因で決定されます。

- タスクが管理するオブジェクトのタイプ。
- タスクを含む管理ロールに適用されるスコープ ルール。 スコープ ルールは、メンバ ポリシー、所有者ポリシー、および管理ポリシーで定義されます。
- ユーザ定義の検索条件。

たとえば、［ユーザの変更］タスク（ユーザ マネージャ ロールに含まれている）について考えてみてください。 ユーザ マネージャ ロールにはスコープ ルールを持つメンバ ポリシーがあり、このスコープ ルールによって、ユーザ マネージャによる従業員組織内のユーザの管理が可能になります。管理者は［ユーザの変更］タスクを開き、次の検索条件を入力します：「Last Name starts with A」 この場合、［ユーザの変更］タスクのスコープは、姓が A で始まる従業員組織内のすべてのユーザになります。

CA Identity Manager による関係タブの表示方法

関係タブでは、タスクの対象と権限セットの関係を表示し管理できます。たとえば、［プロビジョニング ロール］タブでは、ユーザのプロビジョニング ロールが表示されます。

関係タブに表示するオブジェクトを決定するため、CA Identity Manager が多数のセキュリティ評価を実行し、それがパフォーマンスに著しく影響することがあります。

以下の例では、［プロビジョニング ロール］タブを表示するために CA Identity Manager が取る手順を示します。

1. 管理者が［ユーザの変更］タスク内の［プロビジョニング ロール］タブをクリックします。
2. CA Identity Manager が選択されたユーザをメンバとするプロビジョニング ロールを取得します。
3. ロール管理者を管理できるようにタブが設定されている場合は、CA Identity Manager が 2 つ目の呼び出しを行って、選択されたユーザを管理者とするプロビジョニング ロールのリストを取得します。
4. CA Identity Manager が、そのユーザの持つ各プロビジョニング ロールを評価して、タスクを開始した管理者がそのロールのメンバシップを管理できるかどうか確認します。

   管理者がロール メンバを管理できる場合は、CA Identity Manager がタブ上のロール リスト内のそのロールの［メンバシップ］列に、アクティブなチェック ボックスを表示します。
5. CA Identity Manager が、ユーザの各プロビジョニング ロールを評価して、タスクを開始した管理者がそのロールの管理者権限を管理できるかどうか確認します。

   管理者が管理者権限を管理できる場合は、CA Identity Manager がタブ上のロール リスト内のそのロールの［管理者］列に、アクティブなチェック ボックスを表示します。

   ユーザの現在のプロビジョニング ロールを表示するには、CA Identity Manager が手順 2 から 5 を完了する必要があります。 管理者が新しいプロビジョニング ロールを割り当てる必要がある場合は、以下の追加手順が必要となります。
6. 管理者が［追加］ボタンをクリックして、割り当てる新しいプロビジョニング ロールを見つけます。
7. CA Identity Manager は管理者が追加するロールの検索に使用できる検索画面を表示します。
8. 管理者が追加するロールを見つけるための検索フィルタを入力します。

9. CA Identity Manager が以下の条件を満たすプロビジョニング ロールのリストを返します。
   - ロールが管理者によって入力された検索フィルタに一致する。
   - 管理者がロールのメンバシップを管理できる。
   - ユーザがロールの管理者の管理スコープ内にいる。
   - ユーザにまだそれらのプロビジョニング ロールがない。
10. CA Identity Manager が手順 9 を繰り返して、管理者が管理者権限を管理できるロールを決定します。

関係タブとパフォーマンス

CA Identity Manager が実行するセキュリティ評価の数のために、関係タブの表示がパフォーマンスに著しく影響する場合があります。パフォーマンスを決定する要因はタブのタイプに応じて変わります。

ロール関係のタブについては、以下の要因がパフォーマンスに影響する可能性があります。

- タスクの対象がメンバであるロールの数
- タスクの対象が管理者であるロールの数
- 対象のロールを計算するために CA Identity Manager が必要とするシステム内のオブジェクトの合計数
- ロール当たりのメンバ/管理ポリシーの数
- メンバ/管理ポリシー スコープ ルールの複雑さ
- セキュリティ エンフォースメントの影響を制限するために、タスク呼び出し用にキャッシュされた許可をメンテナンスする機能

グループ関係タブのグループ メンバシップおよび管理者権限を決定するには、CA Identity Manager がユーザ ストア内のグループをすべて検索する必要があります。これらの検索のパフォーマンスは、以下の要因に左右されます。

- ユーザ ストア内のグループ オブジェクトの数
- 任意のグループ内のメンバの数
- ユーザ ストアが存在するデータベースまたはディレクトリのパフォーマンス

タスク処理とパフォーマンス

管理タスクにはイベント（CA Identity Manager がタスクを完了するために実行するアクション）が含まれます。 1 つのタスクには、複数のイベントが含まれている場合があります。 たとえば、［ユーザの作成］タスクには一般に、ユーザ プロファイルを作成するイベント、ユーザをグループに追加するイベント、ロールを割り当てるイベントが含まれます。

CA Identity Manager はタスクを処理する際に、タスクと関連付けられた各イベントを処理します。 CA Identity Manager はイベント処理時に各イベントを 4 回保存します。 これにより、予期しないシステム シャットダウンが発生した場合も、CA Identity Manager が処理中のアクションを失わないようにできます。

CA Identity Manager が複数のイベントを同時に処理する場合、それらのイベントはキューに追加されます。 最初のイベントは、そのライフサイクルの最初の段階を完了すると保存され、次に、キューの末尾に移動されて、第 2 段階の処理の開始を待機します。 次に、CA Identity Manager がキューの次のイベントの最初の処理段階を完了し、そのイベントはキューの末尾に移動します。 このプロセスは、キュー内のすべてのイベントが最初の処理段階を完了するまで続行します。次に、キュー内の最初のイベントの 第 2 処理段階が開始されます。キュー内のすべてのイベントが 4 つの処理段階のすべてを完了するまで、これが続行します。

通常の負荷条件下では、この動作がパフォーマンスに影響を与えることはありません。ただし、多数のユーザ群のバルク ロード時など、多数のイベントとタスクをシステムが処理する場合は、各イベントとタスクがキュー内で長時間待機する必要があるので、完了時間が長くなります。

負荷条件下で発生するパフォーマンス上の問題を防止するには、以下のアクションを考慮します。

- タスクの［プロファイル］タブの［タスク優先度］設定を使用する

  ［タスク優先度］設定では、タスクの優先度を「高」、「中」、または「低」に設定できます。

  すぐに処理する必要のあるタスクは、「高」に設定します。 バルク ロードに含まれるタスクは、「低」に設定します。

  タスク優先度が設定されている場合、そのタスクに関連付けられたイベントは、同じ優先度を持つタスクと共に処理されます。 たとえば、［ユーザの変更］タスクの優先度が「高」に設定されていて、管理者がユーザ プロファイルを変更した場合、CA Identity Manager は「中」または「低」の優先度を持つタスクより前に［ユーザの変更］タスクを処理します。 他にも優先度が「高」のタスクがある場合は、CA Identity Manager は最初の「高」優先度イベントの最初の処理段階を完了したら、そのイベントを他の「高」優先度イベントのリストの末尾に移動します。

- 別個の専用の CA Identity Manager サーバをインストールして、バルク ロード操作を処理させる

タスク最適化のガイドライン

デフォルト タスク（CA Identity Manager 環境の作成時に CA Identity Manager によって展開されるタスク）は、広範な管理使用事例をサポートするように設定されています。大半の CA Identity Manager 実装では、デフォルト タスクによって提供される機能の一部しか必要でありません。 CA Identity Manager 環境を作成したら、特定の管理ニーズに合わせて、これらのタスクを変更してください。

以下の手順は、タスクを変更するためのガイドラインです。

- **特化したユーザ管理タスクを作成する。**

  ［ユーザの作成］、［ユーザの変更］、および［ユーザの表示］は、完全な管理機能を提供するデフォルト タスクです。しかし大半の実装では、少数の管理者だけが利用可能な機能をすべて必要とします。

  必要な機能のみを含む新しいタスクを作成してください。 たとえば、大半のユーザ管理タスクがプロファイル管理とグループ管理にしか関与しない場合は、［プロファイル］タブと［グループ］タブのみを含む新しい［ユーザの変更］タスクを作成します。 デフォルトの［ユーザの変更］タスクで利用可能な［管理ロール］タブ、［アクセス ロール］タブ、および［プロビジョニング ロール］タブは削除します。

  使用されないタブを頻繁に使用されるタスク内に残すと、大量のオーバーヘッドを発生させる場合があります。これは、特に TEWS（Task Execution Web Service）クライアントの使用時に当てはまります。その場合は、CA Identity Manager と共に提供される tab java クラスによって、これらのタブが誤ってアクティベートされることがあります。

  作成する特化したタスクは、使用する環境用に定義した委任管理モデル (P. 68)と一致する必要があります。

- **関係タブ内の［管理者の管理］を無効化する**

  デフォルトでは、すべての関係タブに、ロールやグループなどタブが管理するオブジェクトに対する管理者権限を管理する機能があります。 しかし、大半の実装では、この機能を管理者に提供する必要はありません。

この機能が必要でない場合、CA Identity Manager による管理者権限の評価時に発生する追加オーバーヘッドを除去するため、以下のタブで［管理者の管理］オプションをクリアします。

- 管理ロール
- プロビジョニング ロール
- アクセス ロール
- グループ

特定のタブ上の管理者権限を管理できるようにするには、デフォルト タブのコピーを作成して、［管理者の管理］オプションを有効に、［メンバの管理］オプションを無効にします。 それらの新しいタブを特化したタスク（それらのタスクを必要とする管理者だけが使用するタスク）に追加します。

- **ロール関係タブ内の範囲指定検索を有効にする**

  各ロールタブの設定に、ユーザに割り当てる新規ロールの基準を管理者が指定すること可能にする検索機能を含めることができます。 ロール検索は、管理者がユーザに割り当てられるロールを決定するため、CA Identity Manager が評価する必要のあるメンバ/管理者ポリシー ルールの数を制限します。

- **タスク同期オプションを設定する**

  各 CA Identity Manager タスクには、ユーザ同期オプション（ユーザをアイデンティティ ポリシーと同期する）と、プロビジョニング アカウント同期オプション（ユーザをプロビジョニングされたアカウントと同期する）を指定できます。 これらのオプションでは、タスク完了時またはイベント完了時にユーザを同期できます。

  評価と処理の時間をなくすには、イベント完了時でなく、タスク完了時に同期が行われるように設定します。

グループ メンバ/管理者のための最適化ガイドライン

グループ メンバと管理者の検索のパフォーマンスを改善するには、以下の点を考慮します。

- ディレクトリ設定ファイル（directory.xml）で既知の属性を定義します。これらの属性は、CA Identity Manager にユーザ ストアの構造と内容を説明します。

  既知の属性は、CA Identity Manager で特定の意味を持つ属性です。

  グループ メンバ/管理者の検索を改善するには、ユーザ オブジェクトに以下の既知の属性を定義します。

  %MEMBER_OF%

  ユーザがメンバとなっているグループのリストを格納するユーザ オブジェクトの属性を識別します。

この属性が定義されていると、CA Identity Manager はユーザ ストア内のすべてのグループのすべてメンバを検索することを回避できます。 グループ検索は、非常に大きなグループがある場合のパフォーマンスに著しく影響することができます。

%ADMINISTRATOR_OF%

ユーザが管理者となっているグループのリストを格納するユーザ オブジェクトの属性を識別します。

%MEMBER_OF% 属性のように、この既知の属性によってグループ検索にかかる時間が短縮されます。

- ディレクトリ設定ファイルでグループ タイプを指定します。

  CA Identity Manager は、標準グループ、ネストされたグループ、および動的グループの、3 種類のグループをサポートしています。

  ディレクトリ設定ファイルでグループ オブジェクトを定義する際には、ユーザ ストアがサポートするグループのタイプを指定できます。ネストされたグループも動的グループもサポートしない実装の場合は、以下のようにグループ タイプ属性を設定します。

  GroupType=NONE

  設定 NONE は、標準グループのサポートを指定します。

  デフォルトのグループ タイプ設定は ALL です。この設定は、パフォーマンスに悪影響を与える可能性があります。

  注: ディレクトリ設定ファイル内の既知の属性とグループ タイプの詳細については、「設定ガイド」を参照してください。

- プロビジョニング ディレクトリのキャッシュ インデックスの設定により、グローバル グループのパフォーマンスを改善します。

  ユーザ ストアとプロビジョニング ディレクトリを含む CA Identity Manager の統合では、GlobalGroup メンバシップは、ロールとアイデンティティ ポリシーのポリシー ルール評価について最適化できます。

この最適化を有効にするには、以下の属性にインデックスを付けます。それらのインデックスは、プロビジョニング サーバによって、プロビジョニング ディレクトリのキャッシュ内でグループ メンバシップの解決に使用されます。

eTID

一意のオブジェクト ID 属性。 グループ メンバシップの検索では、この値は検索に含まれる特定のユーザまたはグループを表します。

eTPID

メンバシップ関係の検索で使用されるオブジェクトの親 ID。

eTCID

メンバシップ関係の検索で使用されるオブジェクトの子 ID。

さらに、以下のハッシュ エントリを追加します。

eTSuperiorClass

メンバシップ検索における親オブジェクトのタイプ

eTSubordinateClass

メンバシップ検索における子オブジェクトのタイプ

注: プロビジョニング ディレクトリのキャッシュの詳細については、「インストール ガイド」を参照してください。

アイデンティティ ポリシーの最適化

*アイデンティティ ポリシー*は、ユーザが一定の条件やルールを満たすと発生する一連のビジネス変更です。これらの変更には、ロールの割り当てまたは取り消し、グループ メンバシップの割り当てまたは取り消し、ユーザ プロファイル内の属性の更新などがあります。

ユーザ同期が発生すると、CA Identity Manager はアイデンティティ ポリシーを評価します。

アイデンティティ ポリシーのパフォーマンスは、以下の要因に影響されます。

- アイデンティティ ポリシーの設定方法
- ユーザ同期の発生頻度

ユーザとアイデンティティ ポリシーとの同期の方法

アイデンティティ ポリシーを使用する際には、CA Identity Manager でのポリシー評価方法とユーザへの適用方法を理解することが重要です。 ユーザの同期プロセスを十分に理解していない場合、予期しない結果を引き起こすアイデンティティ ポリシーを設定してしまう場合があります。

CA Identity Manager でアイデンティティ ポリシーが評価および適用される方法を以下の手順に示します。

1. ユーザ同期プロセスは以下の方法で開始されます。
   - **自動** — 自動的にユーザ同期をトリガするように CA Identity Manager のタスクを設定できます。
   - **手動** — ユーザ コンソールの［ユーザの同期］タスクを使用して、ユーザを同期します。
2. CA Identity Manager は、ユーザに適用するアイデンティティ ポリシーの組み合わせを判別します。
3. CA Identity Manager は、そのユーザに適用するアイデンティティ ポリシーの一式を、そのユーザに対して適用済みのポリシーの一覧と比較します。

   注: ユーザに適用されたポリシーの一覧は、ユーザ プロファイルの %IDENTITY_POLICY% 汎用属性に格納されています。 属性の設定の詳細については、*「設定ガイド」*を参照してください。
   - 適用可能なポリシーの一覧に含まれるアイデンティティ ポリシーが、以前にそのユーザに適用されて*いない場合*、そのポリシーは CA Identity Manager で割り当て一覧に追加されます。
   - 適用可能なポリシーの一覧に含まれるアイデンティティ ポリシーが、以前にそのユーザに適用されていて、さらにそのポリシーで［1 回のみ適用］設定が無効になっている場合、そのポリシーは CA Identity Manager で再割り当て一覧に追加されます。
   - アイデンティティ ポリシーが適用可能なポリシーの一覧になく、かつ、そのポリシーがユーザに適用されている場合は、ユーザはそのポリシー条件に一致しなくなります。CA Identity Manager ではそれらのポリシーは割り当て解除一覧に追加されます。
4. ユーザに対するすべてのポリシーを CA Identity Manager が評価後、以下の順序でポリシーが適用されます。
   a. 割り当て解除一覧のアイデンティティ ポリシー
   b. 割り当て一覧のアイデンティティ ポリシー
   c. 再割り当て一覧のアイデンティティ ポリシー

5. 各アイデンティティ ポリシーの適用後、CA Identity Manager はポリシーを再評価し、最初の同期化プロセス（手順 2 から 4）で発生した変更に基づいて、新たな変更が必要かどうか確認します。

   この手順は、アイデンティティ ポリシーの適用によって加えられた変更が、他のアイデンティティ ポリシーをトリガしていないことを確認するためのものです。

6. 適用可能なすべてのポリシーとユーザが同期するまで、または管理コンソールで定義された最大再帰レベルに CA Identity Manager で達するまで、CA Identity Manager は引き続きアイデンティティ ポリシーの再評価と適用を実施します。

   たとえば、ユーザがロールに割り当てられると、アイデンティティ ポリシーはユーザの部署を変更します。 新しい部署は、別のアイデンティティ ポリシーをトリガします。ただし、再帰レベルが 1 に設定されている場合は、ユーザが再同期されるまで後続の変更は行われません。

   再帰レベルの設定の詳細については、管理コンソールのオンライン ヘルプを参照してください。

効率的なアイデンティティ ポリシーの設計

アイデンティティ ポリシーを作成する際には、以下のガイドラインに従います。

- **ポリシー オブジェクトの数を制限する**

  CA Identity Manager は、アイデンティティ ポリシーをサポートするオブジェクト ストアにオブジェクトを作成します。オブジェクト ストア内のオブジェクトの数を減らすには、複雑な表現でアイデンティティ ポリシーを作成します。
  ロール ポリシー (P. 78)についても、同様のアプローチが推奨されています。

- **アイデンティティ ポリシー セットの反復を制限する**

  アイデンティティ ポリシーには再帰レベルを設定できます。これによって、ユーザの同期時に CA Identity Manager がアイデンティティ ポリシーを評価および適用する回数が決定します。 たとえば、ユーザがロールに割り当てられると、アイデンティティ ポリシーはユーザの部署を変更します。 新しい部署は、別のアイデンティティ ポリシーをトリガします。 ただし、再帰レベルが 1 に設定されている場合は、ユーザが再同期されるまで後続の変更は行われません。

  再帰レベルの設定によって、CA Identity Manager がアイデンティティ ポリシーを評価する必要のある回数が制限されます。

- **アイデンティティ ポリシー ルール間の依存性を制限する**

  以下の表で示されるように、あるポリシーの変更アクション（［ポリシー適用時のアクション］または［ポリシー削除時のアクション］）が別のポリシーのアイデンティティ ポリシー条件で使用されるアイデンティティ ポリシーを作成できます。

アイデンティティ ポリシー条件	ポリシー適用時のアクション	ポリシー削除時のアクション
where (Job Code = "100")	Make member of (provisioning role "Account Manager")	Remove member of (provisioning role "Account Manager")
Who are members of (provisioning role "Account Manager")	Make member of (group "Account Managers")	Remove member of (group "Account Managers")

CA Identity Manager は、このタイプのポリシーを評価する際には、変更を少なくとも 2 回評価および適用して、両方の条件が満たされていることを確認する必要があります。 再帰レベルは、CA Identity Manager 環境全体に対して設定し、2 以上にする必要があります。そうすれば、アイデンティティ ポリシーセットごとに追加評価が行われます。

ユーザ同期をトリガするタスクの制限

アイデンティティ ポリシーはユーザ同期プロセス時に評価され適用されます。タスクに対して以下のユーザ同期オプションのどれかを指定することで、自動同期を設定できます。

タスク完了時

CA Identity Manager はタスクの全イベント完了後、ユーザの同期化プロセスを開始します。

各イベント発生時

CA Identity Manager はタスクの各イベント完了後、ユーザの同期化プロセスを開始します。

最高のパフォーマンスを得るには、自動的なユーザ同期をトリガするタスクの数を制限します。

ユーザ同期の設定では、以下の点を考慮します。

- **パスワード タスクのユーザ同期を無効にする**

  ほとんどの場合、アイデンティティ ポリシー条件にパスワードは使用されません。

- **［ユーザの同期］タスクのユーザ同期を無効にする**

  ［ユーザの同期］タスクは、アイデンティティ ポリシーの評価をトリガするので、このタスクに対してユーザ同期オプションが有効になっている場合は、CA Identity Manager がそれらの評価を再実行します。

- **特化したタスクを作成する**

  可能な場合は、アイデンティティ ポリシー条件をトリガする変更を実行するタスクを作成し、それらのタスクに関してのみユーザ同期を有効にします。

アイデンティティ ポリシー ルール評価の最適化

ユーザ属性を含むアイデンティティ ポリシー条件の評価時間を短縮するには、インメモリ評価オプションを有効にできます。インメモリ評価オプションが有効になっていると、CA Identity Manager はユーザ ストアから評価対象ユーザに関する情報を取得し、そのユーザの表現をメモリに格納します。CA Identity Manager は、インメモリ表現を使用して、属性値をポリシー条件と照合します。 これにより、CA Identity Manager がユーザ ストアに対して直接行う呼び出しの数が制限されます。

注: インメモリ評価オプションの詳細については、「設定ガイド」を参照してください。

ユーザ ストアの調整

ユーザ ストアの調整には、以下を含め、多数の手順があります。

- ユーザ ストアの構造の最適化
- 基礎を成すストアの調整
- 負荷分散とレプリケーションの実装

これらの手順は、使用するユーザ ストアのタイプによって異なります。これらの領域の調整情報については、ユーザ ストアが含まれるデータベースまたはディレクトリのドキュメントを参照してください。

調整に関する一般的な考慮事項に加えて、以下の CA Identity Manager 固有の調整考慮事項があります。

- **ユーザ ストア検索パフォーマンスの測定**

  最適なパフォーマンスを得るには、CA Identity Manager ポリシー評価検索は 10～20 のミリ秒以内で完了する必要があります。

  CA Identity Manager が推奨時間内にこれらの検索を常に完了できることを確認するには、複数のロード条件下で検索パフォーマンスをテストすることを検討してください。

  また、この測定を使用すると、ユーザ ストア検索がいつ物理的限界に達し、負荷分散用に追加サーバが必要となるかを決定できます。

- **属性のインデックス付け**

  ロール ポリシーまたはアイデンティティ ポリシーで使用される各属性にインデックスを付けます。 属性にインデックスを付けると、パフォーマンスを著しく向上できます。

  注: 属性のインデックス付けの詳細については、ユーザ ストアを格納する LDAP ディレクトリまたはリレーショナル データベースのドキュメントを参照してください。

- **LDAP バインドのキャッシング**

  CA Identity Manager では、すべてのディレクトリの LDAP バインドは CA Identity Manager ディレクトリ オブジェクトで定義されたプロキシ ユーザによって実行されます。 接続ごとに、同じ LDAP バインドが、この同じユーザに対して繰り返し発生します。

  LDAP ディレクトリをユーザ ストアとして使用する場合は、LDAP バインド（またはセッション）をキャッシングするようにディレクトリを設定します（ただし、ディレクトリがそれをサポートする場合）。

- **ユーザ ストア キャッシュの有効化**

  CA Identity Manager がユーザに関するポリシー決定を評価すると、その情報は許可キャッシュに格納されます。 キャッシュされた情報が期限切れになると、CA Identity Manager はそのユーザに関するポリシーをすべて再評価します。

  後続のポリシー ルール評価におけるユーザ ストア検索のパフォーマンスを改善するには、ユーザ ストアによる検索データのキャッシングを有効にします（ただし、ユーザ ストアがそのキャッシングをサポートする場合）。

  CA Directory には、dxCache と呼ばれるキャッシュが含まれています。これはキャッシングされたデータ上で検索が可能なインメモリ データベースの実装です。

  注: CA Directory の詳細については、「CA Directory 管理ガイド」を参照してください。

プロビジョニング コンポーネントの調整

CA Identity Manager の実装にプロビジョニングが含まれている場合は、以下の最適化を使用して、最良のパフォーマンスを確保します。

- CA Identity Manager Server とプロビジョニング サーバ間の接続を最適化する

  CA Identity Manager は、JIAM（Java IAM）API を使用して、プロビジョニング サーバと通信します。 通信のパフォーマンスを改善するには、以下を設定してください。

  - プロビジョニング サーバへの複数接続用 JIAM セッション プール

    注: CA では、初期セッション値を 8、最大セッション値を 128 に設定することを推奨しています。

  - プロビジョニング サーバから取得されたオブジェクト用 JIAM キャッシュ

  注: JIAM の設定値については、「管理ガイド」を参照してください。

- アカウントの同期をタスク終了時に設定する（P. 86）（各イベントの終了時ではない）
- プロビジョニング サーバを調整する

  注: 詳細については、「管理ガイド」と「インストール ガイド」を参照してください。

ランタイム コンポーネントの調整

CA Identity Manager でのビジネス変更は、タスクを介して達成されます。 タスクは 1 つ以上のイベントを含み、それらのイベントは、タスクを完了するために CA Identity Manager が実行するアクティビティです。 たとえば、［ユーザの作成］タスクは CreateUserEvent と AddToGroupEvent を含む場合があります。

CA Identity Manager には、ランタイムにタスクとイベントを処理する以下のコンポーネントがあります。

- CA Identity Manager データベース。CA Identity Manager 機能をサポートします。
- JMS メッセージ。イベントの処理に関与します。

CA Identity Manager データベースの調整

タスクを実行する際に、CA Identity Manager は以下のデータベースを使用します。

- タスク永続性

  CA Identity Manager のタスクおよびイベントに関する情報を長期にわたってメンテナンスします。 これにより、システム障害時に CA Identity Manager がイベントとタスクの最後の既知の状態を復元できます。

  注: タスクとそのイベントがこのデータベースに保存され、状態遷移時にデータベースから取得されるので、このデータベースは CA Identity Manager のパフォーマンスに最も重大な影響を及ぼします。

- 監査

  CA Identity Manager 環境で行われた操作の履歴を提供します。

- ワークフロー

  ワークフロー プロセス定義、ジョブ、スクリプトなど、ワークフロー エンジンが必要とするデータを格納します。

- レポート

  スナップショット データを保存します。スナップショット データには、スナップショット作成時における CA Identity Manager 内のオブジェクトの現状が反映されます。

CA Identity Manager は JDBC 接続プールを介して各データベースと通信します。JDBC 接続プールは、CA Identity Manager をホストするアプリケーション サーバで作成および設定します。JDBC 接続プールを設定する際には、以下の点に注意してください。

- 一度に実行する同時タスクの数について考慮します。
- JDBC 接続プール サイズの設定では、他のランタイム コンポーネントについて考慮します。各ランタイム コンポーネントは他のランタイム コンポーネントと連携して動作します。

  注: CA では、初期接続プール値を 128 に設定することを推奨します。
- タスク永続性データベースの場合、プール内のデータベース接続の数は、実行中の各タスクがそのライフタイムを通じてタスクおよびイベントのデータを取得し更新することを可能にする数である必要があります。
- タスク永続性データベースは、準備されたステートメントを使用します。 タスク永続性データの格納に使用するデータベースには、必ず準備されたステートメントのキャッシュを設定してください。

  注: 準備されたステートメント キャッシュの設定については、タスク永続性のために使用するデータベースのドキュメントを参照してください。

JMS 設定

CA Identity Manager タスクはイベント（タスクを完了するために CA Identity Manager が実行するアクション）を含みます。

イベントは、そのライフサイクル時に以下の状態を遷移します。

- BEGIN
- APPROVED
- EXECUTING
- COMPLETED
- INVALID

ワークフローによって制御されたイベントには、以下の状態もあります。

- PENDING
- REJECTED

CA Identity Manager は、 JMS メッセージを使用して、これらの状態遷移を制御します。

JMS メッセージでイベントの遷移を駆動する方法

CA Identity Manager は、JMS のメッセージを使用してイベントの状態遷移を駆動します。 その手順を以下に示します。

1. ユーザがタスクをサブミットします。
2. タスクが 1 つ以上のイベントを生成します。
3. イベントの処理準備ができると、CA Identity Manager はイベントの状態を BEGIN に設定し、イベントはタスク永続性データベースに保持されます。
4. CA Identity Manager がイベント ID を含む JMS メッセージを作成し、そのメッセージをイベント メッセージ キューにポストします。
5. JMS はメッセージを受信すると、イベント コントローラの実装であるイベント メッセージ ドリブン ビーンのインスタンスを呼び出します。
6. イベント コントローラがメッセージ内のイベント ID を使用して、タスク永続性データベースからイベントを取得し、イベントの現在の状態に対するアクションを実行します。
7. イベントは、その状態を完了すると、次の状態に設定され、タスク永続性データベース内に保持されます。そして、新しい JMS メッセージが次の状態の処理のためにポストされます。

   このサイクルは、イベントがそのステート マシンを完了するまで続行します。

JMS メッセージとパフォーマンス

どのイベントにも、状態遷移に関する JMS のメッセージを必要とする状態が 3 ～ 5 つ存在します。

- BEGIN
- PENDING （Workflow 制御下のみ）
- APPROVED または REJECTED
- EXECUTING
- COMPLETED または INVALID

単一のイベントを処理する場合は、以下のアクションが発生します。

- イベント メッセージ キューへのポスト（3 ～ 5 回）
- メッセージ ドリブン ビーンの呼び出し（3 ～ 5 回）
- タスク永続性データベースへの接続（6 ～ 10 回）。1 つの状態に対して 1 回の読み取りアクションと 1 回の書き込みアクションが発生。

これらのアクションは、CA Identity Manager によるタスク処理の時間に影響する場合があります。

状態遷移時に最良のパフォーマンスを確保するには、 CA Identity Manager をホストするアプリケーション サーバ内の JMS リソースを調整して、十分な JMS リソースを利用できるようにします。

JMS 設定の調整

以下のアプリケーション サーバの JMS 調整パラメータは、キュー接続およびメッセージ ドリブン ビーンのインスタンス プールを定義します。

- **WebSphere JMS の調整**

  WebSphere は、パフォーマンスを改善するために設定できる 2 つのパラメータをキュー接続ファクトリに提供します。 WebSphere 管理コンソールを使用して、以下のプロパティを設定してください。

  - ［Resources］の下で、キュー接続ファクトリ （iam-im-neteQCF および iam-im-wpConnectionFactory）を見つけます。
  - 各キュー接続ファクトリの接続プール プロパティを編集して、最大接続数を 128 に設定します。

- **WebLogic の調整**

  WebLogic アプリケーション サーバでは、キュー接続ファクトリは、JMS スレッド プールのサイズに応じて、サーバの JMS スレッド プールまたはデフォルトの実行プールから接続処理スレッドを取得します。 JMS スレッド プールのサイズが 0 の場合、WebLogic は実行プール内のスレッドを使用します。

  JMS スレッド プールのスレッド数は、CA Identity Manager イベント メッセージ ドリブン ビーンの最大ビーン プール サイズ（デフォルト設定は 128）に等しく設定することを推奨します。

  CA Identity Manager がインストールされているドメインおよびサーバの［JMS Services］プロパティの JMS スレッド プール サイズは、WebLogic サーバ コンソールを使用して設定します。

CA Identity Manager イベント メッセージ ドリブン ビーンのプール サイズは、以下の場所にある記述子ファイル内の max-beans-in-free-pool 設定を変更することで設定します。

WebLogic_home¥domain¥applications¥iam_im.ear¥identityminder_ejb.jar¥META-INF¥weblogic-ejb-jar.xml

```
<weblogic-enterprise-bean>
        <ejb-name>SubscriberMessageEJB</ejb-name>
        <message-driven-descriptor>
            <pool>
                <max-beans-in-free-pool>128</max-beans-in-free-pool>
                <initial-beans-in-free-pool>16</initial-beans-in-free-pool>
            </pool>

<destination-jndi-name>com.netegrity.ims.msg.queue</destination-jndi-name>
        </message-driven-descriptor>
    </weblogic-enterprise-bean>
```

- **JBoss の調整**

  JBoss アプリケーション サーバでは、キュー接続ファクトリはサーバの標準 JMS プール セッション ファクトリから接続処理スレッドを取得します。最大スレッド数は、デフォルトで 15 に設定されます。

  この値は標準メッセージ ビーン コンテナの最大サイズ値に一致させるように推奨します。

  JMS セッション プールのセクション ファクトリは、以下のファイルの JMSContainerInvoker の MaximumSize 要素で設定されます。

  jboss_home¥server¥default¥conf¥standardjboss.xml

```
<invoker-proxy-binding>
         <name>message-driven-bean</name>
         ….
         <proxy-factory-config>

<JMSProviderAdapterJNDI>DefaultJMSProvider</JMSProviderAdapterJNDI>

<ServerSessionPoolFactoryJNDI>StdJMSPool</ServerSessionPoolFactoryJNDI>
            <MaximumSize>128</MaximumSize>
            <MaxMessages>1</MaxMessages>
            ….
         </proxy-factory-config>
     </invoker-proxy-binding>
```

CA Identity Manager イベント メッセージ ドリブン ビーンのプール サイズは、以下の記述子ファイル内の最大サイズ値を変更することによって設定されます。

jboss_home¥server¥default¥conf¥standardjboss.xml

```
<container-configuration>
         <container-name>Standard Message Driven Bean</container-name>
         <call-logging>false</call-logging>

<invoker-proxy-binding-name>message-driven-bean</invoker-proxy-binding-name>
        ……
         <container-pool-conf>
            <MaximumSize>128</MaximumSize>
         </container-pool-conf>
   </container-configuration>
```

JBoss 5 パフォーマンスの調整

JBoss 5 のデフォルト インストールでは、JBoss ホット展開スキャナが 5 秒ごと実行され、JBoss のパフォーマンスに影響を与えます。この機能を無効にするか（機能が必要ない場合）、または実行頻度を変更できます。

ホット展開を無効化または変更する方法

1. 以下の場所にある hdscanner-jboss-beans.xml を編集します。

   単一ノードの場合： *jboss_home*/server/default/deploy

   クラスタの場合： *jboss_home*/server/all/deploy

2. この機能を無効にするには、HDScanner ビーン内に以下の行を追加します。
   `<attribute name="ScanEnabled">False</attribute>`
3. スキャン頻度を変更するには、scanPeriod 属性値を 5000 （ミリ秒）以上に増やします。

注: 詳細については、次のリンクを参照してください。
http://community.jboss.org/wiki/JBossASTuningSlimming。

メモリ不足エラーに対処する方法

Java ヒープのサイズが小さすぎる場合は、「Out of Memory」（メモリ不足）例外が表示される場合があります。 初期サイズには 1024 を推奨します。

第 7 章: 惨事復旧計画の作成

このセクションには、以下のトピックが含まれています。

惨事によるサービスの停止

惨事が発生すると、ユーザのジョブにとって重大なサービスへのアクセスを失う場合があります。 その結果、それらのユーザは他のユーザにサービスを提供できなくます。

サービスへのアクセス復元の緊急度は、CA Identity Manager の実際の使用状況によって左右されます。 一部の組織では、CA Identity Manager から提供されるサービスに間断なくアクセスできることを要求するユーザがいる一方で、他のユーザは一日以内のシステムの復元を必要とします。 いずれのケースについても、システムの部分的または完全な損失を引き起こすイベントから CA Identity Manager の実装を保護できるように準備することを推奨します。

CA Identity Manager の重複アーキテクチャの設定により、ユーザに対するサービスの可用性を高めることができます。 プライマリ コンポーネントに障害が発生すると、代替コンポーネントが同じサービスを引き続き提供します。 さらに、重要な システムおよびソフトウェアの定期的なバックアップにより、完全に失われたシステムまたはデータでも復元することができます。

このドキュメントでは、これらのシナリオに対して一般的な計画のガイドラインを提供します。 これらのガイドラインを使用して、各組織の要件を満たす特定の惨事復旧手順を開発することをお勧めします。

惨事からの復旧を計画する方法

効果的な惨事復旧計画を開発するには、この章で詳述される下記の段階を経る必要があります。

✓	段階
	1. 惨事復旧要件の定義 (P. 105) 組織のニーズに基づいて、どのようなタイプの惨事が予期されるか、そしてどのくらいすばやくサービスを復元する必要があるかを特定します。
	2. 重複アーキテクチャの設計 (P. 106) 要件に従って、リモートの場所で重複コンポーネントを含むアーキテクチャを設計します。
	3. バックアップ計画の開発 (P. 108) インストールを保護するため、コンポーネントをバックアップする計画を開発します。
	4. 復元手順の開発 (P. 110) 失われたコンポーネントを復元する手順を開発します。
	5. 復旧計画の文書化 (P. 113) 惨事から CA Identity Manager を復旧する計画を文書化します。
	6. 復旧計画のテスト (P. 113) 惨事復旧手順に基づいて、イベント発生前の状態に CA Identity Manager の実装を回復できることを確認します。
	7. 惨事復旧トレーニングの提供 (P. 115) 惨事からのシステム復旧を担当するスタッフがそのようにトレーニングされたことを確認して、この開発を完了します。

惨事復旧要件の定義

惨事復旧計画の要件の定義に関して、考慮すべき一般的ガイドラインを以下に示します。

1. 以下の知識を持つチームを編成します。
   - CA Identity Manager をサポートするアーキテクチャおよびシステムに関する知識
   - CA Identity Manager で使用されるリレーショナル データベースおよび LDAP ユーザ ストアをバックアップする方法に関する知識
2. 1 つ以上のサイトでのシステムの部分的または完全な損失を含め、取り組むべき可能な惨事シナリオを特定します。
3. インストールのサポートに不可欠なシステムをリストします。
4. これらのシステムの各々に許容可能な最大ダウンタイムを定義します。

   たとえば、代替のサーバをサポートするシステムは、復元の優先度を低くできます。

重複アーキテクチャの設計

重要なコンポーネントの失敗に対する保護手段として、リモートの場所で代替コンポーネント（サーバとディレクトリ）および重複データベースを使用する以下の保護アクションを考慮してください。

「インストール ガイド」を使用して、CA Identity Manager 用の冗長性を設定します。以下のコンポーネントを含めます。

- クラスタの一部としての重複 CA Identity Manager アプリケーション サーバ ノード。
- フェイルオーバを提供するポリシー サーバ クラスタ（CA SiteMinder で CA Identity Manager を保護する場合）。
- 代替のプロビジョニング サーバ、プロビジョニング ディレクトリ、およびコネクタ サーバ。プライマリ コンポーネントが失われると、代替コンポーネントに切り替わります。

以下のデータベースに冗長性を設定します。

- ワークフローまたは監査データベースなど CA Identity Manager の一部であるあらゆるランタイム データベース。

  ORACLE または Microsoft SQL Server と共に提供されたドキュメントを参照してください。
- ビジネス オブジェクト データベース（レポート サーバを使用する場合）。

  SAP ドキュメント Web サイトにある Business Objects Enterprise のリリース 2 およびリリース 2 SP4 のドキュメントを参照してください。

代替 CA Identity Manager サーバ

CA Identity Manager サーバに重複アプリケーション サーバ ノードを提供すると、拡張性およびパフォーマンスの利点に加えて、個々のサーバが失敗した場合に惨事復旧が行われます。アプリケーション サーバにフェイルオーバを提供する最も一般的な方法は、クラスタの作成です。 クラスタの作成手順は、「インストール ガイド」のクラスタのセクションに記載されています。

注: CA Identity Manager r12.0 およびそれ以降のリリースで、マルチノード展開を実装する唯一の有効な方法は、アプリケーション サーバ クラスタです。 CA Identity Manager 環境では、業界標準の J2EE クラスタ アーキテクチャが必要です。このアーキテクチャでは、バックボーン用に JMS キューを使用します。その結果、CA Identity Manager 設定で複数ノードを使用する唯一の有効な方法は、アプリケーション サーバ クラスタになります。

この変更の詳細については、TechDoc 545594 を参照してください。

代替プロビジョニング コンポーネント

いくつかのプロビジョニング コンポーネントには、高可用性を提供する代替コンポーネントのオプションがあります。 代替コンポーネントは、最高の保護を得るため、リモートサイトに置いてください。

代替のサーバおよびディレクトリの特定設定の詳細については、「インストールガイド」の「高可用性プロビジョニング」の章を参照してください。

マルチサイト プロビジョニング ディレクトリ

プライマリおよび代替のプロビジョニング ディレクトリを作成し、代替ディレクトリはリモートの場所に置くことができます。 CA Directory では、3 つのプロビジョニング ディレクトリ（1 つはプライマリ ディレクトリ、2 つは代替ディレクトリ）をインストールすることを推奨します。

マルチサイト プロビジョニング サーバ

プライマリ プロビジョニング サーバの失敗に対する保護手段として、代替のプロビジョニング サーバを設定できます。 プライマリ プロビジョニング サーバと代替 プロビジョニング サーバ間の差異は、プライマリ サーバのインストールではプロビジョニング ディレクトリのコンテナにエントリが入力されることです。プライマリ サーバをアンインストールすると、それらのエントリも削除されます。インストールとアンインストール以外は、プライマリ サーバと代替サーバは同様に機能します。

マルチサイト コネクタ サーバ

Java または C++ コネクタ サーバのいずれの場合も、同じエンドポイントまたはエンドポイント タイプに対して機能する複数のコネクタ サーバを設定できます。

設定するコネクタ サーバごとに、リモートの場所で同じエンドポイントを処理する代替コネクタ サーバを設定してください。 コネクタ サーバが失敗すると、代替サーバがただちにエンドポイントとの通信を管理します。

重複データベース

サポートされているデータベース ソフトウェア（Microsoft SQL Server および Oracle）は、重複データベースを提供する機能を備えています。 メイン のデータベースが失敗した場合は、重複データベースをただちに利用できます。 サイト全体に影響が及ぶ場合に備え、重複データベースはリモートサイトに配置してください。

バックアップ計画の開発

一部またはすべてのシステムの喪失に対する保護措置として、バックアップする全データのオフサイト ストレージと、最大ダウンタイム要件を満たすバックアップ スケジュールを使用します。バックアップと復元の手順では、さまざまなアプリケーションが使用されます。したがって、それらのアプリケーションを全体として CA Identity Manager システムの復旧に役立つように調整する必要があります。

バックアップ計画には、以下のコンポーネントを含めます。

コンポーネント	説明	バックアップ方式
CA Identity Manager ユーザ ストア	CA Identity Manager ユーザのレコードを格納する LDAP ユーザ ディレクトリまたはリレーショナル データベース。	データベースまたは LDAP ソフトウェアと共に提供されたドキュメントを参照してください。
CA Identity Manager データベース	タスク永続性、ワークフロー、監査、オブジェクト ストア、レポーティング、およびタスク永続性アーカイブの各データベース。 ワークフロー データベース、タスク永続性データベース、および監査データベースは、変更頻度が最も高いので、バックアップを適宜スケジュールする必要があります。	ご使用のデータベース ソフトウェアと共に提供されたドキュメントを参照してください。
SiteMinder ポリシー ストア	SiteMinder ポリシー サーバ用のオブジェクトを持つ LDAP ユーザ ディレクトリまたはリレーショナル データベース（ただし SiteMinder を使用する場合）。	データベースまたは LDAP ソフトウェアと共に提供されたドキュメントを参照してください。
プロビジョニング ディレクトリ	プロビジョニング ユーザおよびプロビジョニング オブジェクトのレコードを含む LDAP ユーザ ディレクトリ。	CA Directory のドキュメントを参照してください。
アプリケーション サーバ JMS 永続性ストア	これらのストアは、CA Identity Manager タスク イベント処理メッセージの保存に使用されます。	アプリケーション サーバのドキュメントを参照してください。

コンポーネント	説明	バックアップ方式
レポート データベース	スナップショット データベース ビジネス オブジェクト データベース	データベース ソフトウェアと共に提供されたドキュメントを参照してください。
カスタム レポート	カスタム レポートおよび関連 XML ファイル	SAP ドキュメント Web サイトにある Business Objects Enterprise リリース 2 およびリリース 2 SP4 のドキュメントを参照してください。

ファイル システム バックアップ プログラムを使用して、バックアップ計画に、以下のコンポーネントを含めます。

コンポーネント	説明
Web サーバ コンポーネント	アプリケーション サーバ プラグインおよび SiteMinder Web エージェントなど、展開された Web サーバ コンポーネントの設定。 負荷分散を使用する場合か、SiteMinder でユーザ コンソールへのアクセスを保護する場合は、Web サーバ フロント エンドが必要です。
XML データ ファイル	CA Identity Manager Object Store オブジェクトを作成し、メンテナンスし、アーカイブするために使用されるすべての CA Identity Manager ディレクトリおよび環境ファイル。
CA Identity Manager カスタマイズ コンポーネント	以下の展開された iam_im.ear フォルダの下にあるファイル ■ Config ■ User_console.war WEB-INF¥web.xml
スクリプトとプログラム	TEWS スクリプト、プログラム、プログラム出口
Connector Xpress コンポーネント	カスタム コネクタ。 Connector Xpress プロジェクト ファイル。
惨事復旧ドキュメント	惨事復旧に関する独自のドキュメントを作成したら、そのドキュメントを定期的にバックアップして、手順の変更に備えます。

復元手順の開発

復元手順は、バックアップ方式によって異なります。 故障したシステムの復旧プロセスは、状況によって異なります。 ただし、多くの場合、ソフトウェアの再インストールが復元の方法です。 詳細については、「インストール ガイド」の「高可用性プロビジョニング」の章を参照してください。

CA Identity Manager ユーザ ストアの復元

CA Identity Manager ユーザ ストアを復元するには、データベースまたは LDAP ソフトウェアと共に提供されたドキュメントを参照してください。 バックアップからのデータ ストアが、すべてのユーザ ストアへのアクセスを含め、完全であることを確認します。

CA Identity Manager データベースの復元

CA Identity Manager データベースを復元するには、データベースと共に提供されたドキュメントを参照してください。 バックアップからのデータ ストアが、すべてのデータベースへのアクセスを含め、完全であることを確認します。

SiteMinder ポリシー ストアの復元

SiteMinder ポリシー ストアを復元するには、データベースまたは LDAP ソフトウェアと共に提供されたドキュメントを参照してください。 バックアップからのデータ ストアが、すべてのユーザ ストアへのアクセスを含め、完全であることを確認します。

CA Identity Manager サーバの復元

CA Identity Manager サーバのクラスタ ノードを失った場合は、以下の手順を実行します。

1. 標準的な文書化された手順を使用して、ノードを追加します。

   「インストール ガイド」のクラスタ インストールに関する章を参照してください。

2. プロビジョニング サーバへの接続を更新します。

   詳細については、「インストール ガイド」の「High Availability」の章にあるフェイルオーバに関するセクションを参照してください。

プロビジョニング サーバおよびディレクトリの復元

失われたプロビジョニング サーバは、代替サーバをインストールすることで復元できます。システムがすべて故障した場合は、惨事発生時に失われたデータを復元します。

以下の手順を使用します。

1. カスタム スキーマ ファイルを CA Directory config¥schema ディレクトリにコピーします。
2. 新しいプロビジョニング ディレクトリをインストールします。

   データ ストアは空になります。

3. バックアップ場所からデータを復元します。
4. プロビジョニング サーバのインストーラを使用し、新しく復元されたプロビジョニング ディレクトリの詳細を提供します。

   ドメイン情報はすでに入力されています。

5. バックアップから任意のカスタム コネクタおよび設定ファイルを復元します。

注: 詳細については、CA Directory のドキュメントを参照してください。

コネクタ サーバの復元

コネクタ サーバを失った場合は、以下の手順を実行します。

1. コネクタ サーバのインストーラを使用して、新しいコネクタ サーバをインストールします。

   そのコネクタ サーバをインストール中にプロビジョニング サーバに登録します。

2. csfconfig または Connector Xpress を使用して、失われたコネクタ サーバの登録を削除します。

レポート サーバの復元

レポート サーバが失われた場合は、適用される手順についてビジネス オブジェクトのドキュメントを参照してください。 SAP ドキュメントの Web サイトで、Business Objects Enterprise のリリース 2 および リリース 2 SP 4 のドキュメントの有無を確認します。

管理タスクの復元

管理タスクは、惨事発生時に処理中だった場合、以下の条件で復旧できます。

- 保留中状態で承認を待機中だった管理タスクは、その状態情報のメンテナンスに使用されたストアが保存されている限り、引き続き利用できます。 これらのストアには、タスク永続性データベース、タスクおよびイベントの JMS メッセージを保持する JMS ストア、ワークフロー データベースなどがあります。
- 実行中状態 (保留中以外の任意の状態) のタスクには、追加条件があります。

  この状態のタスクの処理を続行するには、CA Identity Manager イベント メッセージ キューに新しい JMS メッセージをポストする必要があります。 そのイベントがキューにポストされる前に障害が発生すると、復旧時にタスクが続行されません。

  この状況でタスクを復旧するには、2 つのオプションがあります。

  - タスクが［サブミット済みタスクの表示］で失敗状態として表示されている場合は、タスクの詳細ページに移動し、［タスクのサブミット］オプションでタスクを再サブミットします。
  - 同じ変更を含む新しいタスクをサブミットします。

復旧計画の文書化

この章のガイドラインに基づいて、組織に適用される特定の惨事復旧ドキュメントを開発することを推奨します。

以下のアプローチを検討してください。

1. アーキテクチャ内のシステムの名前および場所と、各システムの代替コンポーネントの名前および場所を特定します。

   システムごとに、インストール済みソフトウェア（インストールされた特定の JDK など）、アプリケーション サーバの修正リリース、およびインストールされたメモリ容量をリストします。 この詳細情報は、完全な再構築が必要と判定したあらゆるシステムについて必要です。

2. 必要な場合は、各コンポーネントの復旧手順または完全なシステムの再構築手順を書き出します。

3. システムおよび CA Identity Manager ユーザ インターフェースに対するユーザ名およびパスワードが 1、2 名の人にしか知られていない場合は、それらを見つけるかリセットする方法を特定します。

4. 惨事復旧ドキュメントを保護するため、そのバックアップ コピーを作成して、既知のオフサイト場所に保存します。

復旧計画のテスト

惨事からの復旧を成功させるには、一定のシステムが利用できなくなる惨事のシミュレーションをスケジュールできます。 以下のテストを検討してください。これらのテストは、以降のセクションで説明されます。

1. フェイルオーバ プロセスのテスト
2. システムの復元のテスト

フェイルオーバ プロセスのテスト

すべてのサーバまたはディレクトリには、以下のコンポーネントを含む代替のサーバまたはディレクトリがリモートサイトに存在する必要があります。

- CA Identity Manager サーバ
- プロビジョニング サーバ
- プロビジョニング ディレクトリ
- C++ および Java コネクタ サーバ
- レポート サーバ
- ポリシー サーバ

手動で各コンポーネントを停止して、代替コンポーネントの使用ですべての操作が引き続き機能することを確認します。たとえば、プロビジョニング サーバについて、以下のテストを実行できます。

1. プライマリ プロビジョニング サーバのあるシステムで、［Windows サービス］ダイアログ ボックスからプロビジョニング サービスのサービスを停止します。

   プライマリ プロビジョニング サーバが停止します。

2. ユーザ コンソールで、以下のアクションを実行します。

   a. プロビジョニング ロールをユーザに割り当てます。

   b. そのユーザのエンドポイント アカウントが作成されることを確認します。

      作成されるアカウントは、CA Identity Manager サーバとの通信を処理する代替プロビジョニング サーバに依存します。

この手順はあるテストの例です。停止するコンポーネントごとに、同様のテストを開発して、代替コンポーネントが使用されていることを確認します。

復元手順のテスト

惨事復旧ドキュメントに従って重要な各コンポーネントをテストして、失われたシステムを復元できることを確認します。

惨事復旧トレーニングの提供

復旧手順の信頼性を確信したら、復旧手順の実装の担当者がその実装を実行できるように支援してください。組織によっては他の手順を必要とする場合があります。一般的ガイドラインは以下のとおりです。

1. 復旧ドキュメントの場所を発表します。
2. トレーニングの予行演習を行います。
3. トレーニングからのフィードバックを取り入れることにより、惨事復旧手順を最終的に十分なものにします。

注: また、復旧調整者の割り当てを行う（あるスタッフを復旧調整者とし、2 人目を代替調整者とする）機会として、トレーニングの使用を選択することもできます。 これらの人々は、惨事復旧計画を開始するため、文書化された場所で会合するように指示されます。