HP Universal CMDB Configuration Manager

Windows および Linux オペレーションシステム向け

ソフトウェア・バージョン：9.20

デプロイメント・ガイド

ドキュメント・リリース日：2011 年 6 月（英語版）
ソフトウェア・リリース日：2011 年 6 月（英語版）

ご注意

保証

HP の製品，またはサービスの保証は，当該製品，およびサービスに付随する明示的な保証文によってのみ規定されるものとします。ここでの記載で追加保証を意図するものは一切ありません。ここに含まれる技術的，編集上の誤り，または欠如について，HP はいかなる責任も負いません。

ここに記載する情報は，予告なしに変更されることがあります。

権利の制限

機密性のあるコンピュータ・ソフトウェアです。これらを所有，使用，または複製するには，HP からの有効な使用許諾が必要です。商用コンピュータ・ソフトウェア，コンピュータ・ソフトウェアに関する文書類，および商用アイテムの技術データは，FAR 12.211 および 12.212 の規定に従い，ベンダーの標準商用ライセンスに基づいて米国政府に使用許諾が付与されます。

著作権について

ドキュメントの更新情報

このガイドの表紙には，次の識別情報が記載されています。

- ドキュメント・リリース日は，ドキュメントが更新されるたびに変更されます。
- ソフトウェア・リリース日は，このバージョンのソフトウェアのリリース期日を表します。

最新の更新のチェック，またはご使用のドキュメントが最新版かどうかのご確認には，次のサイトをご利用ください。

http://support.openview.hp.com/selfsolve/manuals

このサイトを利用するには，HP Passport への登録とサインインが必要です。HP Passport ID の取得登録は，次の Web サイトから行なうことができます。

http://h20229.www2.hp.com/passport-registration.html（英語サイト）

または，HP Passport のログイン・ページの［**New users - please register**］リンクをクリックします。

適切な製品サポート・サービスをお申し込みいただいたお客様は，最新版をご入手いただけます。詳細は，HP の営業担当にお問い合わせください。

サポート

HP ソフトウェア・サポート Web サイトを参照してください。

http://support.openview.hp.com

HP ソフトウェアが提供する製品，サービス，サポートに関する詳細情報をご覧いただけます。

HP ソフトウェア・サポート・オンラインでは，セルフソルブ機能を提供しています。お客様の業務の管理に必要な対話型の技術支援ツールに素早く効率的にアクセスいただけます。HP ソフトウェア・サポート Web サイトのサポート範囲は次のとおりです。

- 関心のある技術情報の検索
- サポート・ケースとエンハンスメント要求の登録とトラッキング
- ソフトウェア・パッチのダウンロード
- サポート契約の管理
- HP サポート窓口の検索
- 利用可能なサービスに関する情報の閲覧
- 他のソフトウェア・カスタマとの意見交換
- ソフトウェア・トレーニングの検索と登録

一部を除き，サポートのご利用には，HP Passport ユーザとしてご登録の上，ログインしていただく必要があります。また，多くのサポートのご利用には，サポート契約が必要です。HP Passport ID を登録するには，次の Web サイトを参照してください。

http://h20229.www2.hp.com/passport-registration.html（英語サイト）

アクセス・レベルの詳細については，次の Web サイトを参照してください。

http://support.openview.hp.com/access_level.jsp

目次

第 I 部

インストールと構成

第 1 章

概要

本章 の内容

コンポーネント

HP Universal CMDB Configuration Manager においては，いくつかのコンポーネントがまとめてリリースされています。

➤ **HP Universal CMDB ファウンデーション**

HP Universal CMDB ファウンデーション（UCMDB ファウンデーション）は 企業の IT 組織向けの構成管理データベース（CMDB）であり，ビジネス・サービス定義や関連するインフラストラクチャ関係の文書化，格納，管理に使用します。

UCMDB ファウンデーションにより，データ・モデル，データ・フロー管理，データ・モデリング機能が実装されるとともに，重要な疑問の答えを導き出し，ビジネス上の問題解決に役立つ包括的な情報を CMDB データから得るためのインパクト分析，変更追跡，レポート機能が提供されます。

➤ HP Universal CMDB Configuration Manager

HP Universal CMDB Configuration Manager（Configuration Manager）では，新しいポリシーベースのトポロジとインベントリ構成の統制を導入しています。構成管理者および構成所有者向けに，UCMDB で提供されている CI データおよびトポロジのコンテンツに加えて，これらの分析を可能にします。構成管理者および構成所有者は Configuration Manager により，トポロジおよびインベントリ構成ポリシーのセットアップを容易にし，組織の基準への適合度を自動的に判別するためのツールを手に入れることができます。

Configuration Manager は Tomcat ベースの追加サーバとしてデプロイされます。UCMDB サーバとの通信には，広範囲の UCMDB SDK を使用します。

➤ HP Discovery and Dependency Mapping Advanced Edition

HP Discovery and Dependency Mapping Advanced Edition（DDMA）ソフトウェアは常に最新のコンテンツを豊富に備えており，UCMDB での IT インフラストラクチャ・データの取得および保守に便利です。

➤ HP Operations Orchestration

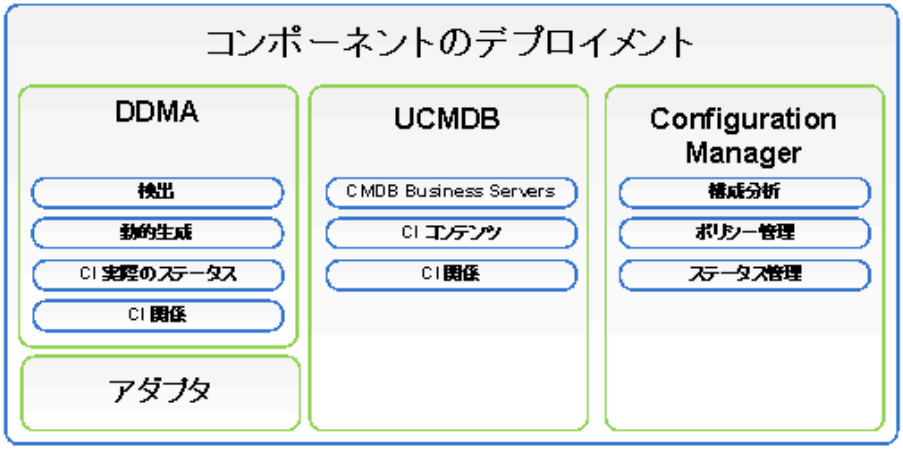
HP Operations Orchestration（OO）は，フロー作成およびデプロイメントのツールです。OO Studio のドラッグでつなぐ操作は直感的で，プログラミング・スキルがほとんど，あるいはまったくなくても，フローの設計，作成，共有，カスタマイズを行うことができます。OO Studio では，バージョン管理機能を通じ，複数の作成者が協力して作業することができます。強力なビルトイン・デバッガによって複数の環境でフローをテストできるため，コンテンツ開発に要する期間を短縮するとともに，フローを検証して実行の安定性と信頼性を確保できます。

また，OO Studio により，フローのデプロイも容易になります。ユーザは複数の環境にわたってフローを比較して進めることができます（開発，テスト，ステージング，本稼働）。標準プロセスを文書化することで，Studio を使用してコンプライアンス要件をサポートするための構造化された文書を生成できます。

➤ Configuration Manager と OO の統合

Configuration Manager には，Configuration Manager フレームワーク内から OO フローを実行する機能があります。OO フローを実行する方法は主に 2 つあります。

- ➤ **プロセスの統合**：外部サービス・デスク要求で，特定の CI と特定の構成ポリシーを対応させる RFC をオープンできます。
- ➤ **ポリシーの改善**：構成に関する問題を改善する OO フローをトリガできます。たとえば，仮想ホスト・マシンに追加メモリを割り当てることが可能です。



環境の特定

本書では, さまざまな始点から HP Universal CMDB Configuration Manager をデプロイするプロセスを説明します。

Configuration Manager について

➤ Configuration Manager バージョン 9.10 がインストールされている場合

Configuration Manager を最新バージョンにアップグレードする方法の詳細については, 37 ページ「Configuration Manager のアップグレード」を参照してください。

➤ Configuration Manager のどのバージョンもインストールされていない場合

詳細については，次を参照してください。

- ➤ 17 ページ「Windows プラットフォームでの HP Universal CMDB Configuration Manager のインストール」
- ➤ 39 ページ「Linux プラットフォームでの HP Universal CMDB Configuration Manager のインストール」

UCMDB について

➤ 9.03 より古いバージョンの UCMDB がインストールされている場合

次の手順を実行します。

- ➤ UCMDB バージョン 9.03 にアップグレードします。詳細については,『HP Universal CMDB デプロイメント・ガイド』（PDF）を参照してください。マニュアルは http://support.openview.hp.com からダウンロードできます。
- ➤ Cumulative Update Pack 2 をインストールします。Configuration Manager のインストール・メディアから入手するか, http://support.openview.hp.com からダウンロードできます。

社内準備のための構成の詳細については，18 ページ「データベースまたはユーザ・スキーマの構成」を参照してください。

➤ UCMDB バージョン 9.03 がインストールされている場合

Cumulative Update Pack 2 をインストールします。Configuration Manager のインストール・メディアから入手するか，http://support.openview.hp.com からダウンロードできます。

社内準備のための構成の詳細については，18 ページ「データベースまたはユーザ・スキーマの構成」を参照してください。

➤ UCMDB のどのバージョンもインストールされていない場合

次のいずれかの手順を実行します。

➤ Deployment Manager（Windows システム専用）を使用して，Configuration Manager と同時に UCMDB をインストールします。詳細については，17 ページ「Windows プラットフォームでの HP Universal CMDB Configuration Manager のインストール」を参照してください。

➤ 39 ページ「Linux プラットフォームでの HP Universal CMDB Configuration Manager のインストール」の手順に従い，Configuration Manager を Linux システムにインストールします。

一般情報

本書では，個々の環境における特別な UCMDB デプロイメント（高可用性デプロイメントなど）も考慮し，デプロイ手順に必要な調整を加えています。

注 : UCMDB と Configuration Manager の両方を，同じサーバにインストールすることができます。本稼働環境での拡張を念頭に置き，HP ソフトウェアではこれらのコンポーネントを別のサーバにインストールすることをお勧めしています。

Configuration Manager を使用するには，UCMDB が統合スキーマ・モードで構成され，新しい UCMDB ステータス（認証済みステータス）が作成されている必要があります。これらの構成はデプロイメント手順によって自動的に実行され，インストール状況（UCMDB がすでにインストールされている場合，Deployment Manager によってインストールされている場合）を問いません。

重要：既存の UCMDB を参照し，スキーマがまだ統合されていない場合，大規模データベース（CI が 500 万を超えるもの）の統合手順に長い時間がかかることがあります（20 ～ 60 分）。

Configuration Manager のみをデプロイする（つまり，既存またはアップグレードした UCMDB を使用する）場合，Configuration Manager のインストールを完了するには，UCMDB サーバが動作している必要があります。

サポート・マトリックス

サーバのシステム要件

CPU	最小 4 コア
メモリ（RAM）	4 GB 以上
プラットフォーム	x64
オペレーティング・システム	Windows（64 ビット） ➤ Windows 2003 Enterprise SP2 および R2 SP2 ➤ Windows 2008 Enterprise SP2 および R2 Linux ➤ Red Hat Enterprise Linux x86（64 ビット）
データベース	➤ Microsoft SQL Server 2005 SP2, 2005 Compatibility Mode 80（すべて Enterprise Editions） ➤ Microsoft SQL Server 2008 ➤ Oracle 10.2.x，11.x
Web サーバ	➤ Microsoft IIS 7 ➤ Apache 2

HP Universal CMDB	➤ HP Universal CMDB バージョン 9.03，CUP 2（一般的なインストールの CMDB） システム要件の全一覧については，『HP Universal CMDB デプロイメント・ガイド』（PDF）を参照してください。 **注：** ➤ HP Universal CMDB サーバを Configuration Manager とともにデプロイする場合，Oracle Enterprise Edition と Oracle Partitioning オプションが必要です。 ➤ HP Universal CMDB サーバと Oracle Standard Edition とともにデプロイしており，Configuration Manager を追加する場合，Partitioning オプションを有効にして，Standard Edition データベースを Enterprise Edition データベースに変換する必要があります。
LDAP（オプション）	➤ Active Directory ➤ SunONE 6.x
データベース・スキーマの推奨最小サイズ（オプション）	2 GB

クライアントの要件

オペレーティング・システム	➤ Windows XP x86（32ビット） ➤ Windows Vista x86（32 ビットおよび 64 ビット） ➤ Windows 7 x86（32 ビットおよび 64 ビット）
ブラウザ	➤ Microsoft Internet Explorer 7.0，8.0 ➤ Mozilla Firefox 3.x，4
Flash Player ブラウザ・プラグイン	Flash Player 9 以降 **注：**Flash Player は http://www.adobe.com/products/flashplayer/ からダウンロードできます。

画面の解像度	➤ 1024×768 以上 ➤ 1280×1024 を推奨
画面の色	16 ビット以上

HP Operations Orchestration（オプション）

HP Operations Orchestration	➤ 7.51, 9.0

第 2 章

Windows プラットフォームでの HP Universal CMDB Configuration Manager のインストール

重要：最新のインストール方法については，必ずリリース・ノートを確認してください。

本章の内容

インストール前のセットアップ

本項の内容

データベースまたはユーザ・スキーマの構成

注：このタスクは，Configuration Manager のインストール・プロセスの一部として自動的に実行されます。ただし，選択して手動で実行することもできます。

Configuration Manager の操作には，データベース・スキーマが必要です。Configuration Manager と UCMDB では，使用するスキーマが異なります。Configuration Manager では，Microsoft SQL Server と Oracle Database Server がサポートされています。このタスクでは，Configuration Manager 用のスキーマの作成方法を説明します。UCMDB をインストールする場合，UCMDB 用の別のデータベースまたはユーザ・スキーマが必要です。詳細については，『HP Universal CMDB デプロイメント・ガイド』（PDF）を参照してください。

注：Microsoft SQL Server と Oracle Server でのシステム要件については，14 ページ「サーバのシステム要件」を参照してください。

データベースを構成するには，次の手順を実行します。

1 Microsoft SQL Server データベースまたは Oracle Server ユーザ・スキーマのいずれかを割り当てます。

- **Microsoft SQL Server の場合**：スナップショット分離を有効にします。

  データベースの作成後，次のコマンドを 1 回実行します。

  ```
  alter database ＜ccm データベース名＞ set read_committed_snapshot on
  ```

  SQL Server のスナップショット分離の詳細については，http://msdn.microsoft.com/ja-jp/library/tcbchxcb(VS.80).aspx を参照してください。

- **Oracle の場合**：Oracle ユーザに **Connect** および **Resource** の役割のみを付与します（**Select any table** 権限を付与すると，スキーマ入力手順でエラーが発生します）。

2 次の表では，この構成プロセスで必要になる情報を示しています。内容を確認してください。

✔	必要な情報
	DB ホスト名とポート
	DB ユーザ名とパスワード
	MS SQL の場合：データベース名
	Oracle の場合：SID

UCMDB 高可用性環境での Configuration Manager のインストール

Configuration Manager を UCMDB 高可用性環境で使用するには，次の手順を実行します。

1 バックアップ（パッシブ）サーバをシャットダウンします。シャットダウンの後，2 分間待ちます。

2 Configuration Manager バージョン 9.20 をインストールします。

- **a** ロード・バランサのホスト詳細を使用します。
- **b** プライマリおよびバックアップの UCMDB サーバ以外のサーバに Configuration Manager をインストールします。

3 UCMDB および Configuration Manager が正常に動作していることを確認します。

4 バックアップ（パッシブ）サーバを起動します。これにより，高可用性環境が実現されます。

注：高可用性モードは HP Universal CMDB Configuration Manager バージョン 9.20 そのものではサポートされていません。

Configuration Manager のインストール

Deployment Manager は UCMDB，Configuration Manager，DDMA をさまざまな構成（インストール・ウィザードの［Products Selection］ページで選択，構成）でインストールできます。

- ➤ UCMDB の新規インスタンスのインストール
- ➤ Configuration Manager の新規インスタンスのインストールと新規または既存インスタンスへの接続
- ➤ Configuration Manager の新規インスタンスの OO の既存インスタンスへの統合
- ➤ DDMA の複数のインスタンスのインストール

注：

- ➤ Deployment Manager により，ターゲット・マシンに製品，コンポーネント，統合をインストールできます。製品のアンインストール，変更，インストール済み製品のパッチのインストールは Deployment Manager では行えないため，手動で実行する必要があります。
- ➤ ［Products Selection］ページで［**Next**］ボタンをクリックした後は，このページに戻ってデプロイメント構成を選択し直すことはできません。デプロイメント構成に変更を加えるには，Deployment Manager を再起動してください。

Configuration Manager をインストールするには，次の手順を実行します。

1. インストールを開始するため，Configuration Manager のインストール・メディアをマシンに挿入し，**setup.exe** ファイルの場所を確認します。
2. **setup.exe** ファイルをダブルクリックして，Deployment Manager を実行します。
3. インストール中，ターゲット・マシンの Windows ファイアウォールを無効にします。ファイアウォールの詳細については，この手順のステップ 6を参照してください。

4 エンド・ユーザ・ライセンス契約の条件に同意し，[**Next**] をクリックすると，[Products Selection] ページが開きます。

注 : ライセンス契約の条件は，Deployment Manager の［Products Selection］ページで選択したすべての製品に適用されます。

---

5 ［Products Selection］ページで，デプロイメントに必要な製品を選択します。完了したら，[**Next**] をクリックして，［Server Location］ページに進みます。

［Products Selection］ページで，インストールする製品を選択し，デプロイメント中に実行する構成オプションを指定できます。

a HP Universal CMDB ファウンデーションのインストール・オプションを選択します。

UCMDB ファウンデーションには，2 つのインストール・オプションがあります。

➤ [**Connect to an Existing Server**] : このオプションを選択すると，Configuration Manager または Discovery and Dependency Mapping が UCMDB ファウンデーション・サーバの既存インスタンスに接続されて構成されます。

注 : 既存のサーバの UCMDB バージョンは 9.03，CUP 2 以降である必要があります。

➤ [**Install New Server**] : このオプションを選択すると，UCMDB ファウンデーション・サーバの新規インスタンスがインストール，構成，接続され，Configuration Manager または DDMA が UCMDB ファウンデーション・サーバの新規インスタンスに接続されます。

b ［**Configuration Manager**］チェック・ボックスを選択し，Configuration Manager の新規インスタンスをインストールして構成します。

必要に応じて，［**Connect to an exsting HP Operation Orchestration instance**］を選択します。このオプションを選択すると，Configuration Manager に OO サーバ構成の詳細が入力され，Configuration Manager と Operations Orchestration の統合が構成されます。

c ［**HP Discovery and Dependency Mapping Advanced Edition**］: このオプションを選択すると，DDMA の新規インスタンスがインストールされて構成されます。

［**Number of DDMA instances**］オプションを選択すると，DDMA の複数のインスタンスをインストールできます。入力フィールドに入力する数は，1 つの UCMDB サーバ・インスタンスに接続する DDMA のインスタンスの数を示します。

注 : Deployment Manager では，同じ DMZ 内で複数の DDMA インスタンスをデプロイできます。デプロイメントあたり最大 10 のディスカバリ・プローブ・インスタンスがサポートされています。ディスカバリ・プローブの数を増やす必要がある場合は，複数のデプロイメント・フェーズで 10 単位でインストールしてください。

---

6 ［Server Location］ページでデプロイメントに対して選択した製品ごとに，ターゲット・デプロイメント・マシンのリモート・サーバの場所と資格情報を入力します。完了したら，［**Next**］をクリックして，［Connections］ページに進みます。

デプロイメント・オプション

ターゲット・マシンのデプロイメント・オプションを選択します。次の 2 つのオプションから選択できます。

- ［**Deploy on the local machine**］: このオプションは，Deployment Manager と同じマシンに製品をデプロイする場合に使用します。この場合，リモート・ホストの詳細および資格情報のフィールドは無効になります。
- ［**Deploy on the following machine**］: このオプションを選択すると，リモート・ホストのアドレスおよびオペレーティング・システムの詳細を入力する必要があります。入力したユーザ資格情報には，リモート・ホストでの管理者権限が必要です。

注 : 製品のデプロイのためにホスト名を入力するとき，使用できるのは文字（a ～ z），数字（0 ～ 9），ハイフン記号（「-」）のみです。

リモート・マシンの詳細を入力する際は，次の情報が必要です。

- **WMI および SMB プロトコル** : リモート・マシンの接続に使用します。Deployment Manager がリモート・マシンに正常に接続するには，次の前提条件が満たされている必要があります。
  - **WMI サービス** : WMI サービスがリモート・マシンで動作している必要があります。
  - **Server サービス** : SMB プロトコルを有効にするには，Server サービスがリモート・マシンで動作している必要があります。
  - **Windows ファイアウォール** : リモート・マシンがリモート管理接続を許可している必要があります。リモート・マシンのコマンド・プロンプト・コンソールで，関連するコマンドを実行します。

オペレーティング・システム	コマンド
Windows XP Windows Server 2003 Windows Server 2003 R2	netsh firewall set service RemoteAdmin enable
Windows Vista Windows 7 Windows Server 2008 Windows Server 2008 R2	netsh advfirewall firewall set rule group="windows management instrumentation (WMI)" new enable=Yes

テスト接続

［**Test Connection**］をクリックして，接続の資格情報および詳細が正しいことを確認し，ローカルおよびリモート・システムのリソースを分析します。

接続テストに失敗した場合，Deployment Manager で詳細なエラー・メッセージが表示されます。［**Next**］ボタンをクリックすると，テスト接続の検証が自動的に強制実行されます。

次の項目に対し，マシン・リソースの検証が実行されます。

- **OS プラットフォーム**：製品のデプロイが認定されたオペテーイング・システムかどうかが検証されます。
- **ディスク領域**：十分なディスク領域があるかどうかが検証されます。
- **メモリ**：十分な物理メモリがあるかどうかが検証されます。
- **ポート**：必要なポートが使用可能かどうかが検証されます。

テスト接続で実行されるリソース検証は，サポートされている製品マトリックスによって異なります。

注：テストで**不明な**エラーが返された場合，デプロイメント・ホスト・マシンで次のサービスが実行されているかどうかを確認します。

- Server
- Windows Management Instrumentation

［**Next**］をクリックする前に，ユーザ・アカウント・コントロール（UAC）がオフになっていることを確認します。UAC の詳細については, http://technet.microsoft.com/ja-jp/library/cc709691(WS.10).aspx を参照してください。

7 ［Connections］ページで選択した製品同士の接続を構成します。［Connections］ページに表示される接続オプションには，［Product Selection］ページでデプロイメントに対して選択したコンポーネントが反映されます。完了したら，［**Next**］をクリックして，［Installation Configuration］ページに進みます。

- UCMDB と Configuration Manager の統合

  本項は，Configuration Manager のインストール時に［**Connect to an Existing Server**］オプションを選択した場合に表示されます。ここで，Configuration Manager と UCMDB の統合を構成できます。

注 : UCMDB の既存インスタンスに接続するには, UCMDB バージョン 9.03, CUP 2 以降である必要があります。

次の UCMDB の詳細を入力します。

フィールド	設定
UCMDB Host Name/IP	UCMDB をデプロイする場所のアドレス。 ➤ UCMDB を高可用性モードで構成している場合，19 ページ「UCMDB 高可用性環境での Configuration Manager のインストール」の手順に従います。 ➤ UCMDB をローカル・マシンにインストールし，Configuration Manager をリモート・マシンにインストールしている場合，ローカル UCMDB インスタンスの名前は localhost ではなく FQDN である必要があります。 ➤ UCMDB と Configuration Manager の DNS ドメイン名が異なり，LW-SSO 統合が必要な場合，既存の UCMDB ホスト入力フィールドに FQDN を入力する必要があります。
Protocol	HTTP または HTTPS プロトコル。
UCMDB HTTP(S) Port	HTTP または HTTPS ポートのデフォルト値は，HTTP が **8080**，HTTPS が **8443** です。
Client Certificate File	このフィールドは，HTTPS プロトコルを選択した場合に表示されます。Configuration Manager のターゲット・ホストに UCMDB クライアント証明書ファイルを手動で置き，隣の入力フィールドにファイル名を含む完全なファイル・パスを入力する必要があります。 UCMDB で HTTPS を使用する場合，キー変換を使用する必要があります。キー変換の検証は，接続テストでは行われません。

フィールド	設定
Customer Name	デフォルトの UCMDB カスタマ名は **Default Client** です。カスタマ名の値は, UCMDB と Configuration Manager の統合の構成時に使用されます。この値の検証は，接続テストでは行われません。間違った値を入力すると，デプロイが失敗します。
JMX Port	デフォルト値は **29601** です。
UCMDB System User (JMX)	UCMDB（JMX）システム・ユーザは，Configuration Manager の統合ユーザの作成，Configuration Manager パッケージのデプロイなどの JMX 機能をアクティブ化するために使用します。初期のデフォルト値は **sysadmin** です。
UCMDB System Password	UCMDB システム・ユーザのパスワード。デフォルト値は **sysadmin** です。

注 : Configuration Manager には，内部ユーザ・リポジトリが構成されています。ユーザ・リポジトリとして外部 LDAP を使用するには，Configuration Manager の構成が必要です。詳細については,『HP Universal CMDB Configuration Manager ユーザーズ・ガイド』の「システム設定」を参照してください。

➤ Configuration Manager と OO の統合

本項は，［**Connect to an Existing HP Operation Orchestration instance**］オプションを選択した場合に表示されます。ここで，Configuration Manager と OO の統合を構成できます。

次の OO の詳細を入力します。

フィールド	設定
OO Version	OO の有効バージョンは 7.5 および 9.0 です。
OO Host Name/IP	OO サーバ・マシンのホストまたは IP アドレス。
OO Port Number	デフォルトのポート番号は **8443** です。
OO Username	OO のデフォルトのユーザ名は **admin** です。このユーザは OO で外部ユーザとして構成されている必要があります。
OO Password	OO のデフォルトのパスワードは **admin** です。

➤ DDMA の構成

次のフィールドは，［**Discovery and Dependency Mapping Advanced Edition instance**］オプションを選択した場合に表示されます。ここで，UCMDB への DDMA の接続を構成できます。

次の DDMA の詳細を入力します。

フィールド	設定
Data Flow Probe Identifier	デフォルト値は DDMA マシンのホスト名です。このフィールドは自動入力されます。値は変更可能です。
Use Default Domain	このオプションはデフォルトで選択されており，ドメイン名の値に影響します。このチェック・ボックスの選択を解除すると，デフォルト名を別の値に変更できます。
Domain Name	デフォルト値は **DefaultDomain** に設定されています。このフィールドを有効にするには，［**Use Default Domain**］チェック・ボックスの選択を解除します。
Initial Heap Size in MB	DDMA の JVM に割り当てられている初期メモリ・サイズ。デフォルト値は 256 MB です。
Maximum Heap Size in MB	JVM に割り当てられる最大メモリ・サイズ。デフォルト値は 512 MB です。

8 ［Installation Configuration］ページで選択した製品のデプロイのため，デプロイメントのターゲット・ディレクトリの詳細を設定します。完了したら，［**Next**］をクリックして，［Database Configuration］ページに進みます。

選択した製品ごとにデフォルトのディレクトリ・パスが入力されます。ローカル・マシンにデプロイする場合，［Browse］オプションで別のディレクトリ・パスを選択できます。リモート・マシンにインストールする場合，このオプションは無効になっています。

注 : インストール・ディレクトリ名にはスペースは使用できず，英文字（a ～ z），数字（0 ～ 9），ハイフン記号（「-」）のみ使用できます。

---

9 ［Database Configuration］ページで，各製品のデータベース接続およびデータベース・スキーマを構成します。完了したら，［**Next**］をクリックして，［Ports Configuration］ページに進みます。

次のデータベース（スキーマ）を構成できます。

- ➤ UCMDB-CM スキーマ
- ➤ UCMDB スキーマ
- ➤ UCMDB 履歴スキーマ

フィールド	設定
Database Host Name/IP	データベース・サーバの場所を示すアドレス。
Port	MSSQL と Oracle では使用するデフォルト・ポートが異なります。Oracle のデフォルトのデータベース・ポートは 1521, MSSQL のデフォルトのデータベース・ポートは 1433 です。
SID (Oracle)	Oracle データベース・インスタンスの名前。
Admin Username (Oracle)	Oracle サーバにおける Oracle 管理者のユーザ名を入力します。
Admin Password (Oracle)	Oracle サーバにおける Oracle 管理者のパスワードを入力します。

フィールド	設定
Test Connection	入力した資格情報を使用して，ターゲット DB ホストへの接続をテストします。
Schema Name (Oracle)	スキーマ名を入力します。
Schema Password (Oracle)	スキーマのパスワードを入力します。このフィールドは，新規スキーマを作成する場合に表示されます。
Default Tablespace (Oracle)	デフォルトのテーブルスペース名を入力します。
Temporary Tablespace (Oracle)	一時テーブルスペース名を入力します。
Database Name (MSSQL)	MSSQL サーバで使用または作成するデータベース・スキーマ名を入力します。
Database Username (MSSQL)	MSSQL サーバにおける MSSQL 管理者のユーザ名を入力します。
Database Password (MSSQL)	MSSQL サーバにおける MSSQL 管理者のパスワードを入力します。

注：

- UCMDB テーブルスペースがいっぱいになった場合，製品のデプロイは成功しますが，製品およびコンポーネントが正常に動作しません。
- 新規 UCMDB スキーマの作成と既存の UCMDB 履歴スキーマへの接続はできません。
- UCMDB をリモートにインストールした場合，UCMDB スキーマで MSSQL データベースを構成するときに NTLM 認証を使用することは，セキュリティ上の理由でできません。NTLM 認証が必要な場合は UCMDB をローカルでデプロイしてください。

スキーマ・モード

Configuration Manager を使用するには，UCMDB が統合スキーマ・モードで構成され，新しい UCMDB ステータスが作成されている必要があります。

既存の UCMDB を参照し，スキーマがまだ統合されていない場合，大規模データベース（CI が 500 万を超えるもの）の自動統合手順に長い時間がかかることがあります（20 ～ 60 分）。

注：Oracle Real Application Cluster（RAC）および SQL Server のNTLM 接続は，このインストール手順では行いません。これらの接続が必要な場合は，まずシンプルなデータベース接続で Configuration Manager をインストールし，インストール・プロセスの完了後に特定の製品構成から接続を変更します。そのためには，データベース仕様に従って **database.properties** ファイルを変更します。詳細については，31 ページ「詳細なデータベース構成（Configuration Manager）」を参照してください。

データベース構成モード

Configuration Manager と UCMDB では，別のスキーマを使用する必要があります。

Configuration Manager により，Oracle または MSSQL データベース・サーバでそれぞれのデータベースを構成できます。

構成タイプ

既存スキーマに接続するか，新規スキーマを作成します。既存スキーマに接続すると，コンテンツが上書きされます。

データベース構成

この手順は Deployment Manager によって自動的に実行されます。この手順を手動で実行するには，18 ページ「データベースまたはユーザ・スキーマの構成」を参照してください。

詳細なデータベース構成（Configuration Manager）

データベース接続を構成し，標準 URL 接続に関連付ける必要があります。さらに高度な機能（Oracle Real Application Cluster など）が必要な場合は，標準接続を設定してから，使用する機能に合わせて **database.properties** ファイルを手動で編集します。

Configuration Manager は，Oracle および Microsoft SQL Server データベース用のネイティブ・ドライバを使用します。データベース URL を使用して構成可能な場合，すべてのネイティブ・ドライバ機能がサポートされます。URL は **database.properties** ファイルで記述されています。

Deployment Manager ウィザードを終了した後，データベースおよびスキーマの追加構成を実行できます。

データベース構成のフィールド

使用可能なデーターベース・タイプは Oracle と MSSQL です。選択したデータベース・タイプによって，入力フィールドが変わります。

10 ［Port Configuration］ページで，Configuration Manager の接続ポートを指定します。完了したら，［**Next**］をクリックして，［User Configuration］ページに進みます。

Configuration Manager の［Port Configuration］ページの入力フィールドには，初期のデフォルト・ポート設定が表示されます。

ポート番号が既存のものと競合する場合，変更する前に IT マネージャに相談してください。

フィールド	設定
Application HTTP Port	8180
JMX HTTP Port	39900
Tomcat Port	8005
AJP Port	8009（Apache Java Protocol）
Application HTTPS Port	8143
JMX Remote Port	39600

［**Revert to Default Values**］ボタンをクリックすると，ポートが Deployment Manager のデフォルト値にリセットされます。

11 ［User Configuration］ページで次のユーザを作成します。

- ➤ 管理者権限を持つ UCMDB-CM 初期ログイン・ユーザ・インスタンス
- ➤ UCMDB の統合ユーザ（UCMDB と Configuration Manager の統合を可能にするため，必要に応じて Configuration Manager により UCMDB に統合ユーザが作成されます）

完了したら，［**Next**］をクリックして，［Security Configuration］ページに進みます。

12 ［Security Configuration］ページで，UCMDB および Configuration Manager の新規インスタンスでグローバル LW-SSO をアクティブにします。LW-SSO の構成は，［Product Selection］ページで行った選択に従い，Configuration Manager または UCMBD の新規インスタンスでのみ行います。完了したら，［**Next**］をクリックして，［Summary］ページに進みます。

LW-SSO は，さまざまなタイプの認証およびセキュリティ・トークン（LW-SSO, SAML2 など）の検証に使用するモジュール式フレームワークです。LW-SSO を使用することで，さまざまな環境の認証情報をまとめ，アプリケーションまたはセキュリティ・フレームワークでのアプリケーション・セキュリティ・コンテキストに合わせて活用します。

LW-SSO の構成は，選択した製品コンポーネントによって異なります。

Configuration Manager を既存の UCMDB または OO インスタンスに接続する場合，LW-SSO の構成は Configuration Manager でのみ行います。UCMDB または OO から LW-SSO 文字列を抽出し，［LW-SSO String］入力フィールドに入力する必要があります。UCMDB と OO の両方に接続する場合，UCMDB インスタンスおよび OO インスタンスに設定した LW-SSO が一致していることを確認してください。

Configuration Manager の新規インスタンスを UCMDB の既存インスタンスに接続する場合，UCMDB ホスト名として FQDN を使用します。

UCMDB から LW-SSO 文字列を抽出するには，次の手順を実行します。

a UCMDB を開き，［**管理**］＞［**インフラストラクチャ設定マネージャ**］を選択します。

b ［**名前**］列で［LW-SSO 初期化文字列］フィールドを選択してダブルクリックします。

c ［現在値］入力フィールドから文字列をコピーします。

d ［Security Configuration］ページで，［LW-SSO string］入力フィールドに値を貼り付けます。

Configuration Manager を新規 UCMDB インスタンスに接続する場合，UCMDB および Configuration Manager で LW-SSO が自動的に構成されます。

13 ［Summary］ページでインストール内容と構成を確認します。完了したら，［**Next**］をクリックして，［Validation］ページに進みます。

［Summary］ページには，構成のすべての詳細とユーザの入力内容がまとまっています。必要に応じてサマリの内容を変更するには，各ページの［Back］ボタンをクリックして目的のページに移動し，デプロイメント設定を調整します。［Summary］ページに戻るには，必要に応じて［**Next**］をクリックします。

14 Deployment Manager により，リモート・マシンに十分なシステム・リソースがあるかどうか，ユーザの入力内容が正しいかどうか，データベース構成が適切かどうかを検証する一連のアクションが実行されます。これらの検証によって，ユーザが行った設定が既知の環境制限に適合するかどうかが示されます。検証プロセスは自動的に開始されます。Deployment Manager で前のページに戻って構成に変更を加えた場合は，［**Run Validation**］をクリックして検証プロセスを開始します。完了したら，［**Deploy**］をクリックして，［Deployment］ページに進みます。

15 ［Deployment］ページには，デプロイメント・プロセスの進行状況が反映されます。デプロイメント・プロセスでは，製品のインストール，手順の開始，統合，製品同士の接続が行われます。

すべての製品が正常に起動されると，デプロイメント・プロセスが完了します。

［**Details**］をクリックすると，各製品をデプロイするために Deployment Manager が実行している手順など，デプロイメントの進行状況の詳細が表示されます。

［**Cancel**］をクリックすると，デプロイメントを安全にキャンセルし，現在のデプロイメント・アクションを完了してからデプロイを終了できます。

［**Abort**］（［**Cancel**］をクリックした場合のみ使用可能）をクリックすると，現在のアクションおよびデプロイを強制終了できます。デプロイを中止することで，製品が不安定な状態になることがあります。

検証

次の表に，Deployment Manager によって実行される検証の一覧を示します。

検証	エラー・メッセージ	説明
ログイン資格情報の検証	Credentials verification failed	入力したユーザ資格情報が正しくありません。
		接続を確立できませんでした。
オペレーティング・システムの互換性の検証	Target operating system platform is <Platform> Product <Product Name> supports the following platforms <Platform>	実際のターゲット・オペレーティング・システムが，製品の認定オペレーティング・システムの一覧に含まれていません。
メモリの検証	The assigned memory (<Memory> MB) exceeds the available memory (<Memory> MB) on <Target>	割り当てられている製品すべてを動かすには，ターゲット・マシンのメモリが不足しています。
	<Memory> MB of memory are verified to be available on <Target Machine>	検証が成功しました。
ディスク領域の検証	assigned disk space for (<Memory> MB) exceeds available disk space (<Memory> MB) on drive <Target>	割り当てられている製品すべてを動かすには，ターゲット・マシンのメモリが不足しています。
	<Memory> MB of disk space are verified to be available on drive <Target>	検証が成功しました。
すべての必須プロパティの入力の検証	Missing the target storage device for the product: <Target>	製品のインストール・ディレクトリが設定されていません。

検証	エラー・メッセージ	説明
デプロイメント・マシンの定義の検証	No deployment machine is defined for <Product Name>	製品をデプロイするマシンが構成されていません。
ログイン資格情報の検証	Credentials verification failed	ログイン資格情報が正しくありません。
UAC の無効化の検証	The UAC is enabled	ターゲット・マシンで UAC が有効です。
空きポートの検証	The required port number <Port> is already in use on <Target>	目的のポートはターゲット・マシンですでに使用中です。
ターゲット・ストレージ・デバイスの存在の検証	The target storage device <Device> does not exist on <Target>	選択したターゲット・ストレージ・デバイスがターゲット・マシンに存在しません。
スキーマの存在の検証	Schema <Name> does not exist/ already exist	スキーマがターゲット・マシンに存在します（または，存在しません）。
スキーマ権限の存在の検証	Validate <Permissions> schema tables user permissions existence	DB ユーザに十分な権限がありません。
スキーマ・テーブルの存在の検証	Schema Tables <Tables> on the database: <Tables> already exist	データベースのスキーマ・テーブルはすでに存在します。
スキーマ・テーブルのユーザ権限の存在の検証	The database user does not have the correct permissions	データベース ユーザは適切な権限を持っていません。

検証	エラー・メッセージ	説明
UCMDB 接続の検証	Connection failed. Connection to UCMDB failed, host: <Host>, username: <User name>, port: <Port>, protocol: <Protocol> due to <Error>	指定した接続設定で UCMDB へのテスト接続に失敗しました。
	Existing UCMDB version must be 9.03 with CUP 2 or later.	既存の UCMDB バージョンは 9.03，CUP 2 以降である必要があります。
DB 接続の検証	The host name/IP address validation failed	指定したデータベースのホスト名/IP アドレスに到達できません。
	The username or password validation failed	指定したユーザ資格情報は有効ではありません。
	The port validation failed	指定したデータベース・ポートに到達できません。
	The SID validation failed	指定したデータベース SID が DB に存在しません。
インストールの検証	The product is already installed	製品はターゲット・ホストにすでにインストールされています。

Configuration Manager のアップグレード

アップグレード手順では，開始前に次のチェックと検証が自動的に行われます。

- UCMDB サーバへの有効な接続があること
- CUP 2 パッチが UCMDB にインストールされていること
- JMX ポートが適切であること

これらのいずれかがインストールされていない，または適切に構成されていない場合，その旨を通知するエラー・メッセージが表示されます。提示された問題を修正し，アップグレードを行ってください。

- UCMDB に接続できないことが原因でアップグレードが失敗する場合，UCMDB サーバが稼働していることを確認します。
- パッチがインストールされていないことが原因でアップグレードが失敗する場合，http://support.openview.hp.com/selfsolve/document/FID/DOCUMENTUM_UCMDB_00045 の指示に従って CUP 2 をインストールします。
- UCMDB JMX ポートが適切でないことが原因でアップグレードが失敗する場合，正しい JMX ポートを選択します。そのためには，**＜ Configuration Manager インストール・ディレクトリ＞ ¥utilities¥Upgrade¥** フォルダにある **upgrade.properties** ファイルで ucmdb.jmx.port プロパティを変更します。

アップグレードするには，次の手順を実行します。

注：アップグレード手順を開始する前に，UCMDB サーバが稼働していることを確認します。

---

1. Configuration Manager および UCMDB スキーマをバックアップします。
2. Configuration Manager のインストール・メディアの Windows サブフォルダで **setup-win64.msi** ファイルの場所を確認します。
3. ファイルをダブルクリックすると，Configuration Manager インストール・ウィザードが実行されます。
4. ［**Next**］をクリックすると［License Agreement］ページが開きます。

5 ライセンス条件に同意し，［**Next**］をクリックすると，［Customer Information］ページが開きます。

6 情報を入力して［**Next**］をクリックすると，［Setup Type］ページが開きます。

7 Configuration Manager をインストールするフォルダを選択します。前のバージョンで使用したのとは別の場所を選択します。

デフォルトでは，Configuration Manager は **c:¥hp¥cnc920** ディレクトリにインストールされます。［**Next**］をクリックしてデフォルトの場所をそのまま使用するか，［**Browse**］をクリックし別の場所を選択してから［**Next**］をクリックします。

注 : インストール・ディレクトリの名前にはスペースは使用できません。

---

8 ［**Next**］をクリックしてインストールを開始します。

インストール・ウィザードが終了した後，Configuration Manager の Post Installation ウィザードが自動的に起動します。

9 ［**Next**］をクリックして，Configuration Manager の新規インストールを行うかアップグレードを行うかを尋ねる画面に進みます。

10 ［**Upgrade**］を選択して，［**Next**］をクリックします。

11 インストールが完了したら，**post_installation.log** ファイル（**＜Configuration Manager インストール・ディレクトリ＞/tmp/log** フォルダ）で，エラーが発生せずにインストールが完了したことを確認します。

アップグレード・プロセスの実行中にエラーが発生した場合，メッセージが表示され，ウィザードを閉じることができます。この場合，HP サポートにお問い合わせください。

12 Configuration Manager サービスを開始します。

注 : アップグレード後，SSL の構成を再度行う必要があります。詳細については，84 ページ「セキュリティの強化」を参照してください。

第 3 章

Linux プラットフォームでの HP Universal CMDB Configuration Manager のインストール

重要：最新のインストール方法については，必ずリリース・ノートを確認してください。

本章の内容

インストール前のセットアップ

本項の内容

前提条件

➤ 400MB 以上の空きディスク領域

➤ 有効な X ディスプレイ（推奨）

setup.bin ファイルの入手

Linux 用インストール・ファイル（**setup.bin**）は，インストール・メディアか，HP の Web サイトからダウンロードできる ISO イメージから入手できます。次のいずれかの方法で，このファイルにアクセスします。

➤ DVD を Linux マシンにマウントします。

```
$ mkdir -p /mnt/cdrom
$ mount /dev/cdrom /mnt/cdrom
```

➤ ISO イメージをループバック・ブロック・デバイスとしてマウントします。

```
$ mkdir -p /mnt/cdrom
$ mount -o loop cnc-<バージョン>.iso /mnt/cdrom
```

➤ **setup.bin** ファイルを，Linux マシンの一時保存場所にコピーします。

Configuration Manager のインストール

このタスクでは，サーバ上に Configuration Manager をインストールする方法と，データベース接続および UCMDB との統合の設定方法を説明します。

有効な X ディスプレイがある場合，UI に Post Installation ウィザードが表示されます。有効な X ディスプレイがない場合は，ウィザード情報がコンソール・モードで表示されます。

注：本書ではコンソール・モードでの手順を説明していますが，UI ウィザードを使用している場合も同等の手順が表示されます。

Configuration Manager をインストールするには，次の手順を実行します。

1 Configuration Manager を現在の場所にインストールするには，次のコマンドを発行します。

```
chmod 755 setup.bin
$ /path/to/installation/kit/setup.bin
```

2 エンド・ユーザ・ライセンス契約（EULA）が表示されるので，同意します。EULA の最後に到達するまでスペース・バーを繰り返しクリックし，EULA の一番下までスクロールします。同意してインストールを続行するため，**yes** と入力して **Enter** を押します。

HP Universal CMDB Configuration Manager が現在の場所の **cnc** サブフォルダにインストールされます。

［Welcome］ページ

```
<============================>
Welcome
<============================>
Welcome to the HP Universal CMDB Configuration Manager
post installation wizard.
Enter [<C>ancel] [Ne<x>t]>
```

Enter を押して次のページに進みます。

データベース・ベンダの選択

```
<============================>
Database Connection Configuration
<============================>
-------
Vendor:
-------
  ->1 - Oracle
    2 - Microsoft
Enter index number from 1 to 2 OR [<C>ancel] [Back<b>] [Ne<x>t]>
```

Enter を押して Oracle を選択するか，**2** と入力してから **Enter** を押して Microsoft を選択します。

データベースのホスト名

```
-------------
Set Hostname:
-------------
        Hostname:= "localhost"
Input the new Hostname: OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

データベースのホスト名を入力し，**Enter** を押します。用意されているホスト名のデフォルト値は **localhost** です。

データベースのポート

```
---------
Set Port:
---------
        Port:= "1521"
Input the new Port: OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Oracle のデフォルト・ポートは 1521，Microsoft のデフォルト・ポートは 1433 です。別のポート番号を使用するには，ここに入力して **Enter** を押します。

SID/DB 名

```
-----------
Set SID/DB:
-----------
        SID/DB:= "orcl"
Input the new SID/DB: OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Oracle の場合，このフィールドでデータベース SID を指定します。Microsoft の場合，このフィールドでデータベース名を入力します。有効な値を入力して **Enter** を押します。

ユーザ/スキーマの名前およびパスワード

```
-------------
Set Username:
-------------
Input the Username: OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

データベース・ユーザ名を入力して **Enter** を押します。

```
Input the Password: OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

スキーマのパスワードを入力して **Enter** を押します。

データベース接続のテスト

```
--------
Set Test
--------
        Test = "Yes"
Choose [<Y>es]/[<N>o] for Test OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Enter を押すと，データベース接続がテストされます。

このウィザードはデータベース・スキーマでテーブル作成を試みるため，データベース接続のテストを強くお勧めします。接続テストを行わない場合は，**No** と入力して **Enter** を押します。

データベース接続テストが正常に完了すると，次のメッセージが表示されます。

```
success
Enter [<C>ancel] [<B>ack] [Ne<x>t]>
```

Enter を押して続行します。接続テストでエラーが発生した場合，エラー・メッセージが表示され，テストの再実行が求められます。接続の問題を修正してテストを再実行し，インストールを続行します。

アプリケーション・サーバのホスト名

```
<============================>
Application Server Configuration
<============================>
Hostname:
----
Set
----
         = "myucmdbcmhost.mydomain"
Input the new  OR [<C>ancel] [Back<b>] [Ne<x>t]>
```

ホスト名のデフォルト値は，マシンの実際のホスト名です。ロード・バランサまたはリバース・プロキシを挟んでインストールする場合，ここに外部名を入力します。

アプリケーション・サーバ・ポートのカスタマイズ

```
-------------------
Select Customize ports
-------------------
        Customize ports = "No"
Choose [<Y>es]/[<N>o] for Customize ports OR [<C>ancel] [<B>ack]
[Ne<x>t]>
```

Configuration Manager にデフォルト・ポートを使用する場合，**Enter** を押します。カスタム・ポートを使用する場合は，**Yes** と入力して **Enter** を押します。デフォルトのポート番号は次のとおりです。

ポート名	ポート番号
HTTP	8180
HTTPS	8443
Tomcat management	8005
AJP	8009
JMX HTTP	39900
JMX RMI	39600

ポートをカスタマイズする選択をした場合，前記の各ポートについて値の入力が求められます。それぞれに新しい値を入力して **Enter** を押します。

```
HTTP port:
----
Set
----
         = "8180"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
HTTPS port:
----
Set
----
         = "8443"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
Tomcat port:
----
Set
----
         = "8005"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
AJP port:
----
Set
----
         = "8009"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
JMX HTTP port:
----
Set
----
         = "39900"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
JMX remote port:
----
Set
----
         = "39600"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

初期管理者ユーザ

```
<============================>
Users Credentials
<============================>
Initial Administrative User
Admin username:
----
Set
----
Input the  OR [<C>ancel] [Back<b>] [Ne<x>t]>
```

初期ログインのためのシステム管理者またはスーパーユーザとして，初期管理者ユーザを作成します。使用する管理者ユーザなを入力して，**Enter** を押します。

```
Admin password:
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

管理者ユーザのパスワードを入力して，**Enter** を押します。

```
Confirm password:
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

確認のため，管理者ユーザのパスワードを再度入力して，**Enter** を押します。

統合ユーザ

```
Platform Integration User
Integration username:
----
Set
----
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

UCMDB 統合ユーザ名を選択します。このユーザは，このインストール後のプロセスで UCMDB に作成されます。統合用とはっきりわかるようなユーザ名を使用することをお勧めします（例：cm_integration）。選択したユーザ名を入力して **Enter** を押します。

```
Integration password:
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

統合ユーザのパスワードを入力して，**Enter** を押します。

```
Confirm password:
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

確認のため，統合ユーザのパスワードを再度入力して，**Enter** を押します。

HP Universal CMDB サーバのホスト名

```
<============================>
HP UCMDB Connection Configuration
<============================>
Hostname:
----
Set
----
         = "localhost"
Input the new  OR [<C>ancel] [Back<b>] [Ne<x>t]>
```

UCMDB サーバのホスト名を入力して，**Enter** を押します。一般的に，これはデフォルトの localhost とは異なります（本稼働環境で UCMDB と Configuration Manager の両方を同じマシンにインストールすることはお勧めしていないため）。

HP Universal CMDB サーバのポート

```
Port:
----
Set
----
         = "8080"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Enter を押して UCMDB サーバのデフォルトのポート番号である 8080 をそのまま使用するか，ポート番号を入力して **Enter** を押します。

HP Universal CMDB サーバのプロトコル

```
Protocol:
  ->1 - HTTP
    2 - HTTPS
Enter index number from 1 to 2 OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Enter を押して HTTP を使用するか，2 と入力してから **Enter** を押して HTTPS を使用します。

注 : HTTPS を選択する場合，UCMDB との変換キーが必要です。.詳細については，84 ページ「セキュリティの強化」を参照してください。この手順では，セキュリティなしの自己署名証明書の HTTPS をセットアップします。

HP Universal CMDB サーバの顧客

```
Customer:
----
Set
----
          = "Default Client"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Enter を押して UCMDB サーバのデフォルトの顧客名をそのまま使用するか，顧客名を入力して **Enter** を押します。

HP Universal CMDB サーバの sysadmin 資格情報

```
Administrative username:
----
Set
----
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

UCMDB サーバの sysadmin ユーザ名を入力します。これは, UCMDB サーバで JMX メソッドを実行できるユーザです。既存のユーザであり，インストール時に作成したユーザではありません。sysadmin ユーザの資格情報は，UCMDB サーバ管理者から入手します。

```
Administrative password:
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

UCMDB サーバの sysadmin ユーザのパスワードを入力して，**Enter** を押します。

HP Universal CMDB サーバの接続テスト

```
--------
Set Test
--------
        Test = "Yes"
Choose [<Y>es]/[<N>o] for Test OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Enter を押すと，UCMDB サーバ接続がテストされます。このウィザードはパッケージをデプロイして UCMDB サーバの構成を試みるため，サーバ接続のテストを強くお勧めします。接続テストを行わない場合は，**No** と入力して **Enter** を押します。

サーバ接続テストが正常に完了すると，次のメッセージが表示されます。

```
success
Enter [<C>ancel] [<B>ack] [Ne<x>t]>
```

Enter を押して続行します。接続テストでエラーが発生した場合，エラー・メッセージが表示され，テストの再実行が求められます。接続の問題を修正してテストを再実行し，インストールを続行します。

サマリ

実行前に，ウィザードで行った選択のサマリが表示されます。

```
<============================>
Post Installation Actions Summary
<============================>
Post installation actions summary
Users
-----
HP Universal CMDB Configuration Management admin username:admin
HP Universal CMDB Platform integration username:cm_integration

Database
--------
Vendor: Oracle
Host: mydbhost.mydomain
Port: 1521
SID/DB: orcl
Encrypt password?Yes
Create schema objects?Yes

Application Server
------------------
hostname: myucmdbcmhost.mydomain
HTTP: 8180
HTTPS: 8443
Tomcat management: 8005
AJP: 8009
JMX HTTP: 39900
JMX remote: 39600
Debug: 7878

Windows Service
---------------
Create service?No

HP Universal CMDB Platform
-----
URL: http://myucmdb.mydomain:8080
Sysadmin username:sysadmin
Customer: Default Client

Enter [<C>ancel] [Back<b>] [Ne<x>t]>
```

Enter を押して構成フェーズに進みます。構成中は，進行状況バーが表示されます。ウィザードによって次のタスクが実行されます。

1 データベース・テーブルおよびオブジェクトの作成

2 データベースへのデフォルト値および初期値の読み込み

3 初期管理者ユーザの作成

4 UCMDB サーバでの統合ユーザの作成

5 UCMDB サーバの統合

6 UCMDB サーバでの認証済みステータスの作成

7 UCMDB サーバへの Configuration Manager パッケージのデプロイ

構成が完了すると，次のメッセージが表示されます。

```
<============================>
Finish
<============================>
Post installation configuration has completed.
Enter [Finish<f>]>
```

Enter を押してウィザードを終了します。

サイレント・インストール・オプション

Configuration Manager のインストールをサイレント・モードで実行できます。サイレント・モードでは，インストール・パッケージからファイルを抽出するだけで，ポスト・インストール構成は実行されません。サイレント・モードでインストールを実行するには，次のコマンドを実行します。

```
$ /path/to/installation/kit/setup.bin -silent
```

Configuration Manager アプリケーション・サーバの実行

Configuration Manager を実行するには，次のコマンドを実行します。

```
$ cd /path/to/installation/location
$ ./start-server-0.sh
```

マシンの起動時に Configuration Manager を自動的に起動するには，**/etc/init.d** ディレクトリにスクリプトを作成します。

第 4 章

Configuration Manager へのログイン

本章の内容

Configuration Manager へのアクセス

Configuration Manager には，Configuration Manager サーバへのネットワーク接続（イントラネットまたはインターネット）が設定されたコンピュータから，サポート対象の Web ブラウザを使ってアクセスできます。ユーザに許可されるアクセス・レベルは，ユーザ権限によって決まります。ユーザ権限の割り当てについては，『HP Universal CMDB Configuration Manager ユーザーズ・ガイド』の"User Management"を参照してください。

Web ブラウザの要件や Configuration Manager を正しく表示するための最低要件の詳細については，14 ページ「サポート・マトリックス」を参照してください。

Configuration Manager へのアクセスでセキュリティを確保する方法については，84 ページ「セキュリティの強化」を参照してください。

Configuration Manager へのアクセスに関するトラブルシューティング情報については，117 ページ「トラブルシューティング」を参照してください。

Configuration Manager へのログイン

1 Web ブラウザで Configuration Manager サーバの URLを入力します。たとえば，http://＜サーバ名または IP アドレス＞.＜ドメイン名＞:＜ポート＞/cncの形式の場合，**＜サーバ名または IP アドレス＞.＜ドメイン名＞**にはConfiguration Manager サーバの完全修飾ドメイン名（FQDN），**＜ポート＞**にはインストール中に選択したポートを指定します。

2 Configuration Manager Post Installation ウィザードで指定したユーザ名とパスワードを入力します。

3 ［**ログイン**］をクリックします。ログイン後，ユーザ名が画面の右上に表示されます。

4 （推奨）組織 LDAP サーバに接続し，管理者の役割を LDAP ユーザに割り当てます。これにより，Configuration Manager 管理者はシステムにアクセスできるようになります。Configuration Manager のユーザに役割を割り当てる方法につい  『HP Universal CMDB Configuration Manager ユーザーズ・ガイド』の"User Management"を参照してください。

ログアウト

セッションが完了したら，不正な侵入を防ぐため，Web サイトからログアウトします。

ログアウトするには，ページ上部の［**ログアウト**］をクリックします。

注：セッションの有効期限は，デフォルトで 30 分に設定されています。

JMX コンソールを使った Configuration Manager へのアクセス

トラブルシューティングや一部構成の変更では，JMX コンソールへのアクセスが必要になる場合があります。

JMX コンソールにアクセスするには，次の手順を実行します。

1 http://＜サーバ名または IP アドレス＞:＜ポート＞/cnc/jmx-console にアクセスし，JMX コンソールを開きます。ポートは，Configuration Manager のインストール時に設定したポートを指定してください。

2 デフォルトのユーザ資格情報を入力します。これは，Configuration Manager へのログイン時に使用するたユーザ資格情報と同じです。

第 5 章

その他の使用例

本章の内容

マシン間での Configuration Manager の移動

この手順では，データベース・スキーマの正常な動作と UCMDB サーバへの接続を維持しながら，マシン間で Configuration Manager を転送する場合に使用します。

1 **＜Configuration Manager インストール・ディレクトリ＞¥cnc¥bin** フォルダで，次のコマンドを実行します。edit-server-0.bat

2 ポート（例：JMX ポート）を含め，みつかったパラメータをすべて記録します。

3 ソース・マシンで Configuration Manager サーバを停止します（ソース・マシンのインストール先が Windows システムである場合は，Configuration Manager サービスを停止します）。

4 ターゲット・マシンに Configuration Manager をインストールします。

   ➤ Windows の場合：**setup-win64.msi** ファイル（インストール・メディアの **¥windows** フォルダ）を実行します。

   ➤ Linux の場合：40 ページ「Configuration Manager のインストール」の手順に従います。

5 Post Installation ウィザードが起動したらキャンセルします。

6 ソース・マシンの古いインストール・ディレクトリからターゲット・マシンの新しいインストール・ディレクトリに，すべてのファイルをコピーします。

7 ターゲット・マシンの **client-config.properties** および **resources.properties**（**¥conf** フォルダ）で，ホスト名をターゲット・マシン名に変更します。

注 : ターゲット・マシンとソース・マシンのドメインが異なる場合，**lwssofmconf.xml** で古いドメイン参照も変更します。

---

8 ターゲット・マシンで **bin/create-windows-service.bat** ファイルを実行し，Windows サービスを作成します。**-h** フラグを設定して使用可能なオプションを表示し，ソース・マシンのサービスについて記録したパラメータ（手順 2）を必要に応じて使用します。ドメイン名パラメータには server-0 を使用します。デフォルト値を使用すると，コマンドは次のようになります。

c:¥HP¥cnc920¥bin>create-windows-service.bat -j 39900 -n server-0 -r 39600

9 ターゲット・マシンで Configuration Manager サーバを起動します。

インストール後のポート番号の変更

1 Configuration Manager サーバを停止します。

2 **＜Configuration Manager インストール・ディレクトリ＞¥servers¥server-0** フォルダのコンテンツをバックアップします。

3 **＜Configuration Manager インストール先＞¥servers¥server-0** フォルダを削除します。

4 **create-node.bat** スクリプトに使用可能なオプションを表示するための **-h** フラグを付けて実行します。必要なポート番号をすべてユーティリティに渡します。

5 ターゲット・マシンの **client-config.properties** および **resources.properties**（**¥conf** フォルダ）で，ポートを新しい HTTP ポート番号に変更します。

6 **＜Configuration Manager インストール・ディレクトリ＞/bin** フォルダにある **edit-server-0.bat** スクリプトを開きます。

7 （Windows システムの場合）HP Universal CMDB Configuration Manager の［プロパティ］ウィンドウで［Java］タブをクリックし，**jmx.http.port** および **com.sun.management.jmxremote.port** を新しいポート番号に設定します。

8 ターゲット・マシンで Configuration Manager サービスを開始します。

システム間でのシステム設定のコピー

1 ソース・マシンで Configuration Manager を開きます。［**システム**］＞［**設定**］を選択し，［**構成セットを zip ファイルにエクスポート**］ボタンをクリックします。

エクスポートする前に，該当する構成項目の横のチェック・ボックスの選択を解除して，構成の特定の部分を除外できます。

2 エクスポートした構成をターゲット・マシンにコピーします。

3 ターゲット・マシンで Configuration Manager を開きます。［**システム**］＞［**設定**］を選択し，［**構成セットのインポート** ］ボタンをクリックします。

バックアップと復元

新たに完全なインストールを行わなくてもさまざまなタイプの障害から回復できるように，インストールした Configuration Manager をバックアップしておくことができます。

バックアップ

次の情報をバックアップします。

- Configuration Manager インストール・ディレクトリの **conf** および **security** サブフォルダ（バックアップはシステムの稼働中に行うことができ，運用は中断されません）
- データベース・スキーマ

復元（Windows システムの場合）

この手順は，Configuration Manager がインストールされていない新規のシステムで実行します。

1. ターゲット・マシンに Configuration Manager をインストールします。そのためには，次のように，**setup-win64.msi** ファイル（インストール・メディアの **¥windows** フォルダ）をサイレント・モードで実行します。

   ```
   msiexec /i setup-win64.msi TARGETDIR=path¥to¥install¥dir /passive
   ```

2. **conf** および **security** ディレクトリを復元します。バックアップに使用した方法に合った復元方法を使用します。手順 1 で行ったインストールで作成したディレクトリを上書きします。
3. データベース・スキーマを復元します。別のデータベース・サーバに復元する場合，**database.properties** ファイル（**conf** ディレクトリ）の **url** プロパティを変更して新しいデータベース・サーバ名に合わせます。
4. **create-windows-service** ユーティリティ（使用可能なオプションを表示するには **-h** フラグを使用）で Windows サービスを作成します。
5. Configuration Manager サーバを起動します。

復元（Linux システムの場合）

1 ターゲット・マシンに Configuration Manager をインストールします。そのためには，**setup.bin** ファイル（インストール・メディア）を実行します。詳細については，40 ページ「Configuration Manager のインストール」を参照してください。ただし，Post Installation ウィザードの最初の手順ではインストールをキャンセルしてください。ファイルはすべてデプロイされますが，システムは未構成になります。

2 **conf** および **security** ディレクトリを復元します。バックアップに使用した方法に合った復元方法を使用します。手順 1 で行ったインストールで作成したディレクトリに上書きします。

3 データベース・スキーマを復元します。別のデータベース・サーバに復元する場合，**database.properties** ファイル（**conf** ディレクトリ）の **url** プロパティを変更して新しいデータベース・サーバ名に合わせます。

4 Configuration Manager サーバを起動します。

第 6 章

詳細構成

本章の内容

詳細なデータベース接続オプション

データベースのデプロイメントで，さらに詳細なデータベース接続プロパティの設定が必要な場合は，Post Installation ウィザードの完了後にオプションを設定できます。Configuration Manager では，ベンダが提供する JDBC ドライバでサポートされるデータベース接続をすべて使用でき，データベース接続 URL を使った構成が可能です。詳細な接続オプションを構成するには，**＜Configuration Manager インストール・ディレクトリ＞¥conf¥database.properties** ファイルにある **jdbc.url** プロパティを編集します。

注：Linux システムで詳細構成を行う場合は，次の手順を実行します。

- 手順に記載されているパスの区切りの円記号をフォワード・スラッシュ（/）に変更します。
- スクリプト実行ファイルの **.bat** を **.sh** に置き換えます。

次に，Microsoft SQL Server での詳細オプションの設定例を示します。

- **Windows（NTLM）認証：**Windows 認証を適用するには，database.properties ファイルで JTDS 接続 URL にドメイン・プロパティを追加します。認証対象となる Windows ドメインを指定します。

  例：

  ```
  jdbc:jtds:sqlserver://myServer:1433/myDatabase;sendStringParametersAsUnicode
  =false;domain=myDomain
  ```

- **SSL：**SSL を使用した MS SQL Server 接続のセキュリティについては，http://jtds.sourceforge.net/faq.html（英語サイト）を参照してください。

次に，Oracle Database Server での詳細オプションの設定例を示します。

- **Oracle URL：**Oracle ネイティブ・ドライバの接続 URL を指定します。有効な Oracle サーバ名と SID を指定します。また，**Oracle RAC** を使用している場合には，Oracle RAC 構成情報を指定してください。

注：ネイティブの Oracle JDBC URL の形式については，http://www.orafaq.com/wiki/JDBC#Thin_driver（英語サイト）を参照してください。Oracle RAC の URL の設定については，http://download.oracle.com/docs/cd/B28359_01/java.111/e10788/rac.htm（英語サイト）を参照してください。

- **SSL :** SSL を使用した Oracle 接続のセキュリティについては，次を参照してください。
  - http://download.oracle.com/docs/cd/E11882_01/network.112/e10746/asojbdc.htm#ASOAG9604（英語サイト）
  - http://download.oracle.com/docs/cd/E11882_01/java.112/e16548/clntsec.htm#insertedID6（英語サイト）

データベース構成 - MLU（多言語ユニット）のサポート

ここでは，ローカライズのサポートに必要なデータベース設定を説明します。

Oracle Server の設定

次の表は，Oracle Server で必要な設定を示します。

オプション	サポートされる設定	推奨	備考
文字セット	WE8ISO8859P1，UTF8，AL32UTF8	AL32UTF8	

Microsoft SQL Server の設定

次の表は，Microsoft SQL Server で必要な設定を示します。

オプション	サポートされる設定	推奨	備考
照合順序	大文字と小文字を区別しない：HP Universal CMDBバイナリ並び替え順と大文字と小文字の区別はサポートされていません。大文字と小文字を区別しないアクセント，かな，文字幅を組み合わせた並び替え順のみがサポートされています。	照合順序は，［照合順序の設定］ダイアログ・ボックスで選択します。バイナリのチェック・ボックスは選択しないでください。アクセント，かな，文字幅の区別は，各データ言語の要件に従って選択します。OS Windows の地域設定の言語と同じ言語を選択してください。	［照合順序］のロケールと英語のデフォルト設定に限定。
照合順序 データベースのプロパティ	サーバのデフォルト		

注：

すべての言語共通：**＜言語＞_CI_AS** は，最低限必要なオプションです。
日本語で「かなを区別する」オプションと「文字幅を区別する」オプションを選択する場合には，**Japanese_CI_AS_KS_WS** または **Japanese_90_CI_AS_KS_WS** を推奨します。この設定は，日本語の文字はアクセントを区別，かなを区別，文字幅を区別することを示しています。

- **アクセントを区別する（_AS）**：アクセント付き文字とアクセントなし文字を区別します。たとえば，**a** と **á** は区別されます。このオプションを選択しないと，Microsoft SQL Server では，アクセント付きの文字とアクセントなしの文字がソートの時に同一とみなされます。
- **かなを区別する（_KS）**：日本語のひらがなとカタカナを区別します。このオプションを選択しないと，Microsoft SQL Server では，ひらがなとカタカナがソートの時に同一とみなされます。
- **文字幅を区別する（_WS）**：半角文字と全角文字を区別します。このオプションを選択しないと，Microsoft SQL Server では，半角文字と全角文字がソートの時に同一とみなされます。

シングル・サインオン（SSO）

Configuration Manager と UCMDB の間でのシングル・サインオンには，HP の LWSSO テクノロジを使用します。詳細については，113 ページ「Lightweight シングル・サインオン認証（LW-SSO）のリファレンス」を参照してください。

本項の内容

Configuration Manager と UCMDB の間での LW-SSO の有効化

Configuration Manager ユーザの中には，UCMDB へのログインが許可されているユーザがいます。Configuration Manager では，このようなユーザ向けに UCMDB に直接リンクできるユーザ・インタフェースが用意されています（[**管理**] > [**UCMDB ファウンデーション**] を選択）。シングル・サインオン（Configuration Manager へのログイン後，UCMDB へのログインを不要にする機能）を使用するには，Configuration Manager と UCMDB の両方で LW-SSO を有効にし，同じ initString を使用するように設定します。Deployment Manager のインストールで実行済みの場合を除き，このタスクは手動で実行してください。

LW-SSO を有効にするには，次の手順を実行します。

1 Configuration Manager のインストール・ディレクトリで，**¥conf¥lwssofmconf.xml** ファイルを編集します。

2 次のセクションを探します。

```
enableLWSSO enableLWSSOFramework="true"
```

値が「**true**」に設定されていることを確認します。

3 次のセクションを探します。

```
lwssoValidation  id="ID000001">
<domain> </domain>
```

<domain> の後に，Configuration Manager サーバ・ドメインを入力します。

4 次のセクションを探します。

<initString="**この文字列を置換**"></crypto>

"この文字列を置換" の部分を，LW-SSO で統合するすべての信頼済みアプリケーションが共有する文字列に置き換えます。

5 次のセクションを探します。

<!--multiDomain>
<trustedHosts>
<DNSDomain>**アプリケーション・ドメインで置換**</DNSDomain>
<DNSDomain>**他のアプリケーションのドメインで置換**</DNSDomain>
</trustedHosts>
</multiDomain-->

注：2 番目の DNSDomain は，Configuration Manager と別のアプリケーションのドメインが異なる場合のみ指定します。

DNSDomain 要素では，（必要に応じて）冒頭のコメント文字を削除し，すべてのサーバ・ドメインを入力します（「**アプリケーション・ドメインで置換**」または「**他のアプリケーションのドメインで置換**」）。70 ページの手順 3 で入力したサーバ・ドメインを指定してください。

6 変更したファイルを保存し，サーバを再起動します。

7 Web ブラウザを起動し，アドレスに
http://＜UCMDB **サーバ・アドレス**＞.＜**ドメイン名**＞:8080/jmx-console と入力します。

JMX コンソールの認証資格情報を入力します。デフォルトは次のとおりです。

- ログイン名 = **sysadmin**
- パスワード = **sysadmin**

8 ［**UCMDB-UI**］の下にある［**LW-SSO Configuration**］をクリックすると，［JMX MBEAN View］ページが開きます。

9 ［**setEnabledForUI**］メソッドを選択し，値を「**True**」に指定して，［**Invoke**］をクリックします。

10 ［**setDomain**］メソッドを選択します。UCMDB サーバのドメイン名を入力し，［**Invoke**］をクリックします。

11 ［**setInitString**］メソッドを選択します。71 ページの手順 4 で，Configuration Manager で指定した initString を入力し，［**Invoke**］をクリックします。

12 Configuration Manager と UCMDB が別のドメインにある場合は，［**addTrustedDomains**］メソッドを選択し，UCMDB と Configuration Manager の各サーバのドメイン名を入力します。［**Invoke**］をクリックします。

13 設定メカニズムで保存されている LW-SSO 構成をそのまま表示するには，［**retrieveConfigurationFromSettings**］メソッドを選択して［**Invoke**］をクリックします。

14 実際に読み込まれた LW-SSO 構成を表示するには，［**retrieveConfiguration**］メソッドを選択して［**Invoke**］をクリックします。

Operations Orchestration での LW-SSO の構成

LW-SSO が Configuration Manager と Operations Orchestration（OO）の両方で有効になっている場合，Configuration Manager にログインしているユーザは，（システム管理者の）ユーザ名とパスワードを入力しなくても Web 階層を通じて Operations Orchestration にサインオンできます。

注：

- 次の手順で，＜OO ホーム＞は Operations Orchestration のホーム・ディレクトリを表しています。
- LW-SSO では，Operations Orchestration および Configuration Manager にログインするために使用するアカウント名が同じである必要があります（パスワードは異なっていてもかまいません）。
- LW-SSO では，Operations Orchestration のアカウントが内部アカウント以外である必要があります。

Operations Orchestration で LW-SSO を構成するには，次の手順を実行します。

1 RSCentral サービスを停止します。

2 次のように，**＜OO ホーム＞¥Central¥WEB-INF¥applicationContext.xml** で，LWSSO_SECTION_BEGIN と LWSSO_SECTION_END の間でインポートを有効にします。

```
<!--  LWSSO_SECTION_BEGIN-->
        <import resource="CentralLWSSOBeans.xml"/>
<!--  LWSSO_SECTION_END -->
```

3 次のように，**＜OO ホーム＞¥Central¥WEB-INF¥web.xml** で，LWSSO_SECTION_BEGIN と LWSSO_SECTION_END の間ですべてのフィルタとマッピングを有効にします。

```
<!--  LWSSO_SECTION_BEGIN-->

<filter>
        <filter-name>LWSSO</filter-name>
        <filter-
    class>com.iconclude.dharma.commons.util.http.DharmaFilterToBeanProx
    y
        </filter-class>
        <init-param>
            <param-name>targetBean</param-name>
            <param-value>dharma.LWSSOFilter</param-value>
        </init-param>
   ......
   </filter>
<!--  LWSSO_SECTION_END -->

<!--  LWSSO_SECTION_BEGIN-->
   <filter-mapping>
      <filter-name>LWSSO</filter-name><url-pattern>/*</url-pattern>
   </filter-mapping>
<!--  LWSSO_SECTION_END -->

<!--  LWSSO_SECTION_BEGIN-->
    <filter-mapping>
          <filter-name>LWSSO2Acegi</filter-name><url-pattern>/*</url-pattern>
    </filter-mapping>
    <filter-mapping>
          <filter-name>dharmaLWSSOGroupsFilter</filter-name><url-
    pattern>/*</url-pattern>
          </filter-mapping>
<!--  LWSSO_SECTION_END -->
```

4 **＜OO ホーム＞¥Central¥conf¥lwssofmconf.xml** で，次の 2 つのパラメータを編集します。

- domain：OO サーバのドメイン名
- initString：OO LW-SSO 構成の initString 値と同じ（最小長：12 文字。例：smintegrationlwsso）

例：

```
<webui>
<validation>
      <in-ui-lwsso>
       <lwssoValidation  id="ID000001">
            <domain>asia.hpqc.net</domain>
            <crypto cipherType="symmetricBlockCipher"
                                    engineName="AES" paddingModeName="CBC"
keySize="256"  encodingMode="Base64Url"
                                    initString=" smintlwsso "></crypto>
       </lwssoValidation>
      </in-ui-lwsso>
</validation>
<creation>
       <lwssoCreationRef id="ID000002">
            <lwssoValidationRef refid="ID000001"/>
            <expirationPeriod>600000</expirationPeriod>
       </lwssoCreationRef>
</creation>
</webui>
```

5 構成を反映するため，RSCentral サービスを再起動します。

ID マネージャの認証の実行

このタスクでは，ID マネージャによる認証を受け付けるように，HP Universal CMDB Configuration Manager を構成する方法を説明します。

ID マネージャを使用している環境に HP Universal CMDB Configuration Manager を追加する場合は，このタスクを実行する必要があります。

このタスクでは，次の手順を行います。

➤ 75 ページ「前提条件」

➤ 75 ページ「ID マネージャを使用するための HP Universal CMDB Configuration Manager の設定」

前提条件

Configuration Manager Tomcat サーバは，ID マネージャで保護されている Web サーバ（IIS または Apache）に Tomcat Java（AJP13）コネクタで接続します。

Tomcat Java（AJP13）コネクタの使用方法については，Tomcat Java（AJP13）のマニュアルを参照してください。

ID マネージャを使用するための HP Universal CMDB Configuration Manager の設定

Tomcat Java（AJP13）と IIS6 を連携する構成を行うために，次の手順を実行します。

1 ユーザ名を含むカスタマイズ・ヘッダ/コールバックを送信する設定を ID マネージャで行い，ヘッダ名を要求します。

2 **＜Configuration Manager インストール・ディレクトリ＞¥conf¥lwssofmconf.xml** ファイルを開き，**in-ui-identity-management** で始まるセクションを探します。

例：

```
<in-ui-identity-management enabled="false">
  <identity-management>
 <userNameHeaderName>sm-user</userNameHeaderName>
  </identity-management>
</in-ui-identity-management>
```

a コメント文字を削除して，機能をアクティブにします。

b **enabled="false"** を **enabled="true"** に変更します。

c **sm-user** を，手順 1 で要求したヘッダ名に変更します。

3 **＜Configuration Manager インストール・ディレクトリ＞¥conf¥client-config.properties** ファイルを開き，次のプロパティを編集します。

   a **bsf.server.url** を ID マネージャの URL に変更し，ポートを ID マネージャのポートに変更します。

      bsf.server.url=http://＜ID マネージャの URL＞:＜ID マネージャのポート＞/bsf

   b **bsf.server.services.url** を HTTP プロトコルに変更し，ポートを元の Configuration Manager ポートに変更します。

      bsf.server.services.url=http://＜Configuration Manager URL＞:
      ＜Configuration Manager ポート＞/bsf

Configuration Manager 向けの ID マネージャ構成で Java コネクタを使用する例（Windows 2003 オペレーティング・システムで IIS6 を使用）

この例では，Windows 2003 オペレーティング・システムで IIS6 を稼働する環境において，Configuration Manager 用の ID マネージャ構成で使用するJava コネクタをインストールして構成する方法を説明します。

Java コネクタをインストールし，Windows 2003 環境の IIS6 向けに構成するために，次の手順を実行します。

1 Java コネクタの最新バージョン（**djk-1.2.21** など）を Apache Web サイトからダウンロードします。

   a http://www.apache.org/dist/tomcat/tomcat-connectors/jk/binaries/win64/ をクリックします。

   b 最新バージョンを選択します。

   c **isapi_redirect.dll** ファイルを **amd64** ディレクトリからダウンロードします。

2 このファイルを**＜Configuration Manager インストール・ディレクトリ＞¥tomcat¥bin¥win32** に保存します。

3 isapi_redirect.dll と同じディレクトリに，**isapi_redirect.properties** という名前で新しいテキスト・ファイルを作成します。

このファイルの内容は次のとおりです。

```
# Jakarta ISAPI Redirector 用の構成ファイル
# ISAPI Redirector Extension へのパス（Web サイトに対する相対パス）
# このファイルは，仮想ディレクトリ（実行権限付き）に格納
extension_uri=/jakarta/isapi_redirect.dll
# ISAPI Redirector のログ・ファイルへの完全パス
log_file=<Configuration Manager installation directory>¥servers
¥server-0¥logs¥isapi.log
# ログ・レベル（debug，info，warn，error，trace）
log_level=info
# workers.properties ファイルへの完全パス
worker_file==＜Configuration Manager インストール・ディレクトリ＞¥tomcat
¥conf¥workers.properties.minimal
# uriworkermap.properties ファイルへの完全パス
worker_mount_file==＜Configuration Manager インストール・ディレクトリ＞¥tomcat
¥conf¥uriworkermap.properties
```

4 **＜Configuration Manager インストール・ディレクトリ＞¥tomcat¥conf** に **workers.properties.minimal** という名前のテキスト・ファイルを新しく作成します。

このファイルの内容は次のとおりです。

```
# workers.properties.minimal -
#
# このファイルには最小限の jk 構成プロパティを記載
# （Tomcat への接続に
# 必要なプロパティ）
#
# 名前が ajp13w，タイプが ajp13 のワーカを定義
# 名前とタイプは必ずしも
# 一致しない点に注意
    worker.list=ajp13w
    worker.ajp13w.type=ajp13
    worker.ajp13w.host=localhost
    worker.ajp13w.port=8009
#END
```

5 **＜Configuration Manager インストール・ディレクトリ＞¥tomcat¥conf** に **uriworkermap.properties** という名前のテキスト・ファイルを新しく作成します。

このファイルの内容は次のとおりです。

```
# uriworkermap.properties - IIS
#
# このファイルにはサンプル・マッピングを記載。例：
# ajp13w ワーカ，workermap.properties.minimal で定義
# このファイルの一般的な構文：
# [URL]=[ワーカ名]
/cnc=ajp13w
/cnc/*=ajp13w
/bsf=ajp13w
/bsf/*=ajp13w
#END
```

重要：Configuration Manager にはルールが 2 つ必要です。新しい構文では，この 2 つを 1 つに統合できます。

/cnc|/*=ajp13w

---

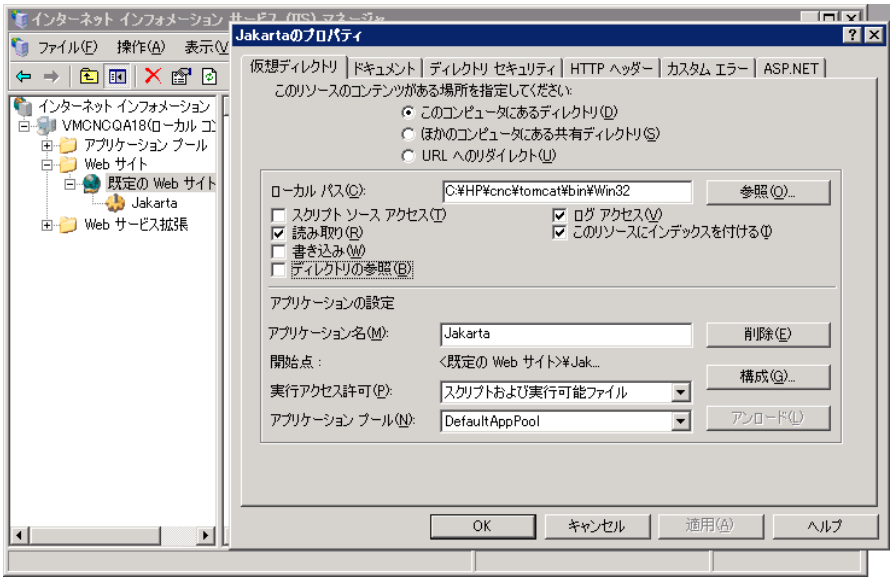
6 IIS 構成で，Web サイト・オブジェクトに仮想ディレクトリを作成します。

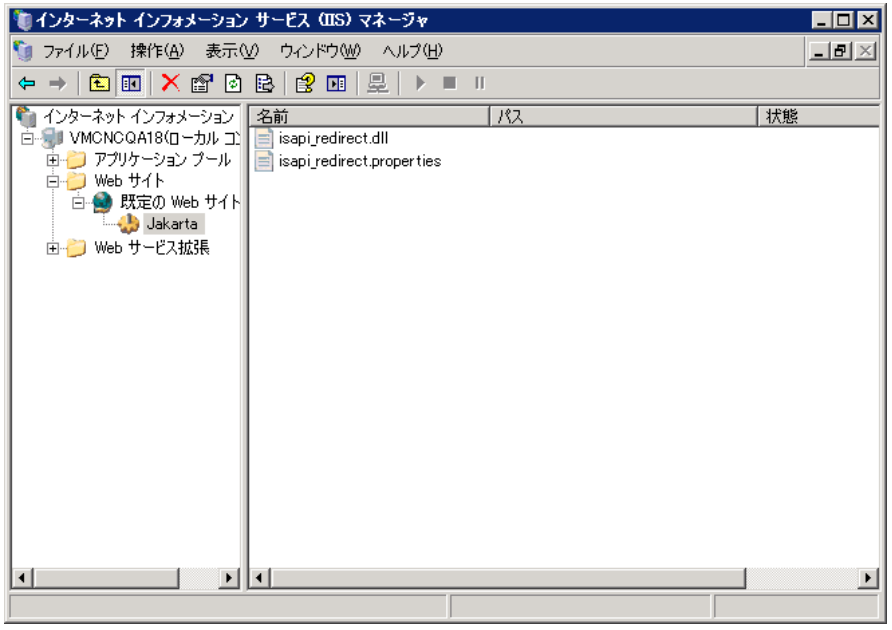
a Windows の［スタート］メニューで，［**設定**］＞［**コントロール パネル**］＞［**管理ツール**］＞［**インターネット インフォメーション サービス (IIS) マネージャ**］を開きます。

b 右の表示枠で，**＜ローカル・コンピュータ名＞¥Web サイト¥＜Web サイト名＞**を右クリックして，［**新規作成**］＞［**仮想ディレクトリ**］をクリックします。

c ディレクトリのエイリアス名を「**Jakarta**」と指定し，ローカル・パスには isapi_redirect.dll を含むディレクトリを指定します。

次に，IIS マネージャのウィンドウの例を示します。





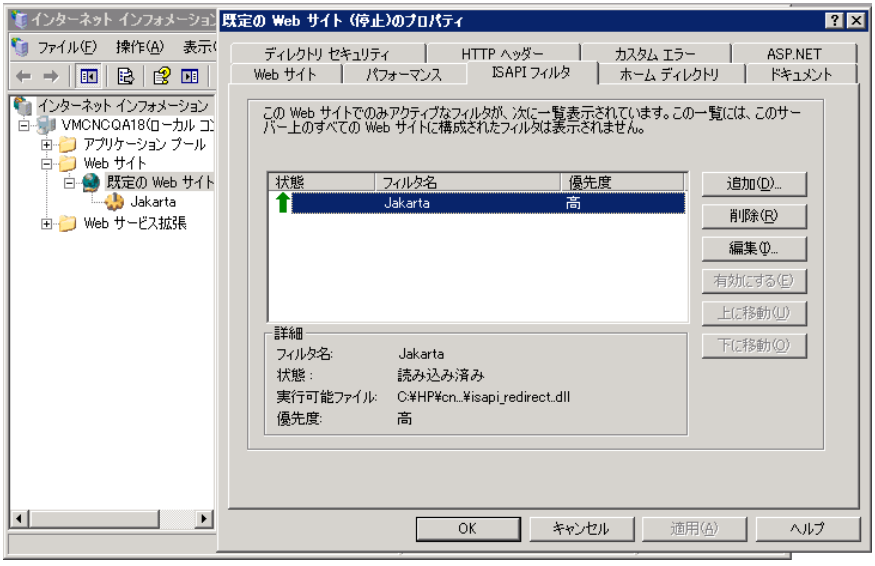
7 ISAPI フィルタに **isapi_redirect.dll** を追加します。

a **<Web サイト名>**を右クリックして［**プロパティ**］を選択します。

b ［**ISAPI フィルタ**］タブを選択し，［**追加**］ボタンをクリックします。

c ［フィルタ名］に「**Jakarta**」と入力し，［参照］をクリックして **isapi_redirect.dll** ファイルを指定します。これでフィルタが追加されますが，まだアクティブな状態ではありません。

次のような画面が表示されます。



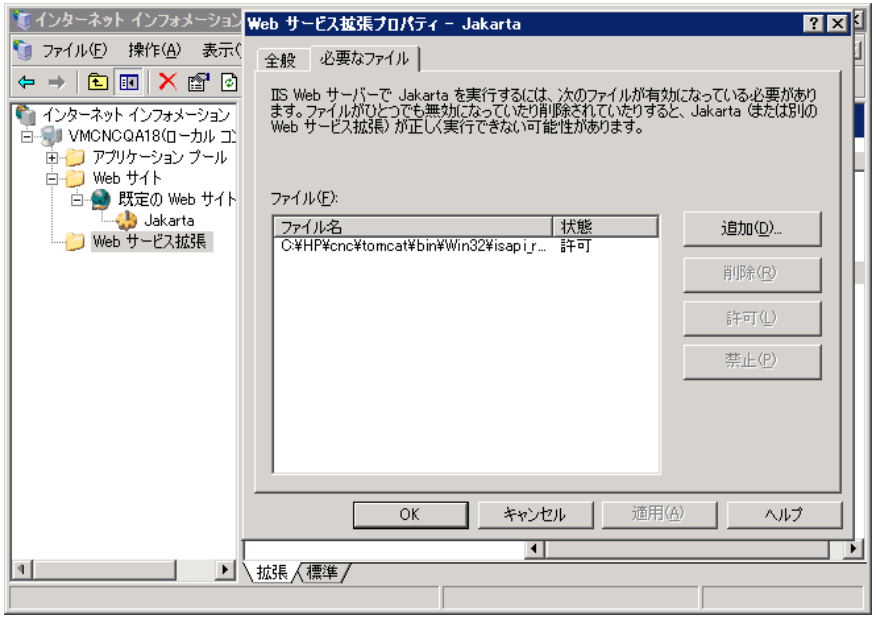
d ［**適用**］ボタンをクリックします。

8 新しい Web サービス拡張を定義し，許可します。

a **<ローカル・コンピュータ名>¥Web サービス拡張**を右クリックし，［**新しい Web サービス拡張の追加**］メニュー項目を選択します。

b 新しい Web サービス拡張の名前に「**Jakarta**」と入力し，［参照］をクリックして **isapi_redirect.dll** ファイルを指定します。

注:［**拡張の状態を許可済みに設定する**］チェック・ボックスを選択してから，［**OK**］ボタンをクリックします。



9 IIS Web サーバを再起動し，Web サービス経由でアプリケーションにアクセスします。

IPv6 のサポート

Configuration Manager は，顧客向け URL のみで IPv6 URL をサポートします。

Configuration Manager で IPv6 アドレスを使用するには，次の手順を実行します。

1 使用中のオペレーティング・システムが IPv6 と IPv4 の両方をサポートしていることを確認します。詳細については，オペレーティング・システムのマニュアルを参照してください。

2 **＜Configuration Manager インストール・ディレクトリ＞/conf** フォルダにある **client-config.properties** ファイルを開き，次の値を編集します。

➤ 次のように，**bsf.server.url** パラメータの値を変更し，ホスト名を使用するようにします。

bsf.server.url=http://mycomputer:8080/bsf

➤ 次のように, **bsf.server.services.url** パラメータの値を変更し, Configuration Manager の URL がホスト名のアドレスになるようにします。

bsf.server.services.url=http://＜Configuration Manager のホスト名＞:
＜Configuration Manager のポート＞/bsf

3 Tomcat の **servers¥server-0¥conf¥server.xml** ファイルを開き，次の値を編集します。

➤ 次のタグに **address="[::]"** を追加することで，SHUTDOWN フックに IPv6 アドレスを追加します。

<Server port="8005" shutdown="SHUTDOWN" **address="[::]"** >

➤ HTTP コネクタをもう一つ追加します。2 番目のコネクタでは，次のように IPv6 [::] アドレスを追加します。

```
<Connector port="8180" protocol="HTTP/1.1"
        connectionTimeout="20000"
        redirectPort="8443" />
<Connector port="8180" protocol="HTTP/1.1" address="[::]"
        connectionTimeout="20000"
        redirectPort="8443" />
```

➤ AJP コネクタをもう一つ追加します。2 番目のコネクタでは，次のように IPv6 [::] アドレスを追加します。

```
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443"  address="[::]" />
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
```

4 サーバに環境変数 useIPv6="true" を追加します。

＜Configuration Manager インストール・ディレクトリ＞/bin フォルダにある **edit_server-0.bat** ファイルを開きます。［Java（Java）］タブで，Java オプションに -DuseIPv6 プロパティを追加します。

5 サーバを再起動します。

LDAP

Configuration Manager 内で LDAP を構成できます。詳細については,『HP Universal CMDB Configuration Manager ユーザーズ・ガイド』の"System Settings"を参照してください。

セキュリティの強化

本項の内容

注 : アップグレード後，SSL の構成を再度行う必要があります。詳細については，37 ページ「Configuration Manager のアップグレード」を参照してください。

Configuration Manager のセキュリティの強化

ここでは，Configuration Manager アプリケーションのセキュリティ保護の概念を紹介し，セキュリティを実装するために必要な計画とアーキテクチャについて説明します。以下の内容を読んでから，セキュリティ強化について説明する後の項に進むことを強くお勧めします。

Configuration Manager は，セキュリティ保護アーキテクチャの一部として使用できるように設計されているので，セキュリティ上の脅威に対処できる機能が用意されています。

セキュリティ強化のガイドラインでは，Configuration Manager のセキュリティ強化に必要な設定作業について取り上げます。

ここで紹介する内容は主に Configuration Manager 管理者を対象としています。セキュリティ強化の作業を開始する前に，セキュリティを強化するための設定や推奨事項について理解するための参考として活用してください。

システムのセキュリティ強化の準備として，次の作業をお勧めします。

- ネットワーク全体でセキュリティ上のリスクやセキュリティの状態を評価し，評価結果に基づいて Configuration Manager をネットワークに統合する最適な方法を検討します。
- Configuration Manager の技術フレームワークと Configuration Manager のセキュリティ機能についてよく理解します。
- セキュリティ強化ガイドラインのすべての内容を検討します。
- Configuration Manager が完全に機能していることを確認してから，セキュリティ強化手順を開始します。
- セキュリティ強化手順は，各項に記載されている順序で実施してください。

重要：

- ここで紹介するセキュリティ強化の手順は，記載内容のみを実施することを前提とするものであり，他で記述されているセキュリティ強化の実施は想定されていません。
- セキュリティ強化手順は特定の分散アーキテクチャを対象としていますが，そのアーキテクチャがユーザ固有の組織のニーズに最適なアーキテクチャであるとは限りません。
- ここで記載する手順は，Configuration Manager 専用のマシンで実行することを想定しています。Configuration Manager 以外の用途にも使用するマシンで実行すると，問題が発生することがあります。
- ここで紹介するセキュリティ強化に関する情報は，ご利用のコンピュータ・システムのセキュリティ・リスクを評価するためのガイドラインではありません。

データベース・パスワードの暗号化

データベース・パスワードは，**＜Configuration Manager インストール・ディレクトリ＞¥conf¥database.properties** ファイルに格納されます。パスワードを暗号化する場合は，FIPS 140-2 標準に準拠した暗号化アルゴリズムがデフォルトで用意されています。

暗号化の処理としては，まずパスワードがキーを使って暗号化されます。次に，キー自体がマスタ・キーを使って暗号化されます。両方のキーとも同じアルゴリズムを使って暗号化されます。暗号化で使用するパラメータの詳細については，87 ページ「暗号化パラメータ」を参照してください。

注意：暗号化アルゴリズムを変更すると，それまでに暗号化したパスワードはすべて使用できなくなります。

データベース・パスワードの暗号化の設定を変更するには，次の手順を実行します。

1 **＜Configuration Manager インストール・ディレクトリ＞¥conf¥encryption.properties** ファイルを開いて次のフィールドを編集します。

   ➤ **engineName：**暗号化アルゴリズムの名前を入力します。

   ➤ **keySize：**選択したアルゴリズムのマスタ・キーのサイズを入力します。

2 **generate-keys.bat** スクリプトを実行します。これにより，**cnc920¥security¥encrypt_repository** ディレクトリが作成され，暗号化キーが生成されます。

3 **bin¥encrypt-password** ユーティリティを実行してパスワードを暗号化します。**-h** フラグを設定し，使用可能なオプションを表示します。

4 パスワード暗号化ユーティリティの結果をコピーし，**conf¥database.properties** ファイルに貼り付けます。

暗号化パラメータ

次の表は，データベース・パスワードの暗号化で使用するパラメータの一覧です。このパラメータは，**encryption.properties** ファイルで定義されます。データベース・パスワードの暗号化の詳細については，86 ページ「データベース・パスワードの暗号化」を参照してください。

パラメータ	説明
cryptoSource	暗号化アルゴリズムを実装するインフラストラクチャを示します。次のオプションを選択できます。 ➤ **lw :** Bouncy Castle（軽量暗号化パッケージ，デフォルト・オプション） ➤ **jce :** Java 暗号化拡張機能（標準の Java 暗号化インフラストラクチャ）
storageType	キーストアのタイプを示します。 現在サポートされているのは，**binary file** のみです。
binaryFileStorageName	ファイル内でマスタ・キーが格納されている場所を示します。
cipherType	暗号のタイプ。現在サポートされているのは，**symmetricBlockCipher** のみです。
engineName	暗号化アルゴリズムの名前。 次のオプションを選択できます。 ➤ **AES :** American Encryption Standard の略。この暗号化方式は FIPS 140-2 に準拠しています（デフォルト・オプション） ➤ **Blowfish** ➤ **DES** ➤ **3DES :**（FIPS 140-2 準拠） ➤ **Null**：暗号化なし
keySize	マスタ・キーのサイズ。このサイズは，アルゴリズムによって異なります。 ➤ **AES :** 128，192，256 のいずれか（デフォルトは 256） ➤ **Blowfish :** 0-400 ➤ **DES :** 56 ➤ **3DES :** 156

パラメータ	説明
encodingMode	暗号化された文字列（バイナリ）の ASCII エンコーディング。 次のオプションを選択できます。 ➤ **Base64**（デフォルト・オプション） ➤ **Base64Url** ➤ **Hex**
algorithmModeName	アルゴリズムのモード。現在サポートされているのは，**CBC** のみです。
algorithmPaddingName	使用するパディング・アルゴリズム。 次のオプションを選択できます。 ➤ **PKCS7Padding**（デフォルト・オプション） ➤ **PKCS5Padding**
jceProviderName	JCE 暗号化アルゴリズムの名前。 **注：**指定できるのは，crytpSource が **jce** の場合のみです。**lw** の場合は engineName が使用されます。

自己署名証明書を使用したサーバ・マシンでの SSL の有効化

ここでは，Secure Sockets Layer（SSL）チャネルを使用した認証および暗号化をサポートする設定を Configuration Manager で行う方法について説明します。

Configuration Manager は，Tomcat 7.0 をアプリケーション・サーバとして使用します。

注：すべてのディレクトリとファイルの場所は，プラットフォーム，OS，インストール設定によって異なります。

---

1 前提条件

次に示す手順を始める前に，**＜Configuration Manager インストール・ディレクトリ＞¥java¥lib¥security¥tomcat.keystore** にある古い **tomcat.keystore** ファイルを削除してください。

2 サーバ・キーストアの生成

自己署名証明書と秘密鍵を使用してキーストア （JKS タイプ）を作成します。

➤ Java をインストールした ＜Configuration Manager インストール・ディレクトリ＞ の bin ディレクトリで，次のコマンドを実行します。

```
keytool -genkey -alias tomcat -keyalg RSA -keystore ..¥lib¥
security¥tomcat.keystore
```

コンソール・ダイアログ・ボックスが開きます。

➤ キーストアのパスワードを入力します。パスワードを変更した場合は，ファイル内のパスワードを手作業で変更します。

➤「**What is your first and last name?**」という質問に回答します。Configuration Manager の Web サーバ名を入力します。組織での指定に基づいて，他のパラメータを入力します。

➤ キーのパスワードを入力します。キーのパスワードには，キーストアのパスワードと同じものを入力してください。

tomcat.keystore という名前の JKS キーストアが作成され，**hpcert** という名前のサーバ証明書が格納されます。

3 クライアントの信頼されたストアに証明書を配置

コンピュータの Internet Explorer で，クライアントの信頼されたストアに証明書を追加します（［**ツール**］＞［**インターネット オプション**］＞［**コンテンツ**］＞［**証明書**］）。ここで追加しないと，Configuration Manager を初めて使用しようとするときに追加が求められます。

クライアント証明書の詳細については，95 ページ「クライアント証明書」を参照してください。

制限事項：**tomcat.keystore** にはサーバ証明書が 1 つしかない場合があります。

---

4 クライアント構成の確認

＜Configuration Manager インストール・ディレクトリ＞の **conf** ディレクトリにある **client-config.properties** ファイルを開きます。**bsf.server.url** のプロトコルを **https** に，ポートを **8443** に設定します。

5 server.xml ファイルの変更

＜Configuration Manager インストール・ディレクトリ＞¥servers¥server-0¥conf にある **server.xml** ファイルを開きます。次の文字列で始まるセクションに移動します。

Connector port="8443"

この部分はコメントになっているので，コメント文字を削除してスクリプトをアクティブにしてから，HTTPS コネクタに次の属性を追加します。

keystoreFile="＜tomcat.keystore ファイルの格納場所＞"（89 ページの手順 2 を参照してください）
keystorePass="＜パスワード＞"

次の行をコメントアウトします。

<Listener className="org.apache.catalina.core.AprLifecycleListener"
SSLEngine="on" />

6 サーバの再起動

7 サーバ・セキュリティの確認

Configuration Manager サーバのセキュリティを確認するには，Web ブラウザで次の URL を入力します。**https://＜Configuration Manager サーバ名または IP アドレス＞:8443/cnc**

ヒント : 接続を確立できない場合は，他のブラウザを使用するか，ブラウザを新しいバージョンにアップグレードしてください。

認証局から取得した証明書を使用したサーバ・マシンでの SSL の有効化

認証局（CA）が発行した証明書を使用するには，Java 形式のキーストアが必要です。ここでは，例を使って Windows マシンでキーストアの形式を指定する方法を説明します。

1 前提条件

次に示す手順を始める前に，**＜Configuration Manager インストール・ディレクトリ＞¥java¥lib¥security¥tomcat.keystore** にある古い **tomcat.keystore** ファイルを削除してください。

2 サーバ・キーストアの生成

a 認証局の署名入り証明書を生成し，Windows にインストールします。

b Microsoft 管理コンソール（**mmc.exe**）を使用して，証明書を ***.pfx** ファイルにエクスポートします（秘密鍵を含む）。

➤ **pfx** ファイルのパスワードとして使用する文字列を入力します（キーストアのタイプを JAVA キーストアに変換するとき，このパスワードを入力する必要があります）。
これで，**.pfx** ファイルには公開証明書と秘密鍵が格納され，パスワードで保護された状態になります。

c 作成した **.pfx** ファイルを**＜Configuration Manager インストール・ディレクトリ＞¥java¥lib¥security** フォルダにコピーします。

d コマンド・プロンプトを開き，**＜Configuration Manager インストール・ディレクトリ＞¥bin¥jre¥bin** に移動します。

➤ 次のコマンドを実行し，キーストアのタイプを **PKCS12** から **JAVA** に変更します。

```
keytool -importkeystore -srckeystore ＜Configuration Manager インストール・ディレクトリ＞¥conf¥security¥＜pfx ファイル名＞ -srcstoretype PKCS12 -destkeystore tomcat.keystore
```

変換元（**.pfx**）のキーストアのパスワードを入力するプロンプトが表示されます。手順 b で pfx ファイルを作成したときに指定したパスワードを入力してください。

3 クライアント構成の確認

＜Configuration Manager インストール・ディレクトリ＞¥cnc¥conf¥client-config.properties ファイルを開き，**bsf.server.url** プロパティが **https** に，ポートが **8443** に設定されていることを確認します。

4 server.xml ファイルの変更

＜Configuration Manager インストール･ディレクトリ＞¥servers¥server-0¥conf にある **server.xml** ファイルを開きます。次の文字列で始まるセクションに移動します。

Connector port="8443"

この部分はコメントになっているので，コメント文字を削除してスクリプトをアクティブにしてから，次の 2 行を追加します。

keystoreFile="../../java/lib/security/tomcat.keystore"
keystorePass="password" />

次の行をコメントアウトします。

<Listener className="org.apache.catalina.core.AprLifecycleListener"
SSLEngine="on" />

5 サーバの再起動

6 サーバ・セキュリティの確認

Configuration Manager サーバのセキュリティを確認するには，Web ブラウザで次の URL を入力します。**https://＜Configuration Manager サーバ名または IP アドレス＞:8443/cnc**

制限事項：**tomcat.keystore** にはサーバ証明書が 1 つしかない場合があります。

注 : すべてのディレクトリとファイルの場所は，プラットフォーム，オペレーティング・システム，インストール設定によって異なります。

例 : java/{os name}/lib

クライアント証明書を使った SSL の有効化

Configuration Manager Web サーバが使用している証明書がよく知られた認証局 （CA）によって発行されたものである場合，特別な設定を行わなくても Web ブラウザで証明書を検証できる可能性が高くなります。

CA がサーバの信頼ストアによって信頼されていない場合は，CA 証明書をサーバの信頼ストアにインポートする必要があります。

ここでは，自己署名の **hpcert** 証明書をサーバの信頼ストア（cacerts）にインポートする方法を，例を使って説明します。

サーバの信頼ストアに証明書をインポートするには，次の手順を実行します。

1 クライアント・マシンで，**hpcert** 証明書を検索し，名前を **hpcert.cer** に変更します。

2 **hpcert.cer** をサーバ・マシンの **＜Configuration Manager インストール・ディレクトリ＞¥java¥bin** フォルダにコピーします。

3 次のコマンドを実行し，サーバ・マシン上で keytool ユーティリティを実行し，CA 証明書を信頼ストア（cacerts）にインポートします。

＜Configuration Manager インストール・ディレクトリ＞¥java¥bin¥keytool.exe -import -alias hp -file hpcert.cer -keystore ..¥lib¥security¥cacerts

4 **server.xml** ファイル（**＜Configuration Manager インストール・ディレクトリ＞¥servers¥server-0¥conf** フォルダ）を次のように変更します。

a 90 ページの手順 5 に従って変更を行います。

b これらの変更を行った後，HTTPS コネクタに次の属性を追加します。

```
truststoreFile="../../java/lib/security/cacerts"
truststorePass="changeit" />
```

c clientAuth="true" を設定します。

5 90 ページの手順 7 に従って，サーバ・セキュリティを確認します。

認証のみで SSL を有効化

このタスクでは，認証のみをサポートするように Configuration Manager を設定する方法を説明します。Configuration Manager を使用するには，このレベルのセキュリティが最低限必要になります。

1 88 ページ「自己署名証明書を使用したサーバ・マシンでの SSL の有効化」から90 ページの手順 6までの手順，または91 ページ「認証局から取得した証明書を使用したサーバ・マシンでの SSL の有効化」から92 ページの手順 5までの手順に従って，サーバ・マシン上で SSL を有効化します。

2 Web ブラウザで次の URL を入力します。http://＜Configuration Manager サーバ名または IP アドレス＞:8180/cnc

クライアント証明書の認証を有効化

このタスクでは，クライアント側の証明書を認証するために Configuration Manager を設定する方法を説明します。

1 88 ページ「自己署名証明書を使用したサーバ・マシンでの SSL の有効化」の手順に従って，サーバ・マシン上で SSL を有効にします。

2 **＜Configuration Manager インストール・ディレクトリ＞¥conf¥lwssofmconf.xml** ファイルを開き，in-client certificate で始まるセクションを探します。次に例を示します。

```
<in-clientCertificate userIdentifierRetrieveField="SubjectDN"
userIdentifierRetrieveMode="FieldPart" userIdentifierRetrieveFieldPart="e" />
```

コメント文字を削除して，クライアント証明書機能をアクティブにします。

3 次の手順で，証明書からユーザ名を特定します。

a **userIdentifierRetrieveField** パラメータは，証明書のどのフィールドにユーザ名が格納されているかを示します。次のオプションを選択できます。

- **SubjectDN**
- **SubjectAlternativeName**

b **userIdentifierRetrieveMode** パラメータは，フィールドに格納されている内容全体がユーザ名か，一部としてユーザ名が含まれているのかを示します。次のオプションを選択できます。

- **EntireField**
- **FieldPart**

c **userIdentifierRetrieveMode** の値が **FieldPart** の場合，**userIdentifierRetrieveFieldPart** パラメータは，フィールドのどの部分がユーザ名なのかを示します。この値は，証明書内で定義されている凡例に基づくコード文字です。

4 **＜Configuration Manager インストール・ディレクトリ＞¥conf¥client-config.properties** ファイルを開いて次のプロパティを編集します。

- **bsf.server.url** を変更します。88 ページ「自己署名証明書を使用したサーバ・マシンでの SSL の有効化」の手順に従って，HTTPS プロトコルの使用と HTTPS ポートを設定してください。
- **bsf.server.services.url** を変更します。HTTP プロトコルの使用とオリジナルの HTTP ポートを設定してください。

クライアント証明書

本項の内容

クライアント証明書情報

本項では，クライアント証明書情報と，クライアント証明書からユーザ ID を取得する方法を説明します。

➤ ユーザ ID

ユーザ ID はクライアント証明書独自の部分であり，ユーザの身元を特定するために使用されます。

➤ 基本的なクライアント証明書情報

基本的なクライアント証明書情報には，次のものがあります。

証明書のフィールド	説明
Version	エンコードされた証明書のバージョン。 例：1 (0x1)
Serial Number	認証局が各証明書に割り当てた正の整数。 例：0 (0x0)
Signature Algorithm	認証局が証明書への署名に使用するアルゴリズムのアルゴリズム識別子。 例：md5WithRSAEncryption
Issuer	証明書に署名して発行したエンティティ。 例：CN=Issuer，C=US，ST=NY，L=New York，O=Work Organization，O=example.com

証明書のフィールド	説明
Validity	認証局が証明書のステータス情報の保持を保証する期間。 ➤ **Not Before**：証明書の有効期間の開始日を指定します。 例：Nov 25 04:34:49 2009 GMT ➤ **Not After**：証明書の有効期間の終了日を指定します。 例：Nov 25 04:34:49 2010 GMT
Subject	サブジェクト公開鍵キー・フィールドに格納されている公開鍵に関連付けられているエンティティ。
Subject Public Key Info	公開鍵の送信とテストに使用するアルゴリズムを識別するために使用します（例：RSA，DSA，Diffie-Hellman）。

詳細については，インターネット X.509 PKI 証明書と証明書失効リスト（CRL）プロファイルを参照してください。

http://tools.ietf.org/html/rfc5280

➤ **Subject フィールド**

Subject フィールド（サブジェクト識別名，SubjectDN）は，公開鍵と関連付けられているエンティティを識別します。

Subject フィールドには，次のような属性があります。

サブジェクト属性	サブジェクト属性の説明	例
CN	共通名	CN=Bob BobFamily
emailAddress	電子メール・アドレス	emailAddress=bob@example.com
C	国名	C=US
ST	州名または県名	ST=NY

サブジェクト属性	サブジェクト属性の説明	例
L	地域名	L=New York
O	組織名	O=Work Organization
OU	組織単位名	OU=Managers

サブジェクトからユーザ ID を取得するには，SubjectDN フィールド全体または SubjectDN 属性を使用します。

➤ クライアント証明書情報の拡張

X.509 v3 証明書の拡張により，ユーザや公開鍵に追加属性を関連付けたり，認証局同士の関係を管理したりすることができます。Subject Alternative Name フィールドにユーザ ID を含めることができます。

➤ Subject Alternative Name フィールド

サブジェクト代替名の拡張により，証明書のサブジェクトに ID をバインドできます。これらの ID は，証明書の Subject フィールドの ID に追加して，またはその代わりとして含めることができます。

Subject Alternative Name フィールドには，次の ID を含めることができます。

ID	例
otherName	Other Name: Principal Name= bobOtherAltName@example.com
rfc822Name	RFC822 Name =bobRFC822AltName@example.com
dNSName	DNS Name=example1.com
x400Address	
directoryName	Directory Address: E=bobDirAltName@example.com, CN=bob, OU=Gold Ballads, O=Gold Music, C=US
ediPartyName	
uniformResourceIdentifier	URL=http://example.com/

ID	例
iPAddress	IP Address=192.168.7.1
registeredID	Registered ID=1.2.3.4

サブジェクト代替名からユーザ識別子を取得するには，いずれかの ID を使用します。

構成

Configuration Manager は LW-SSO を使用して，クライアント証明書のユーザ識別子を活用します。クライアント証明書ハンドラは，ユーザ識別子を活用するための LW-SSO の構成に次の属性を使用します。

クライアント証明書の情報を活用するため，Configuration Manager でユーザ識別子を取得する方法を構成する必要があります。

次の点を決定します。

- 使用するフィールド（SubjectDN フィールド，Subject Alternative Name フィールド）
- フィールド全体を使用するか，フィールドの一部のみを使用するか
- 入力フィールドの一部を使用する場合の値の入力（SubjectDN にサブジェクト属性を入力するか，Subject Alternative Name に ID を入力するか）

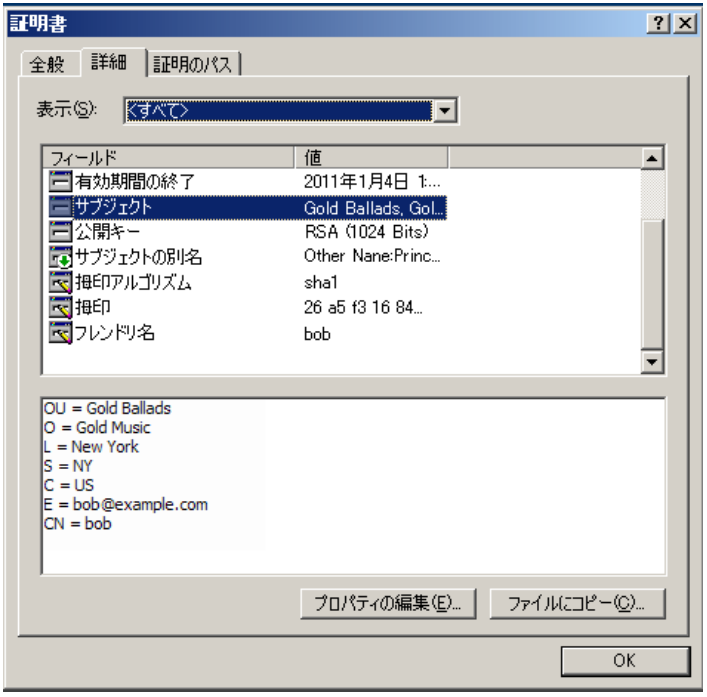
クライアント証明書ハンドラは，次の属性を使用して LW-SSO を構成します。

属性名	説明
enabled	ハンドラが有効か無効かを指定します。 **重要：**この値を明示的に false に設定して，ハンドラを有効にするのは，クライアント証明書の検証が必要な場合のみにすることを強くお勧めします。
userIdentifierRetrieveField	このパラメータは，証明書のどのフィールドにユーザ識別子が格納されているかを示します。オプションは **SubjectDN** または **SubjectAlternativeName** です。

属性名	説明
userIdentifierRetrieveMode	このパラメータは，フィールドに格納されている内容全体がユーザ識別子か，一部としてユーザ識別子が含まれているのかを示します。オプションは **EntireField** または **FieldPart** です。
userIdentifierRetrieveFieldPart	**userIdentifierRetrieveMode** の値が **FieldPart** の場合，このパラメータは，フィールドのどの部分がユーザ名なのかを示します。この値は，証明書内で定義されている凡例に基づくコード文字です。 **注：userIdentifierRetrieveMode** が **FieldPart** に設定されている場合，この値を空にすることはできません。また，**userIdentifierRetrievField** が **SubjectAlternativeName** に設定されている場合も，この値を空にすることはできません。

例（Internet Explorer の場合）

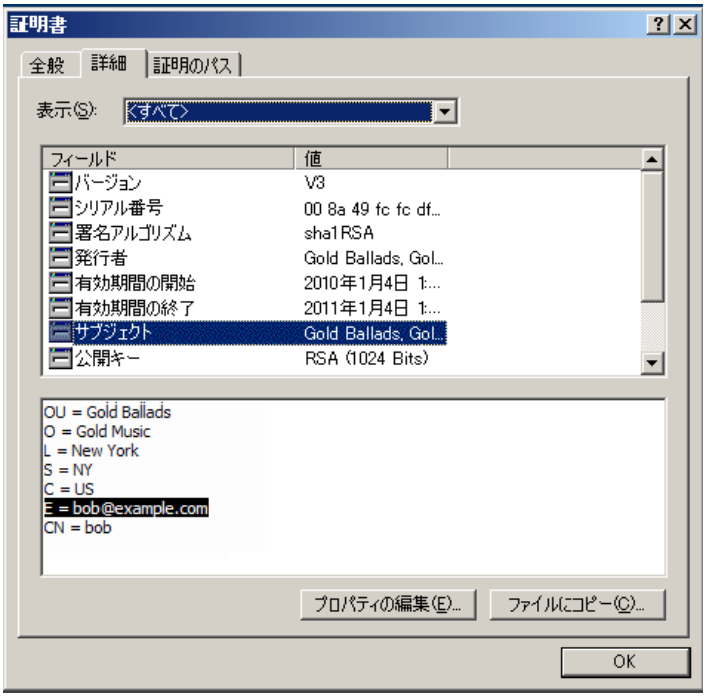
➤ **Subject を使用してユーザ識別子を格納**



次の例は，SubjectDN 全体からユーザ識別子を取得するようにハンドラを構成する方法を示しています。

```
<in-clientCertificate userIdentifierRetrieveField="SubjectDN"
userIdentifierRetrieveMode="EntireField" />
```

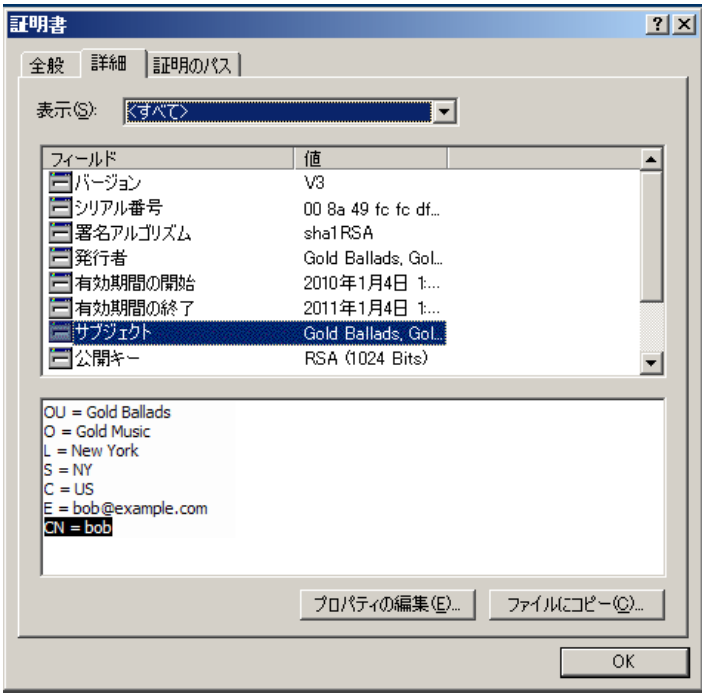
➤ Subject の Email フィールドを使用してユーザ識別子を格納



クライアント証明書の凡例で確認できるフィールド名を使用します。次の例は, Subject の Email フィールドからユーザ識別子を取得するようにハンドラを構成する方法を示しています。

```
<in-clientCertificate userIdentifierRetrieveField="SubjectDN"
userIdentifierRetrieveMode="FieldPart" userIdentifierRetrieveFieldPart="E" />
```

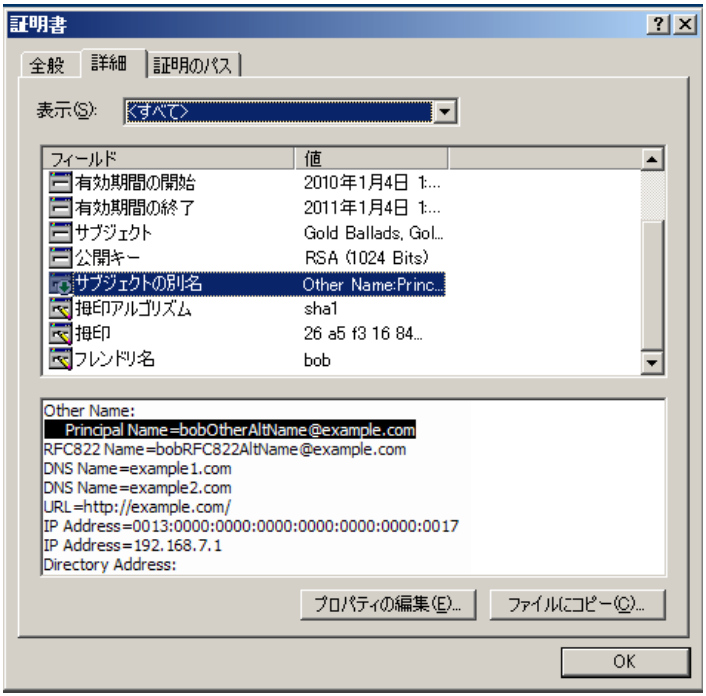
➤ **Subject の Command Name フィールドを使用してユーザ識別子を格納**



クライアント証明書の凡例で確認できるフィールド名を使用します。次の例は, Subject の Custom Name フィールドからユーザ識別子を取得するようにハンドラを構成する方法を示しています。

```
<in-clientCertificate userIdentifierRetrieveField="SubjectDN"
userIdentifierRetrieveMode="FieldPart" userIdentifierRetrieveFieldPart="CN" />
```

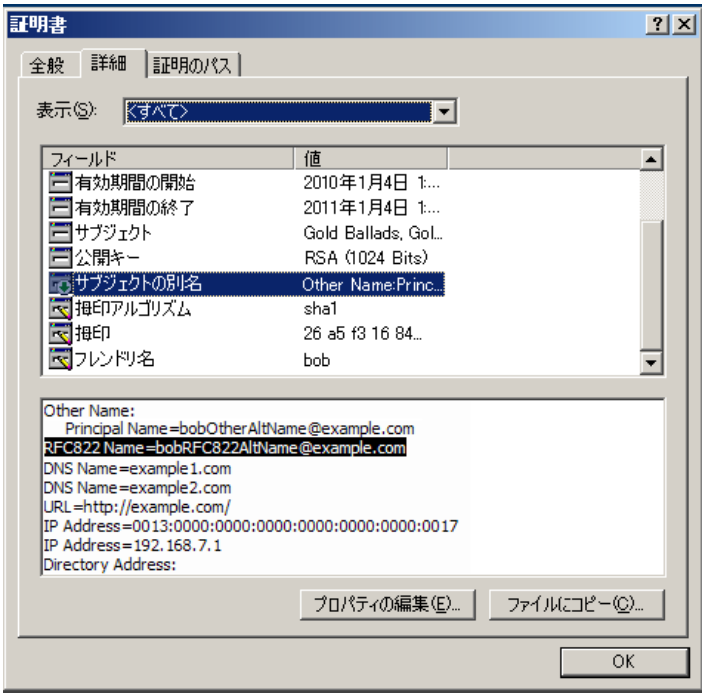
➤ Subject Alternative Name の otherName ID を使用してユーザ識別子を格納



クライアント証明書の凡例で確認できる ID 名を使用します。次の例は，Subject Alternative Name の otherName ID からユーザ識別子を取得するようにハンドラを構成する方法を示しています。

```
<in-clientCertificate userIdentifierRetrieveField="SubjectAlternativeName"
userIdentifierRetrieveMode="FieldPart" userIdentifierRetrieveFieldPart="Principal
Name" />
```

➤ Subject Alternative Name の rfc822Name ID を使用してユーザ識別子を格納



クライアント証明書の凡例で確認できる ID 名を使用します。次の例は，Subject Alternative Name の rfc822Name ID からユーザ識別子を取得するようにハンドラを構成する方法を示しています。

```
<in-clientCertificate userIdentifierRetrieveField="SubjectAlternativeName"
userIdentifierRetrieveMode="FieldPart" userIdentifierRetrieveFieldPart="Principal
Name" />
```

SSL を使用した Configuration Manager と UCMDB の連携の構成

Configuration Manager では，UCMDB の接続に Secure Sockets Layer（SSL）を使用する構成が可能です。UCMDB の標準設定では，SSL コネクタはポート 8443 で有効になります。

サーバ証明書をエクスポートしてクライアントのトラスト・ストアにインポートするには，次の手順を実行します。

1 **＜UCMDB インストール・ディレクトリ＞¥bin¥jre¥bin** に移動し，次のコマンドを実行します。

keytool -export -alias hpcert -keystore ＜UCMDB サーバ・ディレクトリ＞¥conf¥security¥server.keystore -storepass hppass -file ＜証明書ファイル＞

2 Configuration Manager のトラスト・ストア（標準設定の JRE トラスト・ストア）に証明書をインポートします。

＜CM_JAVA_HOME＞¥bin¥keytool -import -trustcacerts -alias hpcert -keystore ＜CM_JAVA_HOME＞¥lib¥security¥cacerts -storepass changeit -file ＜証明書ファイル＞

3 UCMDB 接続プロパティを Configuration Manager で設定します。

［**システム**］＞［**設定**］＞［**統合**］＞［**UCMDB ファウンデーション**］＞［**UCMDB ファウンデーション**］を選択します。接続ストラテジを **HTTPS** に，UCMDB サーバ・ポートを UCMDB HTTPS ポートに設定します。UCMDB アクセス URL を https://＜ホスト名＞:8443 に設定します。

4 構成セットを保存し，アクティブ化します。Configuration Manager を再起動します。

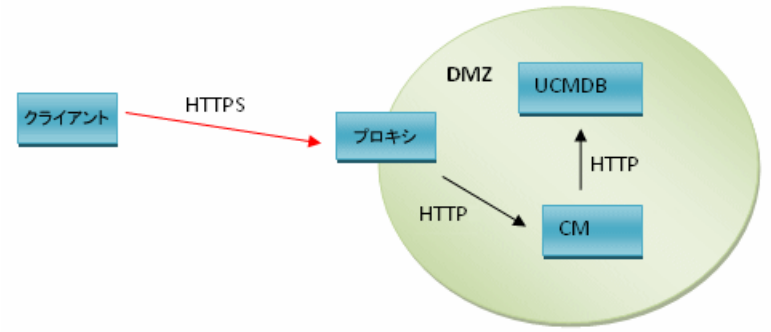
他の製品（負荷分散装置など）との接続に Secure Sockets Layer（SSL）を使用する設定を Configuration Manager で行う場合は，次のコマンドを実行します。これにより，製品のセキュリティ証明書が Configuration Manager トラスト・ストア（標準設定の JRE トラスト・ストア）にインポートされます。

＜CM_JAVA_HOME＞¥bin¥keytool -import -trustcacerts -alias ＜エイリアス＞ -keystore ＜CM_JAVA_HOME＞¥lib¥security¥cacerts -storepass changeit -file ＜証明書ファイル＞

リバース・プロキシ

Configuration Manager と UCMDB が DMZ にある場合，リバース・プロキシ・サーバを使用する設定を行うことをお勧めします。設定の手順は，UCMDB でリバース・プロキシを使用する設定と同じです。Configuration Manager へのアクセスを有効にするには，**/cnc** と **/bsf** の各パスを，Configuration Manager がインストールされているリモート・サーバの URL にマッピングする必要があります。

次の図は, Configuration Manager でのリバース・プロキシの構成プロセスを示しています。



たとえば，リバース・プロキシが Apache サーバの場合，次の行を **Apache2.2¥conf¥extra¥httpd-ssl.conf** ファイルに追加して Apache サーバを再起動します。

ProxyPass /cnc http://＜CM ホスト名＞:＜CM HTTP ポート＞/cnc
ProxyPassReverse /cnc http:// ＜CM ホスト名＞:＜CM HTTP ポート＞/cnc
ProxyPass /bsf http://＜CM ホスト名＞:＜CM HTTP ポート＞/bsf
ProxyPassReverse /bsf http://＜CM ホスト名＞:＜CM HTTP ポート＞/bsf

リバース・プロキシのタイプによって設定手順も異なるため，詳細についてはプロキシ・サーバのドキュメントを参照してください。

Configuration Manager でリバース・プロキシを構成するには，次の手順を実行します。

＜Configuration Manager インストール・ディレクトリ＞¥conf フォルダにある **client-config.properties** を次のとおり更新します。

```
bsf.server.url=https://<proxy-server-name>:443/bsf
```

Apache プロキシのデフォルトの HTTP ポートは 443 です。

第 II 部

付録

付録 A

容量の制限

次の表は，Configuration Manager の容量の上限値を示します。

ビューの最大数	100
ポリシーの最大数	300
ビューあたりの複合 CI の最大数	5000
同時ユーザの最大数	50
構成分析モジュールでの複合 CI の最大数	1000

付録 B

Lightweight シングル・サインオン認証（LW-SSO）のリファレンス

本章の内容

LW-SSO 認証の概要

LW-SSO とは，アクセス制御方法の 1 つであり，一度ログインしたユーザは，再びログインしなくても複数のソフトウェア・システムのリソースにアクセスできるようになります。構成されたソフトウェア・システム・グループ内のアリケーションは認証を信頼するので，アプリケーション間を移動する際に追加で認証を行う必要はありません。

ここでは，LW-SSO バージョン 2.2 および 2.3 に関する内容を説明します。

LW-SSO へのアクセスに関するトラブルシューティング情報については，130 ページ「LW-SSO - トラブルシューティングおよび制限事項」を参照してください。

本項の内容

➤ 114 ページ「マルチドメイン機能」

➤ 114 ページ「URL 機能で使用する SecurityToken の取得」

LW-SSO トークンの有効期限

LW-SSO トークンの有効期限に基づいて，アプリケーションのセッションの有効期限が決まります。したがって，トークンの有効期限は，アプリケーションのセッション有効期限またはそれよりも後にする必要があります。

LW-SSO トークンの有効期限の推奨値

LW-SSO を使用するアプリケーションごとに，トークンの期限を設定する必要があります。推奨値は 60 分です。高度なセキュリティを必要としないアプリケーションでは，300 分に設定することも可能です。

GMT 時間

LW-SSO に参加するアプリケーションはすべて同じ GMT 時間を使用し，誤差が 15 分以内になるように調整してください。

マルチドメイン機能

マルチドメイン機能では，LW-SSO に参加するアプリケーションを，異なる DNS ドメインのアプリケーションと統合する場合，すべてのアプリケーションで trustedHosts 設定（または **protectedDomains** 設定）を行う必要があります。さらに，**lwsso** 要素に正しいドメインを追加する必要があります。

URL 機能で使用する SecurityToken の取得

他のアプリケーションが **URL の SecurityToken** として送信した情報を受信するには，ホスト・アプリケーション設定の **lwsso** 要素で正しいドメインを設定する必要があります。

LW-SSO のセキュリティに関する警告

ここでは，LW-SSO 設定に関するセキュリティ上の警告について説明します。

➤ **LW-SSO の InitString 機密パラメータ**：LW-SSO では，対称暗号化方式を使用して LW-SSO トークンを検証および生成します。構成した **initString** パラメータは，秘密キーの初期化に使用されます。アプリケーションがトークンを生成すると，同じ initString パラメータを使用する各アプリケーションがトークンを検証します。

注意：

➤ **initString** パラメータを設定しないと，LW-SSO は使用できません。

➤ **initString** パラメータは機密情報なので，公開や転送は慎重に行い，永続性を考慮して取り扱ってください。

➤ **initString** パラメータの共有は，LW-SSO を使用して相互に統合されたアプリケーション間のみに限定する必要があります。

➤ **initString** パラメータは，12 文字以上である必要があります。

➤ **必要な場合のみ LW-SSO を有効化**：LW-SSO は，必要な場合以外は無効にしてください。

➤ **認証セキュリティのレベル**：LW-SSO に参加するアプリケーションの中で最も弱い認証フレームワークを使用し，他の参加アプリケーションによって信頼されている LW-SSO トークンを発行するアプリケーションが基準となって，アプリケーション全体の認証セキュリティ・レベルが決まります。

したがって，LW-SSO トークンの発行は，強力で安全な認証フレームワークを使用するアプリケーションに限定することをお勧めします。

- **対称暗号化方式による影響**：LW-SSO は，対称暗号化方式を使用して LW-SSO トークンを発行および検証します。LW-SSO を使用するアプリケーションによって発行されるトークンは，同じ **initString** パラメータを共有するすべてのアプリケーションによって信頼されることになります。したがって，initString を共有するアプリケーションが信頼されていない場所に配置されている場合や信頼されていない場所からアクセス可能な場合には，セキュリティ上のリスクが伴います。

- **ユーザのマッピング（同期）**：LW-SSO フレームワークでは，統合アプリケーション間のユーザ・マッピングは保証されません。したがって，統合アプリケーションではユーザ・マッピングを監視する必要があります。すべての統合アプリケーションで同じユーザ・レジストリ （LDAP/AD など）を共有することをお勧めします。

  ユーザのマッピングに失敗すると，セキュリティ違反が発生し，アプリケーションが予期しない動作をすることがあります。たとえば，実際には異なるユーザでも，複数のアプリケーションで同じユーザ名が割り当てられている可能性があります。

  また，ユーザがあるアプリケーション（AppA）にログインしてから，コンテナ認証またはアプリケーション認証を使用する別のアプリケーション（AppB）にアクセスする場合，ユーザのマッピングに失敗すると，ユーザは手動で AppB にログインしてユーザ名を入力しなければなりません。このとき，AppA へのログイン時とは別のユーザ名を入力し，AppA または AppB からさらに別のアプリケーション（AppC）にアクセスする場合，AppC へのログインには，AppA または AppB へのログインで使用したユーザ名がそのまま使用されます。

- **ID マネージャ**：認証に使用される機能です。ID マネージャ内にある保護されていないリソースはすべて，LW-SSO 構成ファイル内で **nonsecureURLs** に設定する必要があります。

付録 C

トラブルシューティング

本章の内容

一般的なトラブルシューティングおよび制限事項

制限事項

UCMDB で新規作成した CI タイプは，Configuration Manager をログアウトしてからログインし直すまでは表示されません。

トラブルシューティング

問題：［ノード］CI タイプの **name** 属性に［変更をモニタ］の修飾子が付かず，CI 認証で認証済みステータスにコピーされない。これは，Configuration Manager バージョン 9.20 が UCMDB 向けの Content Pack 9 なしでインストールされている場合に発生します。

解決策：次のいずれかの手順を実行します。

➤ UCMDB CI タイプ・マネージャで，**name** 属性に［変更をモニタ］の修飾子が付くように手動で設定します。

➤ Content Pack 9 をインストールします。

問題：Configuration Manager サービスを開始すると，次のエラー・メッセージが表示される。

ローカル コンピュータで HP Universal CMDB Configuration Manager を起動できません。詳細については，システム マネージャ イベント ログを確認してください。これが Microsoft 以外のサービスである場合は，サービスの製造元に問い合わせてサービス固有のエラー コード 0 を参照してください。

解決策：次の手順を実行します。

1 **＜Configuration Manager インストール・ディレクトリ＞¥cnc¥bin** に移動し，次のコマンドを実行します。

edit-server-0.bat

2 ［Startup］タブを選択します。（下部の）［Mode］ドロップダウン・リストで，**exe** の代わりに **jvm** を選択します。

3 ［Shutdown］タブを選択します。［Class］フィールドで最後の名前を **Boostrap** から **Bootstrap** に変更します。

4 ［**OK**］をクリックします。

5 サービスを実行します。

Deployment Manager - トラブルシューティングおよび制限事項

Deployment Manager のトラブルシューティングを行うには，次のディレクトリにある前回のセッションのセッション・ログを開きます。

%temp%¥HP¥ucmdb-dm¥Workspace¥Sessions

再デプロイに関する一般的なガイドライン

インストール中，Deployment Manager の［検証］ページでデプロイ済みの各コンポーネントの横の［詳細］ボタンをクリックして表示される警告やエラーに注意してください。

デプロイ中に問題が発生し，解決策がみつかった場合，次の手順を実行します。

1 デプロイされた製品をアンインストールし，マシンを再起動します。

2 Deployment Manager を再起動し，すべての構成を入力し直します。

デプロイの失敗に関する問題

問題：デプロイ中に権限エラーが発生する。

セッション・ログには，新規スキーマの作成時のデータベース・ユーザの権限に問題があることが示されています。

解決策：新規データベースを作成するには，適切な権限が必要です。デプロイに使用したユーザ資格情報がテーブルスペースおよびスキーマの作成に十分かどうかを確認してください。

問題：UCMDB でスキーマやデータベースを構成できない。

セッション・ログには，Deployment Manager でスキーマまたはデータベースの作成に失敗したことが示されています。

解決策：

注：（データベース・サーバのタイプにかかわらず）UCMDB の新規スキーマを作成して既存の UCMDB 履歴スキーマに接続することはできません。

UCMDB スキーマおよび UCMDB 履歴スキーマで，次の接続タイプが使用されていないことを確認してください。

➤ UCMDB スキーマ - Create New Schema

➤ UCMDB 履歴スキーマ - Connect to Existing Schema

問題：UCMDB でスキーマやデータベースを構成できない。

セッション・ログには，スキーマを作成できなかったことが示されています。

解決策：session.log を開き，次のメッセージを確認します。
SQL error executing statement CREATE USER **＜スキーマ名＞**

Deployment Managerの［Database Configuration］ページで Oracle スキーマに名前を付けるとき，使用できるのは文字（a ～ z），数字（0 ～ 9），ハイフン記号（「-」）のみです。

問題：領域が不足しているため，スキーマを作成できない。

解決策：スキーマまたはデータベースの空き領域を増やします。Oracle および Microsoft から提供されている標準の管理インタフェースを使用します。

問題：データベース構成で次のエラーが発生する。
NT AUTHORITY¥ANONYMOUS LOGON Could not connect to database.

MSSQL サーバを選択するときに UCMDB データベース構成に NTLM 認証を選択すると，データベース構成でエラーが発生し，デプロイが失敗します。

解決策: UCMDB を localhost マシン（NTLM 認証がサポートされている唯一のマシン）にデプロイします。

問題：新規データベースを作成しているときに，Configuration Manager データベース構成に失敗する。

Deployment Manager の［詳細］パネルに，次のエラーが発生することがあります。

Failed to create Oracle schema due to error: ORA-01031: insufficient privileges

または

Failed to create a schema to the database: machineName. Reason: ORA-01919: role 'RESOURCE' does not exist

解決策：データベース・ユーザに次の役割の権限があることを確認します。

- 接続
- リソース

問題：ターゲット・ホスト・マシンのディスク領域不足のため，デプロイを実行できなかった。

解決策：ターゲット・ホスト・マシンにログインし，デプロイを正常に実行するために十分なディスク領域があることを確認します。

- UCMDB 用に 1GB の空き領域
- Configuration Manager 用に 1GB の空き領域
- DDMA 用に 1GB の空き領域

注：個々の製品に必要なディスク領域に加え，一時ファイルの処理のためにさらに 1GB の空き領域が必要です。

問題：Ping UCMDB ユーティリティでエラーが発生する。

このユーティリティは Configuration Manager マシンから実行され，既存の UCMDB インスタンスへの接続が使用可能かどうかを確認します。session.log を開き，次のメッセージを確認します。
Failed to test connection due to error: java.net.ConnectException: Connection refused: connect.

解決策：

- ターゲット UCMDB のポート 8080 が Windows ファイアウォールによってブロックされていないことを確認します。
- Configuration Manager マシンから UCMDB サーバにアクセスできることと, UCMDB のデプロイが正常に完了して稼働していることを確認します。

ホスト・マシンの接続不可

問題：RPC が使用できない。または，不明なエラーが発生する。

［テスト接続］ボタンをクリックすると，RPC 使用不可のエラーが発生します。

解決策：ホスト名が間違っている場合は修正し，WMI サービスとサーバ・サービスが動作していることと, Windows ファイアウォールが WMI インタフェースへのアクセスをブロックしていないことを確認します。

Windows ファイアウォールを無効にするか, ファイアウォールに例外を追加して, リモート管理アクセスを有効にします。

リモート管理アクセスを有効にするためには，コントロール・パネルで［**ファイアウォール**］を開いて［**受信の規則**］を選択します。すべてのファイルおよびプリンタ，WMI ルール，ポート 8080 を有効にします。

テスト接続に失敗

問題：アクセスが拒否される。

アクセスが拒否されるのは，ユーザ名やパスワードが間違っている場合，DNS 設定が無効な場合，デプロイで使用したユーザ名にターゲット・ホスト・マシンでの管理者資格情報がない場合です。

解決策：指定したユーザ資格情報が正しいことと，そのユーザにターゲット・ホスト・マシンでの管理者資格情報があることを確認します。

アプリケーションへのアクセスの失敗

問題：デプロイに成功した後，アプリケーション（UCMDB または Configuration Manager）へのアクセスに失敗する。

解決策：次の UCMDB および Configuration Manager サービスが存在し，動作していることを確認します。

- **UCMDB_Server** サービス
- **HPUCMDBCMoasisSNAPSHOTserver0** サービス

セッション・ディレクトリにあるデプロイメント・ログで，エラーを確認します。

LW-SSO の無効化

問題：デプロイに成功したが，LW-SSO 機能が無効になっている。

解決策：LW-SSO の初期化文字列とドメインが UCMDB と Configuration Manager（および該当する場合は OO）の両方で同じであることを確認します。

次の方法で，製品の LW-SSO 構成セットを確認します。

- Configuration Manager の場合：**lwssofmconf.xml** ファイルを開き，ドメインおよび初期化文字列の設定を確認します。このファイルは **＜ Configuration Manager インストール・ディレクトリ＞¥conf** フォルダにあります。
- UCMDB の場合：UCMDB を開き，［**マネージャ**］＞［**管理**］＞［**インフラストラクチャ設定マネージャ**］を選択します。

Configuration Manager と UCMDB が存在するホスト・マシンの DNS ドメインが異なる場合，**信頼済みドメイン**の設定に両製品で有効な DNS ドメインの両方が含まれていることを確認します。

デプロイメントに関する追加情報を受信するには，Deployment Manager をデバッグ・モードにします。デバッグ・モードにすると，デプロイメントに関する追加情報を取得できます。

デバッグ・モードを有効にするには，次の手順を実行します。

1. Deployment Manager を実行した後，ブラウザ・ウィンドウを開いてアドレス・バーに %temp% と入力します。
2. **hp¥ucmdb-dm** フォルダに移動します。

3 **ini** ファイルをテキスト・エディタで開き，ファイルの最後の行に次のプロパティを追加します。

-Ddebug.mode=true

4 **%temp%¥HP¥ucmdb-dm¥ucmdb-dm.exe** で Deployment Manager を実行します。

Configuration Manager へのアクセス - トラブルシューティングおよび制限事項

制限事項

➤ Configuration Manager Tomcat サーバで時刻を変更した場合は，サーバ上の時刻を更新するために，サーバの再起動が必要です。

トラブルシューティング

問題：［**システム**］＞［**設定**］で構成セットを変更した後，サーバが起動しない。

解決策：構成セットを変更前の状態に戻します。次の手順を実行してください。

1 次のコマンドを実行し，最後にアクティブ化した構成セットの ID を取得します。

＜Configuration Manager インストール・ディレクトリ＞¥bin¥export-cs.bat ＜データベース・プロパティ＞ --history

＜データベース・プロパティ＞には，**＜Configuration Manager インストール・ディレクトリ＞¥conf¥database.properties** ファイルの場所を指定するか，各データベース・プロパティを指定します。次に例を示します。

cd ＜Configuration Manager インストール・ディレクトリ＞¥bin export-cs.bat -p ..¥conf¥database.properties --history

2 次のコマンドを実行し，最後にアクティブ化した構成セットをエクスポートします。

＜Configuration Manager のインストール・ディレクトリ＞¥bin¥export-cs.bat ＜データベース・プロパティ＞ ＜構成セット ID＞ ＜ダンプ・ファイル名＞

＜構成セット ID＞には前記の手順で取得した構成セット ID，**＜ダンプ・ファイル名＞**には構成セットをするのに使用する一時ファイルの名前を指定します。たとえば，ID が **491520** の構成セットを **mydump.zip** ファイルにエクスポートするには，次のコマンドを実行します。

cd ＜Configuration Manager インストール・ディレクトリ＞¥bin export-cs.bat -p ..¥conf¥database.properties -i 491520 -f mydump.zip

3 Configuration Manager サービスを停止します。

4 次のコマンドを実行し，上記の構成セットをインポートしてからアクティブ化します。

＜Configuration Manager のインストール・ディレクトリ＞¥bin¥import-cs.bat ＜データベース・プロパティ＞ -i ＜ダンプ・ファイル名＞ --activate

問題：UCMDB 接続でエラーが発生する。

解決策：次のいずれかが原因として考えられます。

- UCMDB サーバが起動していません。UCMDB が完全に稼働状態になってから（UCMDB サーバのステータスが［**Up**］であることを確認），Configuration Manager を再起動します。
- UCMDB サーバは稼働していますが，Configuration Manager の接続資格情報または URL に誤りがあります。Configuration Manager を起動します。［**システム**］＞［**設定**］＞［**統合**］＞［**UCMDB ファウンデーション**］＞［**UCMDB ファウンデーション**］を選択し，設定を変更して新しい構成セットを保存します。構成セットをアクティブ化して，サーバを再起動します。

問題：LDAP 接続設定に誤りがある。

解決策：構成セットを変更前の状態に戻します。正しい LDAP 接続を設定し，新しい構成セットをアクティブ化します。

問題：UCMDB クラス・モデルの変更が Configuration Manager で検出されない。

解決策：Configuration Manager サーバを再起動します。

問題：Configuration Manager ログに **UCMDB 実行タイムアウト・**エラーが記録される。

解決策：このエラーは，UCMDB データベースが過負荷状態になると発生します。エラーが発生しないようにするには，接続タイムアウトの値を大きくします。

1 jdbc.properties ファイルを **UCMDBServer¥conf** フォルダに作成します。

2 次のように入力します。QueryTimeout＝＜秒数＞

3 UCMDB サーバを再起動します。

問題：管理ビューを Configuration Manager に追加できない。

解決策：管理ビューを追加すると，UCMDB で新しい TQL が作成されます。アクティブな TQL の数が上限に達すると，ビューを追加できなくなります。UCMDB でサポートされるアクティブな TQL の最大数を増やすには，インフラストラクチャ設定マネージャで次の値を変更します。

- サーバ内の最大アクティブ TQL 数
- 最大カスタマ アクティブ TQL 数

問題：HTTPS サーバの証明書が有効でない。

解決策：次のいずれかが原因として考えられます。

- 証明書の有効期限が切れています。新しい証明書を取得する必要があります。
- 証明書の証明機関が信頼された機関ではありません。信頼されたルート証明機関リストに証明機関を追加してください。

問題：Configuration Manager のログイン・ページからログインすると，ログイン・エラーまたはアクセス拒否ページが表示される。

解決策：次のいずれかが原因として考えられます。

- ユーザ名が認証プロバイダ（外部/共有 LDAP）で定義されていない可能性があります。ユーザを認証プロバイダ・システムに追加してください。
- ユーザは定義されていますが，Configuration Manager に対するログイン権限が割り当てられていません。ログイン権限を割り当ててください。ベスト・プラクティスとして，すべての Configuration Manager ユーザのルート・グループに，ログイン権限を割り当てる方法が推奨されています。
- 上記の解決方法は，IDM システム・ログインからのログインに失敗した場合にも適用できます。

問題：誤ったデータベース資格情報を入力したことが原因で Configuration Manager サーバが起動しない。

解決策：データベース資格情報を変更した後にサーバが起動しなくなった場合は，資格情報に誤りがある可能性があります。(**注：**Post Installation ウィザードでは，入力した資格情報は自動的にテストされません。［**テスト**］ボタンをクリックする必要があります)。データベース・パスワードを再度暗号化し，新しい資格情報を構成ファイルに入力する必要があります。次の手順を実行してください。

1 コマンド・ラインで次のコマンドを実行し，変更後のデータベース・パスワードを暗号化します。

＜Configuration Manager のインストール・ディレクトリ＞¥bin¥encrypt-password.bat -p ＜パスワード＞

暗号化されたパスワードが返されます。

2 暗号化されたパスワード（{ENCRYPTED} プレフィックスも含む）を **＜Configuration Manager インストール・ディレクトリ＞¥conf¥database.properties** の **db.password** パラメータにコピーします。

問題：DNS の設定に誤りがあると，ログイン時にサーバ IP アドレスを指定する必要があるが，IP アドレスを入力するとさらに別の DNS エラーが発生する。

解決策：マシン名ではなく IP アドレスを指定します。例：

次の IP アドレスを使用してログインします。http://16.55.245.240:8180/cnc/

この場合，DNS エラーが発生し，アドレスとマシン名が表示されます。次に例を示します。http://my.example.com:8180/bsf/secure/authenicationPointURL.jsp...

次のように入力します。http://10.0.0.1:8180/bsf/secure/authenicationPointURL.jsp...

再度，ブラウザでアプリケーションを起動します。

問題：Configuration Manager Tomcat サーバが起動しない。

解決策：次のいずれかの手順を実行してください。

- Post Installation ウィザードを実行して，Configuration Manager サーバ・ポートを変更します。
- Configuration Manager ポートを使用している他のプロセスを中断します。
- Configuration Manager 構成ファイルで指定されているポートを手作業で変更します。**＜Configuration Manager インストール・ディレクトリ＞¥servers¥server-0¥conf¥server.xml**）を編集し，次の関連ポートを変更します。
  - HTTP (8180)：69 行
  - HTTPS (8443)：71 行，90 行

問題：「メモリ不足」のメッセージが表示される。

解決策：次の手順で，サーバ起動パラメータを変更します。

1 次のバッチ・ファイルを実行します。

＜Configuration Manager インストール・ディレクトリ＞/bin/edit-server-0.bat

2 次の設定を変更します。

-Dapplication.ms=＜メモリ・プールの初期サイズ＞
-Dapplication.mx=＜メモリ・プールの最大サイズ＞

問題：Post Installation ウィザードで［**完了**］をクリックした後の処理に長時間かかる。

解決策：事前に UCMDB システムを統合モードに設定していない場合，スキーマの統合に時間がかかることがあります（データ量によってかかる時間の長さは異なります）。15 分待っても処理が進まない場合，Post Installation ウィザードを中断してプロセスを再開してください。

問題：UCMDB で CI を変更したが，Configuration Manager に反映されない。

解決策：Configuration Manager で実行される分析プロセスは，オフラインのプロセスであり，非同期的に実行されます。したがって，UCMDB の最新の変更がまだ処理されていない可能性があります。この問題を解決するには，次のいずれかの手順を実行してください。

- 数分間待ちます。分析プロセスの実行間隔は，デフォルトで 10 分に設定されています。［**システム**］＞［**設定**］で設定できます。
- JMX 呼び出しを実行します。これにより，ビューに含まれるオフラインの分析計算が実行されます。
- ［**管理**］＞［**ポリシー**］＞［**構成ポリシー**］を選択します。［**ポリシー分析の再計算**］ボタンをクリックします。これにより，オフラインの分析プロセスがすべてのビューで実行されます（多少時間がかかる場合があります）。また，ポリシーを人為的に変更して保存する操作が必要になることもあります。

問題：［**管理**］＞［**UCMDB ファウンデーション**］をクリックすると，UCMDB のログイン・ページが開く。

解決策：再度ログインせずに UCMDB にアクセスするには，シングル・サインオンを有効にする必要があります。詳細については，70 ページ「シングル・サインオン（SSO）」を参照してください。さらに，ログインに使用する Configuration Manager ユーザが UCMDB ユーザ管理システムで定義されていることを確認してください。

問題：Post Installation ウィザードで IPv6 アドレスに対する UCMDB 接続を設定しようとすると，［**管理**］＞［**UCMDB ファウンデーション**］が使用できなくなる。

解決策：次の手順を実行してください。

1 ［**システム**］＞［**設定**］＞［**統合**］＞［**UCMDB ファウンデーション**］＞［**UCMDB ファウンデーション**］を選択します。

2 UCMDB アクセス URL の IP アドレスを角括弧で囲みます。たとえば，http://[x:x:x:x:x:x:x:x]:8080/ のようになります。

3 構成セットを保存し，アクティブ化します。

4 Configuration Manager を再起動します。

LW-SSO - トラブルシューティングおよび制限事項

既知の問題

ここでは，LW-SSO 認証に関する既知の問題について説明します。

➤ **セキュリティ・コンテキスト**：LW-SSO のセキュリティ・コンテキストでは，1 つの属性名につき 1 つの属性値のみがサポートされます。

したがって，SAML2 トークンが同じ属性名の値を複数送信しても，LW-SSO フレームワークは 1 つの値しか受信しません。

同様に，同じ属性名の値を複数送信するように IdM トークンが設定されていても，LW-SSO フレームワークで許可される値は 1 つのみです。

➤ **Internet Explorer 7 使用時のマルチドメインのログアウト機能**：次の場合，マルチドメインのログアウト機能は失敗することがあります。

➤ Internet Explorer 7 を使用していて，アプリケーションのログアウト手順で HTTP 302 リダイレクトの動作が 4 回以上連続で呼び出された場合。

この場合，Internet Explorer 7 では HTTP 302 リダイレクト応答が正しく処理されず，［**Internet Explorer ではこのページは表示できません**］というエラー・ページが表示されることがあります。

この問題を回避するには，アプリケーションのログアウト手順で実行するリダイレクト・コマンドの回数を少なくすることを推奨します。

制限事項

LW-SSO 認証では，次の制限に注意してください。

➤ **アプリケーションへのクライアント・アクセス**

ドメインが LW-SSO 構成で定義されている場合

➤ アプリケーションのクライアントは，ログイン URL で FQDN（完全修飾ドメイン名）を使用してアプリケーションにアクセスする必要があります（http://myserver.**companydomain**.com/WebApp など）。

➤ LW-SSO では，IP アドレスを使用した URL はサポートされていません（http://192.168.12.13/WebApp など）。

➤ LW-SSO では，ドメイン指定のない URL はサポートされていません（http://myserver/WebApp など）。

LW-SSO 構成でドメインが定義されていない場合: クライアントは，ログイン URL で FQDN が指定されていないアプリケーションにアクセスできます。この場合，このマシン専用に，ドメイン情報なしで LW-SSO のセッション Cookie が作成されます。この Cookie は他のブラウザに委譲されたり，同じ DNS ドメインにある別のコンピュータに渡されることはありません。したがって，LW-SSO は同じドメインで機能しなくなります。

➤ **LW-SSO フレームワークの統合**：アプリケーションで LW-SSO 機能を使用するには，アプリケーションをあらかじめ LW-SSO フレームワーク内に統合しておく必要がありおます。

➤ **マルチドメインのサポート**

➤ マルチドメイン機能は，HTTP リファラを使用します。したがって，LW-SSO ではアプリケーション間のリンクはサポートされていますが, 両方のアプリケーションが同じドメイン上にある場合を除き, ブラウザ・ウィンドウでの URL 入力はサポートされていません。

➤ 最初のクロスドメイン・リンクには **HTTP POST** を使用できません。

マルチドメイン機能では，最初に **HTTP POST** 要求を使用することはサポートされていません（**HTTP GET** 要求のみサポートされています）。たとえば，あるアプリケーションから別のアプリケーションへの HTTP リンクでは，**HTTP GET** 要求はサポートされていますが，**HTTP FORM** 要求はサポートされていません。2 回目以降の要求は，すべて **HTTP POST** か **HTTP GET** のいずれかになります。

- LW-SSO トークンのサイズ

  LW-SSO が異なるドメインのアプリケーション間で転送できる情報量は，15 のグループ/役割/属性までに制限されています（各項目の長さは平均 15 文字です)。

- マルチドメイン・シナリオでの，保護されたページ（HTTPS）から保護されていないページ（HTTP）へのリンク

  保護されたページ（HTTPS）から保護されていないページ（HTTP）にリンクする場合，マルチドメインは機能しません。これはブラウザの制限事項の 1 つです。保護されたリソースから保護されていないリソースにリンクする際，リファラ・ヘッダは送信されません。具体例については，
  http://support.microsoft.com/support/kb/articles/Q178/0/66.ASP を参照してください。

- **SAML2 トークン**

  - SAML2 トークンを使用する場合，ログアウト機能がサポートされません。

    したがって, SAML2 トークンを使用して別のアプリケーションにアクセスすると，最初のアプリケーションからログアウトするユーザが，2 番目のアプリケーションからログアウトできなくなります。

  - SAML2 トークンの期限切れはアプリケーションのセッション管理に反映されません。

    したがって，SAML2 トークンを使用して別のアプリケーションにアクセスする場合，アプリケーションのセッション管理は個別に処理されます。

- **JAAS Realm**：Tomcat の JAAS Realm はサポートされていません。

- **Tomcat ディレクトリでの空白文字の使用**：Tomcat ディレクトリでは，空白文字はサポートされていません。

  Tomcat インストール・パス（フォルダ）に空白文字が含まれ（「Program Files」など)，LW-SSO 構成ファイルが **common¥classes** Tomcat フォルダに格納されていると，LW-SSO は使用できなくなります。

- **負荷分散装置の構成**:LW-SSO を使ってデプロイした負荷分散装置では, スティッキー・セッションを使用する設定が必要です。

トラブルシューティング

問題：ログイン後，LW-SSO Cookie が作成されない。

- **考えられる原因：**構成の LW-SSO 要素で，空でないドメインが不適切に定義されている。
- **解決策：**構成の LW-SSO 要素で定義したドメインがアプリケーションのドメインと同じであることを確認します。
- **考えられる原因：**enableSSO 関数にパラメータとして渡される空でないドメインが正しくない。
- **解決策：**enableSSO 関数にパラメータとして渡されるドメインがアプリケーションのドメインと同じであることを確認します。
- **考えられる原因：**LW-SSO 構成でドメインが定義されているとき，アプリケーションにアクセスするためのログイン URL で完全修飾ドメイン名（FQDN）を使用していない（例：http://192.168.12.13/WebApp）。
- **解決策：**アプリケーションにアクセスするため，ログイン URL で完全修飾ドメイン名（FQDN）を使用します（例：http://myserver.companydomain.com/WebApp）。

問題：LW-SSO で AutoCookieCreation 機能の Cookie が作成されない。

- **考えられる原因：**構成の LW-SSO 要素で，ドメインが適切に定義されていない。
- **解決策：**構成の LW-SSO 要素で定義したドメインがアプリケーションのドメインと同じであることを確認します。

問題：LW-SSO トークンが検証されない。

- **考えられる原因：**構成の暗号化要素で，2 つのアプリケーションの initString パラメータ（またはその他の暗号化パラメータ）が異なる。
- **解決策：**（LW-SSO 作成要素のその他のすべての暗号化パラメータに加えて）両方のアプリケーションで同じ initString を使用します。
- **考えられる原因：**2 つのアプリケーションの GMT 時間の誤差が 15 分を超えている。

➤ **解決策：**LW-SSO 統合に参加するアプリケーションがすべて同じ GMT 時間を使用し，誤差が 15 分以内になるように調整してください。

➤ **考えられる原因：**構成の LW-SSO 要素でドメインが空で，同じ DNS ドメインを持つ他のコンピュータ上の別のアプリケーションにアクセスしている。

➤ **解決策：**構成の LW-SSO 要素で定義したドメインがアプリケーションのドメインと同じであることを確認します。

➤ **考えられる原因：**構成の LW-SSO 要素でドメインが定義されておらず，同じ DNS ドメインを持つ他のコンピュータ上の別のアプリケーションにアクセスしている。

➤ **解決策：**LW-SSO 要素にドメインを追加し，そのドメインがアプリケーションのドメインと同じになるように定義されていることを確認します。

問題：マルチドメイン環境において，LW-SSO で LW-SSO トークンを検証できない。

➤ **考えられる原因：**いずれかのアプリケーションの構成において，LW-SSO 要素でドメインが不適切に定義されている。

➤ **解決策：**アプリケーション構成の LW-SSO 要素に定義されているドメインは，使用中の実際のドメインと一致し，アプリケーションのドメインと同じである必要があります。

➤ **考えられる原因：**いずれかのアプリケーション構成において，trustedHosts 設定（または protectedDomains 設定）でドメインが不適切に定義されている。

➤ **解決策：**すべてのアプリケーション設定の trustedHosts 設定（または protectedDomains 設定）のドメインが正しく定義されていることを確認します。

➤ **考えられる原因：**Internet Explorer 6.0，7.0，8.0 を使用している場合で，LW-SSO セッション Cookie がブロックまたは拒否される。

➤ **解決策：**コンピュータの Internet Explorer のセキュリティ・ゾーンで，［イントラネット］/［信頼済み］ゾーンにすべての LW-SSO サーバを追加します（［ツール］＞［インターネット オプション］＞［ローカル インターネット］＞［サイト］＞［詳細設定］）。これで，すべての Cookie が受け入れられます。

- **考えられる原因：**構成の暗号化要素で，いくつかのアプリケーションの initString パラメータ（またはその他の暗号化パラメータ）が異なる。
- **解決策：**（LW-SSO 作成要素のその他のすべての暗号化パラメータに加えて）すべてのアプリケーションで同じ initString を使用します。
- **考えられる原因：**いくつかのアプリケーションで，GMT 時間の誤差が 15 分を超えている。
- **解決策：**LW-SSO 統合に参加するアプリケーションがすべて同じ GMT 時間を使用し，誤差が 15 分以内になるように調整してください。
- **考えられる原因：**保護されたリソース（HTTPS）から保護されていない（HTTP）リソースへのマルチドメイン・リンクがある。
- **解決策：**複数のドメインをまたぐリンクでは，保護されたリソース（HTTPS）からの最初のリンクやドメインをまたぐ要求の行き先が別の保護されたリソース（HTTPS）になっていることを確認します。

IPv6 のサポート - トラブルシューティングおよび制限事項

制限事項

- URL に IP アドレスを含めることができません。
- オペレーティング・システムでは IPv6 と IPv4 の両方がサポートされている必要があります。IPv4 アドレスが閉じられていない，またはサポートされていない場合，Configuration Manager サーバにログインできません。
- Configuration Manager Tomcat サーバで時刻を変更した場合は，サーバ上の時刻を更新するために，必ず再起動してください。

トラブルシューティング

問題：インストール時に IPv6 アドレスへの UCMDB 接続を構成した後，［**管理**］＞［**UCMDB ファウンデーション**］が使用できなくなる。

解決策：次の手順を実行します。

1. ［**システム**］＞［**設定**］＞［**統合**］＞［**UCMDB ファウンデーション**］＞［**UCMDB ファウンデーション**］を選択します。
2. ［UCMDB アクセス URL］フィールドの IP アドレスを角括弧で囲みます。たとえば，http://[x:x:x:x:x:x:x:x]:8080/ucmdb-ui/ のようになります。
3. 構成セットを保存し，アクティブ化します。
4. Configuration Manager を再起動します。

認証 - トラブルシューティングおよび制限事項

本項では，認証に関する既知の問題について説明します。

問題：アプリケーションの認証中，認証ポイントにリダイレクトされた後にエラー 500 が発生する。

- **考えられる原因**：構成の暗号化要素で，Configuration Manager WAR と BSF WAR の initString パラメータ（またはその他の暗号化パラメータ）が異なる。

➤ **解決策：**（LW-SSO 作成要素のその他のすべての暗号化パラメータに加えて）両方のアプリケーションで同じ initString を使用します。

問題：アプリケーションの認証中，認証ポイントにリダイレクトされた後にログイン・フォームが表示されない。

解決策：Internet Explorer バージョン 6.X，7.X，8.X を使用している場合，Configuration Manager 認証セッション Cookie がブロックまたは拒否されます。コンピュータの Internet Explorer のセキュリティ・ゾーンで，[**イントラネット**]/[**信頼済み**]ゾーンに Configuration Manager サーバを追加します（[**ツール**] > [**インターネット オプション**] > [**ローカル インターネット**] > [**サイト**] > [**詳細設定**]）。これで，すべての Cookie が受け入れられます。

問題：認証後，エラー 403 が発生する。

➤ **考えられる原因：**アプリケーション構成の LW-SSO 要素で，ドメインが不適切に定義されている。

➤ **解決策：**アプリケーション構成の LW-SSO 要素で定義したドメインがアプリケーションのドメインと同じであることを確認します。

➤ **考えられる原因：**LW-SSO 構成でドメインが定義されているとき，アプリケーションにアクセスするためのログイン URL で完全修飾ドメイン名（FQDN）を使用していない（例：http://192.168.12.13/WebApp）。

➤ **解決策：**アプリケーションにアクセスするため，ログイン URL で完全修飾ドメイン名（FQDN）を使用します（例：http://myserver.companydomain.com/WebApp）。

問題：認証後，[**Get Acegi User Details**] ページが表示される。

解決策：Internet Explorer バージョン 6.X，7.X，8.X を使用している場合，Configuration Manager 認証セッション Cookie がブロックまたは拒否されます。コンピュータの Internet Explorer のセキュリティ・ゾーンで，[**イントラネット**]/[**信頼済み**]ゾーンに Configuration Manager サーバを追加します（[**ツール**] > [**インターネット オプション**] > [**ローカル インターネット**] > [**サイト**] > [**詳細設定**]）。これで，すべての Cookie が受け入れられます。