CHAPTER 8

# Unified CCE のセキュリティ管理

この章では Unified CCE ソリューションのセキュリティ管理の重要性を説明するとともに、セキュリティ管理に役立つリソースを紹介します。この章は、次の項から構成されています。


- 「セキュリティの概要」（P.8-2）
- 「セキュリティ レイヤ」（P.8-3）
- 「プラットフォームの違い」（P.8-4）
- 「セキュリティのベスト プラクティス」（P.8-5）
- 「ネットワーク ファイアウォール」（P.8-7）
- 「Active Directory の展開」（P.8-9）
- 「IPSec の展開」（P.8-13）
- 「ホスト ベース ファイアウォール」（P.8-14）
- 「サーバ セキュリティの設定」（P.8-16）
- 「ウイルス保護」（P.8-16）
- 「侵入防御」（P.8-17）
- 「パッチ管理」（P.8-19）
- 「エンドポイント セキュリティ」（P.8-20）


## この章の新トピック

表 8-1 は、この章の新トピックまたはこのマニュアルの前リリースから大幅な変更があったトピックの一覧です。

**表 8-1　新しい情報またはこのマニュアルの前リリースから変更された情報**

| 新規または改訂されたトピック | 説明箇所 |
|---|---|
| Cisco Unified Contact Center セキュリティ ウィザード | 「サーバ セキュリティの設定」（P.8-16） |
| 影響評価速報 | 「パッチ管理」（P.8-19） |
| Network Isolation IPSec ユーティリティ | 「IPSec の展開」（P.8-13） |

# セキュリティの概要

Unified CCE システムのセキュリティを実現するには、アクセス、接続要件、およびコンタクト センター内でのシステム管理を正確に定義する、効果的なセキュリティ ポリシーが必要です。優れたセキュリティ ポリシーが用意されると、内部および外部の脅威からデータ センター リソースを保護するために、また、データ プライバシー、整合性、およびシステム アベイラビリティを確保するために、シスコが数多く提供する最新のテクノロジーと製品を使用できます。

重要なセキュリティ リソースは、Unified Communications Security Solution ポータルです。このポータルは、次の URL からアクセスできます。

http://www.cisco.com/go/ipcsecurity

このサイトには、アプリケーション設計者が、エンドポイント、コール制御システム、転送ネットワーク、およびアプリケーションを使用して、安全性および信頼性に優れた Cisco Unified Communications 環境を設計するうえで役立つ重要なドキュメントおよび資料が含まれています。

Cisco Unified Communications ネットワークにおけるこれらのアプリケーションの 1 つとして Unified CCE セキュリティがありますが、高レベルでのこのセキュリティに関する考慮事項は、Cisco Unified Communications ソリューションを構成するその他のアプリケーションに関する考慮事項と大きな違いはありません。Unified CCE の展開は差異が大きく、多くの場合、音声、Virtual Private Network（VPN; バーチャル プライベート ネットワーク）、Quality of Service（QoS; クオリティ オブ サービス）、Microsoft Windows Active Directory などに加えて、レイヤ 2 およびレイヤ 3 ネットワーキングの全領域におけるコンピテンスが要求される複雑なネットワーク設計が必要になります。この章ではこれらのさまざまな領域に関連するガイダンスを示しますが、セキュア Unified CCE ネットワークの展開をすべて包括するガイドとなるものではありません。

多くの設計および展開についての疑問を解決するには、このドキュメントに加え、Unified Communications Security Solution ポータルとあわせて、シスコのその他のソリューション リファレンス ネットワーク デザイン（SRND）ガイドを使用してください。SRND には、Cisco Unified Communications のネットワーク インフラストラクチャを構築するための実績のあるベスト プラクティスが記載されています。SRND は、次の URL から入手できます。

http://www.cisco.com/go/designzone

このサイトの SRND の中には、セキュリティおよび Cisco Unified Communications に関連する次のドキュメントがあり、Unified CCE ネットワークを正しく展開するには、これらのドキュメントを使用する必要があります。

- 『*Cisco Unified Communications SRND Based on Cisco Unified Communications Manager*』
- 『*Data Center Networking: Server Farm Security SRNDv2*』
- 『*Site-to-Site IPSec VPN SRND*』
- 『*Voice and Video Enabled IPSec VPN (V3PN) SRND*』
- 『*Business Ready Teleworker SRND*』

これらのマニュアルへの変更や追加が定期的に掲載されますので、SRND Web サイトに頻繁にアクセスすることをお勧めします。

この章では、Windows Active Directory の設計および展開における複雑さについては限定して説明します。新しい Active Directory の論理構造、Active Directory を初めて展開する方法、既存の Windows 環境を Windows Server 2000 または 2003 Active Directory にアップグレードする方法、および現在の環境を Windows Active Directory 環境に再構築する方法については、Microsoft から追加情報を入手できます。特に、『*Microsoft Windows Server 2003 Deployment Kit*』の「*Designing and Deploying*

*Directory and Security Services*」の項は、組織の Active Directory の設計目標や展開目標をすべて満たすのに役立ちます。この開発キットおよび関連ドキュメントは、Microsoft の次の URL から入手できます。

http://www.microsoft.com/windowsserver2003/techinfo/reskit/deploykit.mspx

# セキュリティ レイヤ

セキュリティで適切に保護された Unified CCE 展開には、さまざまな脅威の中でも、標的にされた攻撃およびウイルスの伝搬からシステムとネットワークを保護するために、多層にわたる対策が必要です。この章は、Unified CCE 展開の保護に関連するさまざまな領域について説明することを目的としていますが、各領域の詳細については扱いません。具体的な詳細は、関連する製品のドキュメントを参照してください。

次のセキュリティ レイヤを実装し、それらの周辺のポリシーを確立することを強くお勧めします。

- 物理セキュリティ

  シスコのコンタクト センター アプリケーションを提供しているサーバが物理的に保護されていることを確認する必要があります。これらのサーバは、承認された担当者だけがアクセスを許可されたデータ センター内に配置される必要があります。また、ケーブル プラント、ルータ、およびスイッチは、アクセスが制御されていることが必要です。強力な物理層ネットワーク セキュリティ プランの実装には、データ スイッチでのポート セキュリティなども含まれます。

- 境界セキュリティ

  このドキュメントでは、セキュリティで保護されたデータ ネットワークを設計および展開する方法については詳しく説明しませんが、コンタクト センター アプリケーション向けに、効果的にセキュリティで保護された環境を確立するうえで役立つリソースの参照資料を紹介しています。

- データ セキュリティ

  お客様の機密情報を盗聴から保護するレベルを強化するために、Unified CCE では、CTI OS および Cisco Agent Desktop における Transport Layer Security（TLS; トランスポート レイヤ セキュリティ）と、サーバ間での通信チャネルを保護する IPSec をサポートしています。

- サーバ強化

  より強化された Windows Server 2003 のサポートに加えて、アプリケーションに合わせて特別に設計されたセキュリティ設定で自動的にサーバを設定できます。

- ホスト ベース ファイアウォール

  不正な着信トラフィックを使用してサーバを攻撃する悪意のあるユーザやプログラムから保護するために、Windows ファイアウォールを利用するユーザは、サーバ上で Windows Firewall Configuration Utility を使用するか Agent Desktop Installer を使用して、それぞれ Windows Server 2003 SP1/SP2 および Windows XP SP2 のファイアウォール コンポーネントを組み込むことができます。

- ウイルス保護

  すべてのサーバで、最新のウイルス定義ファイルを使用するウイルス対策アプリケーションを（毎日アップデートするようにスケジュールして）実行する必要があります。『*Hardware and System Software Specification (Bill of Materials) for Cisco ICM/IPCC Enterprise & Hosted Editions*』には、テストされたサポート対象のウイルス対策アプリケーションのリストが記載されています。この資料は、次の URL から入手できます。

  http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_implementation_design_guides_list.html

- 侵入防御

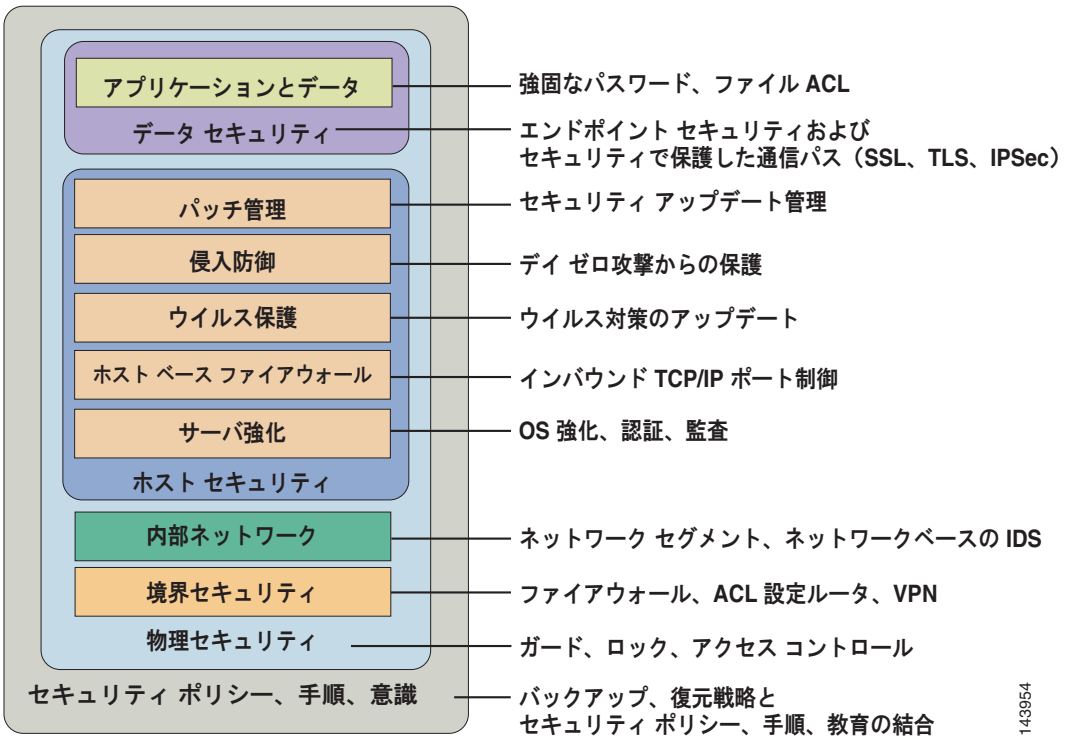
  重要な防御レイヤとなる Unified CCE Cisco Security Agent ポリシーを使用すると、サーバ上で脅威に対する「デイ ゼロ」防御を実現できます。このポリシーは、セキュリティに対する既知および未知の脅威を識別、防御、および除去することによって、運用コストの削減を図ります。

- パッチ管理

  システムは一般に、すべてのセキュリティ アップデートが適用されるまで、稼動中のネットワークに接続しないようにする必要があります。Microsoft（Windows、SQL サーバ、Internet Explorer など）およびその他のサードパーティのセキュリティ パッチを適用して、すべてのホストを最新の状態に維持することが重要です。

これらのセキュリティ レイヤの大部分に対して、Unified CCE ソリューションは、図 8-1 に示す多層防御パラダイムを実施する多くの機能をサポートしています。ただし、セキュア Unified CCE ソリューションを展開および維持するための企業ポリシーと手順をシスコが制御したり強制したりすることはできません。

**図 8-1　　多層防御**




# プラットフォームの違い

Unified CCE ネットワークに必要なさまざまなセキュリティ レイヤを設計する方法について説明する前に、この項では、Unified CCE ソリューションを構成するアプリケーションによって異なる違いについて説明します。

Unified CCE ソリューションは、管理手順の異なる多数のアプリケーション サーバによって構成されています。このドキュメントで最も重点的に扱うプライマリ サーバは、ルータ、Logger（セントラル コントローラとしても知られる）、ペリフェラル ゲートウェイ（Unified System CCE 展開では

Agent/IVR Controller と呼ばれる）、アドミン ワークステーション、Historical Data Server、WebView サーバなどです。これらのアプリケーション サーバは、標準的な（デフォルトの）オペレーティング システム インストレーションにだけインストールできます。アップグレードの場合、これらのアプリケーションは Windows 2000 Server または Advanced Server に残すことができますが（限定された移行期間の間）、新規のインストールはすべて Windows Server 2003 の Standard Edition または Enterprise Edition で実行する必要があります。デバイス ドライバ、セキュリティ アップグレードなどに関するこのオペレーティング システムのメンテナンスは、所定のベンダーから必要なソフトウェアを取得するので、お客様の責任になります。この章では、アプリケーション サーバのこのカテゴリを重点的に扱います。

セカンダリ サーバ グループ（ソリューションの一部であるが展開が異なるアプリケーションを実行するサーバ）は、Cisco Unified Communications Manager（Unified CM）、Cisco Unified IP Interactive Voice Response（Unified IP IVR; 音声自動応答装置）などです。これらのサーバは、Cisco Unified Communications Operating System（CIPT OS）へのインストールを必要とします。このオペレーティング システムは、特にこれらのアプリケーション用に設定されています。デフォルトで強化されており、シスコによって出荷および維持されます。お客様は、このオペレーティング システムに関するすべてのパッチおよびアップデートをシスコから入手する必要があります。このオペレーティング システムのセキュリティ強化のための仕様は、『*Cisco Unified Communications Solution Reference Network Design (SRND)*』およびその他の Unified CM の製品マニュアル内で参照できます。これらのガイドは、次の URL から入手できます。

http://www.cisco.com/

Unified CCE ソリューションを保護する手法は、上記のさまざまなレイヤに関連するため、サーバのグループごとに異なります。ご利用の環境でこれらのサーバを設計、展開、および維持するときには、この点に注意してください。シスコの Unified Communications 製品は、同じカスタマイズ済みオペレーティング システム、ウイルス対策アプリケーション、およびセキュリティ パス管理技術をサポートするという最終目標に向けて、常に機能強化されています。これらの機能拡張の例としては、シスコのホスト ベースの侵入防御ソフトウェア（Cisco Security Agent）、カスタマイズ済みオペレーティング システムまたはアプリケーションによるデフォルトのサーバ強化が挙げられます。

# セキュリティのベスト プラクティス

Unified CCE 7.0 のドキュメント セットの一部として、シスコはプライマリ サーバ グループに対するベスト プラクティス ガイドを発行しています。このガイドでは、Unified CCE 展開を保護するための一般的なガイダンスとあわせて、このリリースにおける新しい実装に関する多くの領域をカバーしています。ベスト プラクティス ガイドには、次のトピックが含まれています。

- 暗号化のサポート
- IPSec および NAT のサポート
- Windows ファイアウォールの設定
- 自動セキュリティ強化
- Microsoft Windows のアップデート
- SQL サーバの強化
- SSL 暗号化
- 侵入防御（CSA）
- Microsoft Baseline Security Analysis
- 監査
- ウイルス対策のガイドラインおよび推奨事項

- セキュア リモート管理
- 付加的なセキュリティ ベスト プラクティス
  - WebView および IIS の強化（Windows 2000）
  - Sybase EAServer（Jaguar）の強化
  - RMS リスナの強化
  - WMI サービスの強化
  - SNMP の強化
  - その他

最新のセキュリティ ベスト プラクティスについては、『*Security Best Practices Guide for ICM and IPCC Enterprise & Hosted Editions*』の最新バージョンを参照してください。次の URL から入手できます。

http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_technical_reference_list.html

『*Security Best Practices Guide*』内に含まれた推奨事項は、他のサードパーティ ベンダーによる強化のための推奨事項だけではなく、『*Windows Server 2003 Security Guide*』内の推奨事項など、Microsoft によって発行された強化ガイドラインに部分的に基づいています。このガイドは、製品におけるセキュリティ機能の大部分に対する基準にもなります。さらに、アプリケーション インストーラ、Windows Firewall Configuration Utility、SSL Configuration Utility、Network Isolation IPSec ユーティリティ、および Unified CC セキュリティ ウィザードとバンドルされた自動セキュリティ強化のインストール ガイドにもなります。

『*Security Best Practices Guide*』が用意されているため、この章では、多数の領域について概要だけを説明し、詳細な説明は省略しています。これにより、他のソースで入手可能な情報との重複を避けています。

### その他のセキュリティ ガイド

セキュリティ ガイダンスを記載したその他のドキュメントには、表 8-2 にリストするものが含まれますが、これらに限定されません。

**表 8-2　その他のセキュリティ ドキュメント**

| セキュリティ トピック | ドキュメントおよび URL |
|---|---|
| サーバのステージングおよび Active Directory の展開 | 『*Staging Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*』<br>http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_technical_reference_list.html |
| Cisco Security Agent | 『*Cisco Security Agent Installation/Deployment Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*』<br>http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_installation_and_configuration_guides_list.html |
| CTI OS の暗号化 | 『*CTI OS System Manager's Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*』<br>http://www.cisco.com/en/US/products/sw/custcosw/ps14/prod_installation_guides_list.html |
| | 『*Cisco CAD Installation Guide*』<br>http://www.cisco.com/en/US/products/sw/custcosw/ps427/prod_installation_guides_list.html |

表 8-2　その他のセキュリティ ドキュメント （続き）

| セキュリティ トピック | ドキュメントおよび URL |
|---|---|
| WebView のユーザ認証および管理 | 『*WebView Installation and Administration Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*』<br>http://www.cisco.com/en/US/products/sw/custcosw/ps4145/prod_installation_guides_list.html |
| SNMPv3 の認証および暗号化 | 『*SNMP Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*』<br>http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_installation_and_configuration_guides_list.html |
| Unified ICM のパーティショニング（データベース オブジェクト/アクセス コントロール） | 『*ICM Administration Guide for Cisco ICM Enterprise*』<br>http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_maintenance_guides_list.html<br>（注）　パーティショニングは Unified ICM Enterprise に対してだけサポートされています。Unified CCE、Unified ICM Hosted Edition、および Unified CCH Edition ではサポートされていません。 |
| 機能制御（ソフトウェア アクセス コントロール） | 『*ICM Configuration Guide for Cisco ICM Enterprise*』<br>http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_installation_and_configuration_guides_list.html |
| リアルタイム クライアントの検証 | 『*Setup and Configuration Guide for Cisco IPCC Hosted Edition*』<br>http://www.cisco.com/en/US/products/sw/custcosw/ps5053/prod_installation_guides_list.html |

# ネットワーク ファイアウォール

Unified CCE ネットワークでファイアウォールを展開するときには、検討が必要な重要な要素がいくつかあります。Unified CCE ソリューションを構成するアプリケーション サーバ（Cisco Collaboration Server は例外）は、DeMilitarized Zone（DMZ; 非武装地帯）に配置するようには考慮されていないため、外部から認識可能なネットワークおよび内部企業ネットワークから分離する必要があります。これらのアプリケーション サーバをデータ センターに配置し、適切なファイアウォールやルータをアクセス コントロール リスト（ACL）により当該サーバをターゲットとするトラフィックを制御するように設定して、指定されたネットワーク トラフィックだけをパススルーするようにする必要があります。

ファイアウォールが配置されている環境でアプリケーションを展開する場合には、使用されている TCP/UDP IP ポート、ファイアウォールの展開とトポロジの考慮事項、および Network Address Translation（NAT; ネットワーク アドレス変換）の影響についてネットワーク管理者がよく理解している必要があります。

# TCP/IP ポート

アプリケーションのコンタクト センター スイート全体で使用されているポートのコンポーネントについては、次のドキュメントを参照してください。

- 『*Port Utilization Guide for Cisco ICM/IPCC Enterprise and Hosted Editions*』。このガイドは、次の URL から入手できます。

  http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_installation_and_configuration_guides_list.html

- 『*Cisco Unified Contact Center Express Port Utilization Guide*』。このガイドは、次の URL から入手できます。

  http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

- 『*Cisco Unified Communications Manager TCP and UDP Port Usage Guide*』。このガイドは、次の URL から入手できます。

  http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

これらのガイドには、ファイアウォールの設定を支援するために、エージェント デスクトップとサーバ間の通信、アプリケーション管理、およびレポート生成に使用されるプロトコルとポートが記載されています。また、イントラ サーバ通信に使用されるポートのリストも記載されています。

# トポロジ

図 8-2 に示す展開トポロジは、ファイアウォールの推奨配置および Unified CCE の展開におけるその他のネットワーク インフラストラクチャ コンポーネントを表しています。図 8-2 に示すデザイン モデルでは、親 Unified ICM システムを従来のペリフェラル ホストに統合し、子 Cisco Unified System Contact Center（Unified SCC）を Unified CM クラスタに統合しています。このタイプの展開には次のベスト プラクティスが当てはまります。

- 企業境界ファイアウォールで、次のポートをブロックします。
  - UDP ポート 135、137、138、および 445
  - TCP ポート 135、139、445、および 593
- ポート ガイドの説明に従って設定されたレイヤ 3 ACL およびレイヤ 4 ACL を展開します。
- 専用の WebView サーバおよび Historical Data Server をインストールして、データベースと Web サービスを分離します。
- アドミン ワークステーション ディストリビュータ（AWD）の数を最小限にし、クライアント AW（データベース不要）および Internet Script Editor クライアントを活用します。
- 親 Unified ICM または子 Unified System CCE セントラル コントローラが地理的に分散しているときには、同じ展開ガイドラインを使用します。
- Windows IPSec を使用して、これらのサーバを管理する Cisco Support Tools Server で Support Tools Node Agent を実行するアプリケーション サーバを認証します。
- イントラサーバ通信を暗号化するように Windows IPSec（ESP）を展開します。メイン CPU に対する暗号化の影響を最小にし、Unified CCE システムでサポートされる負荷レベル（エージェント数、コール レートなど）を維持するために、ハードウェア オフロード ネットワーク カードを使用する必要があります。詳細な図および内容については、「IPSec の展開」（P.8-13）の項を参照してください。

- 地理的に分散したサイト、リモート ブランチ サイト、またはアウトソース サイトの間におけるサイト間 VPN には Cisco IOS IPSec を使用します。

## ネットワーク アドレス変換

Network Address Translation（NAT; ネットワーク アドレス変換）は、ネットワーク ルータ上に常駐する機能で、プライベート IP アドレス割り当ての使用を可能にします。プライベート IP アドレスとは、インターネット上にはルーティングできない IP アドレスのことです。NAT が有効になっているときには、プライベート IP ネットワーク上のユーザは NAT ルータ経由でパブリック ネットワーク上のデバイスにアクセスできます。

NAT が有効になっているルータに IP パケットが到達すると、ルータがプライベート IP アドレスをパブリック IP アドレスで置き換えます。HTTP や Telnet などのアプリケーションの場合は、NAT で問題が発生することはありません。ただし、IP パケットのペイロード内で IP アドレスを交換するアプリケーションの場合は、IP パケットのペイロードに入れて送信される IP アドレスは変換されないために問題が発生します。置き換えられるのは、IP ヘッダー内の IP アドレスだけです。

この問題を解決するために、Cisco IOS ベースのルータおよび PIX/ASA ファイアウォールには、Skinny Client Control Protocol（SCCP; Skinny クライアント コントロール プロトコル）や CTIQBE（TAPI/JTAPI）などのさまざまなプロトコルやアプリケーションに対する「フィックスアップ」が実装されています。このフィックスアップを使用すれば、NAT の処理を実行するときに、ルータがパケット全体を参照して必要なアドレスを置き換えるようになります。この処理が正しく行われるためには、IOS または PIX/ASA のバージョンと Unified CM のバージョンに互換性があることが必要です。

Unified CCE では、CTI OS デスクトップのモニタリングや録音を使用しているとき以外は、NAT を使用した接続性がサポートされています。エージェントの電話の IP アドレスは NAT IP アドレスに見えるので、エージェント デスクトップでは、IP パケットに対して不適切なフィルタリングが行われます。詳細については、次のリンク先にある『*Security Best Practices Guide for ICM and IPCC Enterprise & Hosted Editions*』の「*IPSec and NAT Support*」の項を参照してください。

http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_technical_reference_list.html

# Active Directory の展開

この項では、図 8-2 に示すトポロジについて説明します。Active Directory（AD; アクティブ ディレクトリ）の詳細な展開ガイダンスについては、『*Staging Guide for Cisco ICM/IPCC & Hosted Editions*』を参照してください。このガイドは、次の URL から入手できます。

http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_technical_reference_list.html

Unified ICM システムおよび Unified CCE システムが、専用の Windows Active Directory ドメインに展開されている場合がありますが、これは要件ではありません。これを可能にするのが、組織単位にインストールされるソフトウェア セキュリティ プリンシパルの機能です。このように AD と密接に統合し、セキュリティ委任の権限を行使することで、企業の AD ディレクトリは、アプリケーション サーバ（ドメイン メンバシップ用）、ユーザおよびサービスのアカウント、およびグループを収容するのに使用できます。

## 親 / 子の展開

親 / 子システムは、同じ AD ドメインまたはフォレスト上に展開できますが、完全に異なる AD 環境に展開することも可能です。この展開が一般的となるシナリオは、子 Unified System CCE システムがアウトソース コンタクト センター側に収容される場合です。この場合、親ノードである Gateway PG は

親 AD ドメインのメンバとなります（ワークグループ メンバシップは、サポートはされていますが、管理上の制約により推奨されていません）。このタイプの展開は現在では一般的であり、リモート ブランチ オフィスは、ルータ、Logger、およびディストリビュータがメンバとして所属するセントラル サイトのドメインのメンバとして追加された PG を備えています。

図 8-2 に示すトポロジは、この展開に含まれる 2 つの AD ドメインそれぞれに対する AD 境界、およびアプリケーション サーバがどのドメインに結合されるかを表しています。親 AD ドメイン境界は、セントラル データ センター サイトを超えて拡張され、ACD PG（レガシー サイト）および子 Unified System CCE サイトの Gateway PG に加えて、Unified ICM セントラル コントローラおよび付随するサーバを含みます。子 Unified System CCE サイトおよびその AD 境界は、Unified System CCE サーバをメンバとして持ちます。これは、アウトソーサの企業 AD 環境の一部にすることもしないこともできます。当然、Unified System CCE の専用 AD ドメインにすることもできます。

# AD サイト トポロジ

Unified ICM または Unified CCE が地理的に分散した展開では、各サイトに冗長ドメイン コントローラを配置する必要があり、さらに適切に設定されたサイト間レプリケーション接続を各サイトのグローバル カタログで確立する必要があります。Unified CCE アプリケーションは、それらのサイトに存在する AD サーバと通信する設計になっていますが、そのためにはサイト トポロジが Microsoft のガイドラインに準拠して適切に実装されていることが必要です。

# 組織単位

### 作成されるアプリケーション

Unified ICM ソフトウェアまたは Unified CCE ソフトウェアをインストールするには、サーバがメンバである AD ドメインがネイティブ モードであることが必要になりました。このインストールによって、ソフトウェアの動作に必要な多数の Organizational Unit（OU; 組織単位）オブジェクト、コンテナ、ユーザ、およびグループが追加されます。これらのオブジェクトは、インストール プログラムを実行するユーザに制御が委任された AD 内の組織単位だけで追加できます。OU はドメイン階層内の任意の場所に配置でき、AD 管理者は、Unified ICM/Unified CCE OU 階層を作成および移植できるネストの深さを決定します。

（注）　ローカル サーバのアカウントおよびグループは、アプリケーション サーバ上には作成されません。作成されるグループはすべてドメイン ローカル セキュリティ グループとなり、ユーザ アカウントはすべてドメイン アカウントとなります。サービス ログオン ドメイン アカウントは、アプリケーション サーバのローカル管理者のグループに追加されます。

Unified ICM および Unified CCE のソフトウェア インストールは Domain Manager ツールに統合されています。このツールはソフトウェアが必要とする OU 階層およびオブジェクトをプリインストールするために単独で使用したり、セットアップ プログラムが起動したときに AD 内に同じオブジェクトを作成したりするために使用できます。AD/OU は、実行中のサーバがメンバであるドメイン、または信頼できるドメイン上に作成できます。Cisco Unified System Contact Center（Unified SCC）では、この機能は Unified CCE Machine Initializer によって実現し、デフォルトではマシンの結合したドメインとなり、1 つの入力、つまり <ファシリティ > 名だけを受け取ります。Unified SCC 展開の場合、インスタンス名は常に **ipcc** となります。

AD オブジェクトの作成と Group Policy Objects（GPO）の作成を混同しないでください。標準の Microsoft Security Template フォーマットに従って提供される自動セキュリティ強化は、GPO の設定を介したソフトウェア インストールの一部として AD に追加されることはありません。このカスタマイズされたテンプレート（Unified ICM/Unified CCE アプリケーションの場合）によって提供されるセ

キュリティ ポリシーは、ユーザが強化の適用を選択したときにローカルに適用されますが、提供されるポリシー ファイルの CiscoICM_Security_Template.inf を使用して手動で AD を設定することによって、GPO に適用範囲を拡大することもできます。

### 管理者によって作成される AD

前述のとおり、一部の AD オブジェクトは管理者が作成できます。図 8-2 での主な例としては、OU コンテナである Unified CCE Servers があります。これは、所定のドメインのメンバであるサーバを格納するために手動で追加されます。これらのサーバは、ドメインに結合したら、この OU に移動する必要があります。これによって、ある程度の分離が行われ、だれがサーバを管理できるかまたはできないか（制御の委任）を制御し、さらに重要なことには、OU 内に存在するこれらのアプリケーション サーバがどの AD ドメイン セキュリティ ポリシーを継承できるかまたはできないかを制御できるようになります。

前に説明したように、Unified ICM/Unified CCE サーバは、Microsoft Windows Server 2003 High Security ポリシーをモデルとした、カスタマイズ済みセキュリティ ポリシーを適用して出荷されます。このポリシーは、Group Policy Object（GPO）を介してこのサーバ OU レベルで適用できますが、異なるポリシーはすべて Unified ICM/Unified CCE サーバの OU での継承をブロックする必要があります。OU オブジェクト レベルでの設定オプションである継承のブロックは、高い階層レベルで [Enforced]/[No Override] オプションが選択されたときには無効にできることに注意してください。グループ ポリシーの適用は、最も一般的な基準で始まる十分に検討されたデザインに準拠する必要があり、またこれらのポリシーは階層の適切なレベルだけで制限的となる必要があります。グループ ポリシーを適切に展開する方法の詳細な説明は、『*Windows Server 2003 Security Guide*』を参照してください。このガイドは、次の URL から入手できます。

http://www.microsoft.com/technet/security/prodtech/windowsserver2003/w2003hg/memberserversgch00.mspx

図 8-2　Active Directory およびファイアウォールの展開トポロジ

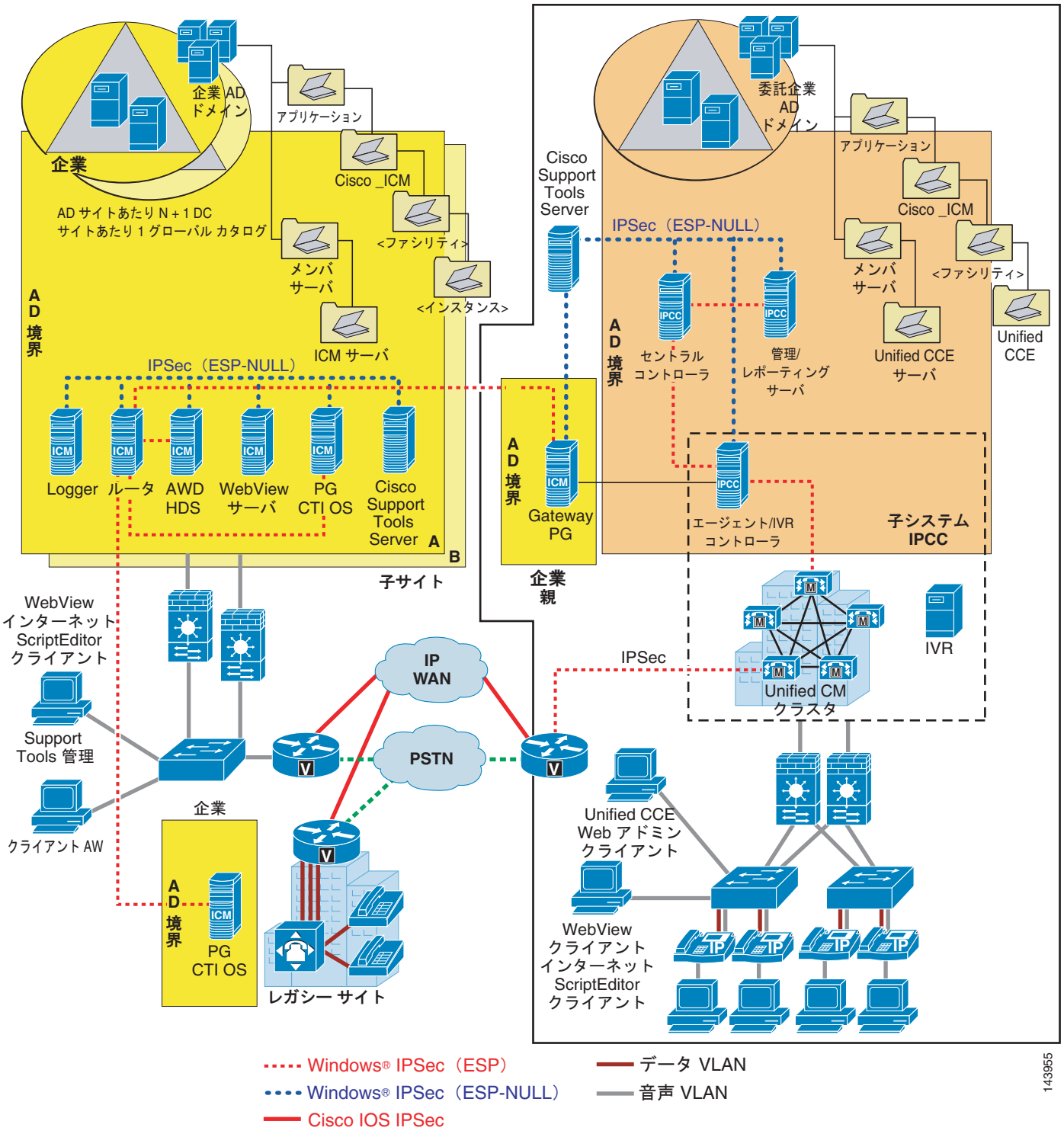


図 8-2 には、次の注が適用されます。

- Cisco_ICM および ipcc 組織単位オブジェクト階層は、アプリケーション インストーラによって作成されます。
- Unified ICM Servers および Unified CCE Servers 組織単位オブジェクトは、AD 管理者が作成し、必要に応じて GPO を介してカスタム Cisco Unified ICM セキュリティ ポリシーを個別に適用する必要があります。
- Flexible Single Master Operation サーバは、Microsoft の推奨事項に従って、該当するサイトのドメイン コントローラに配布する必要があります。

# IPSec の展開

Unified CCE ソリューションは、Microsoft Windows IPSec や Cisco IOS IPSec に基づいて、アプリケーション サーバとサイトの間の重要なリンクを保護します。このソリューションをセキュリティで保護するには、サーバとサイトの間にピアツーピア IPSec トンネルを展開するか、より制限的な事前設定の Network Isolation IPSec ポリシーを展開するか、またはこれら両方を組み合わせて使用します。ピアツーピア IPSec 展開では、Microsoft が提供するツールを使用して、セキュリティで保護する必要がある各通信パスを手動で構成する必要があります。一方、Network Isolation IPSec ポリシーは、Network Isolation IPSec ユーティリティを使用することにより各サーバで自動的に展開でき、例外を作成しない限り、サーバとの間のすべての通信パスがセキュリティで保護されます。Network Isolation IPSec ユーティリティは、すべての Unified CCE 7.5 サーバにデフォルトでインストールされ、Unified CCE 7.0、7.1、および 7.2 リリースではダウンロードして利用できます。

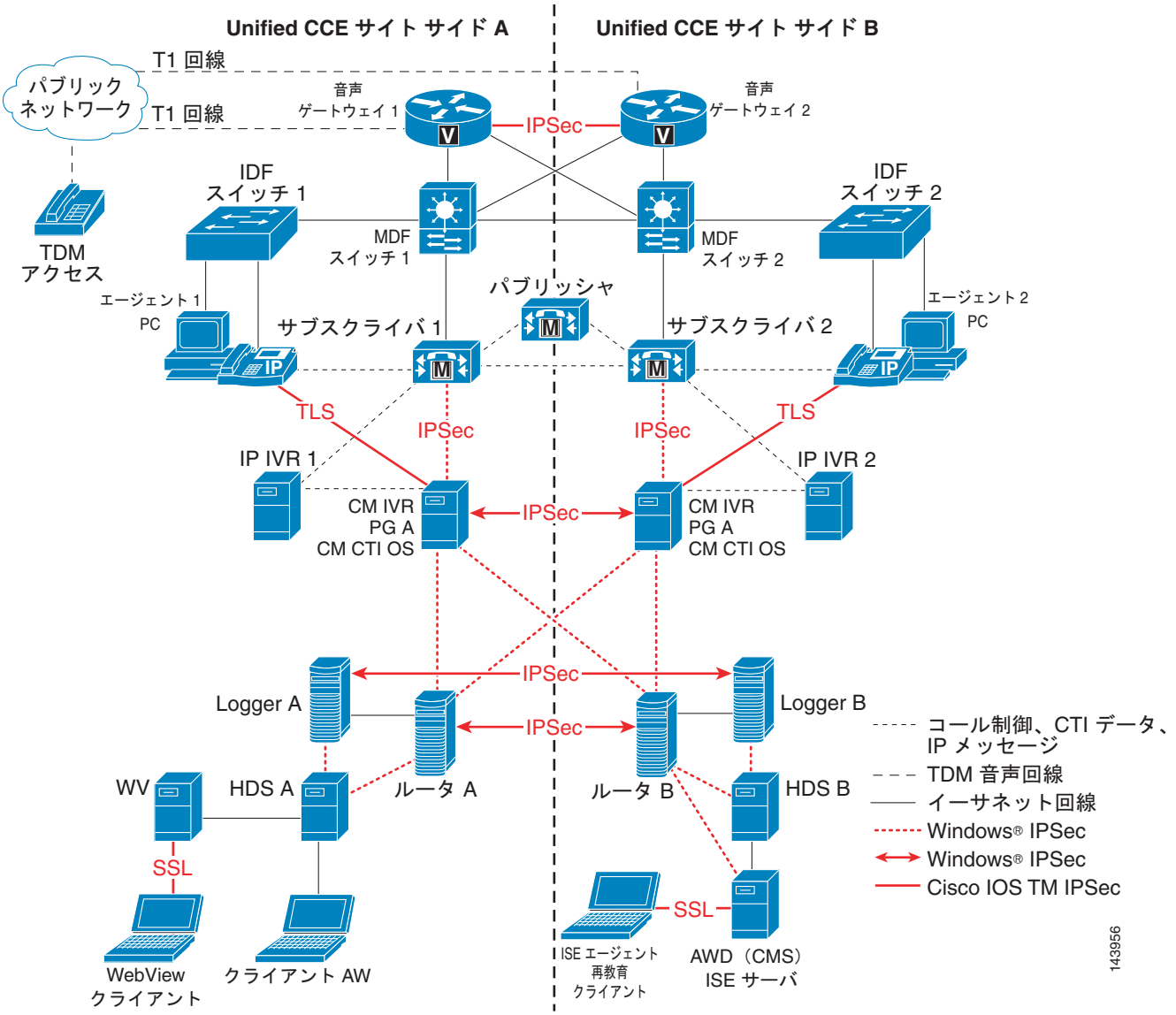
詳細については、次の URL にある『*Security Best Practices Guide for ICM and IPCC Enterprise & Hosted Editions*』を参照してください。

http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_technical_reference_list.html

『*Security Best Practices Guide*』には、サポートされるパスだけでなく、推奨設定などを含めて、ユーザが Windows IPSec を展開するときに役立つ情報も記載されています。

図 8-2 に、IPSec がサポートされる多数の接続パスを示します。図 8-3 は、この章で記載したガイドラインを示し、Windows IPSec または Cisco IOS IPSec のいずれかによる保護が必要なさまざまなサーバの相互接続を示しています。この図は、SSL および TLS をサポートする多数のパスも示しています。TLS サポートの詳細については、「エンドポイント セキュリティ」（P.8-20）の項を参照してください。

図 8-3　IPSec の展開例




# ホスト ベース ファイアウォール

ネットワークの最も内側のレイヤでホスト ファイアウォール プロテクションを実施することによって、Windows Server 2003 Service Pack 1（SP1）で導入された新しいセキュリティ コンポーネントである Windows ファイアウォールは、多層防御セキュリティ戦略の一部として効果的に機能します。Unified CCE は、アプリケーション サーバ上での Windows ファイアウォールの展開をサポートしています。『*Security Best Practices Guide*』には、この機能の実装および設定に関する章があります。

このドキュメントで説明した多数のセキュリティ レイヤを搭載した統合システムを設計するうえで、Windows ファイアウォールと Cisco Security Agent（CSA）の間には互換性に制限があることに注意する必要があります。CSA の詳細については、「Cisco Security Agent」（P.8-17）の項、および『*Cisco Security Agent Installation/Deployment Guide for Cisco Unified ICM/CCE & Hosted Editions, Release 7.1*』を参照してください。

**注意**　Unified ICM 7.1 に付属する Cisco Security Agent（CSA）バージョン 4.5 は、Windows Server 2003 SP1 上で Windows ファイアウォールが同時に実行されるときには、Windows ファイアウォールを無効にします。Windows ファイアウォールが最後のシステム起動以降に有効になり、Cisco Unified ICM Firewall Configuration Utility（CiscoICMfwConfig）を使用して設定されている場合でも、システムが再ブートされるたびに無効になります。

企業で Cisco Security Agent と Windows ファイアウォールの両方を展開する場合は、Active Directory を使用して、Windows ファイアウォール グループ ポリシー設定を使用する Windows ファイアウォールを有効にする必要があります。Unified CCE アプリケーションには AD インフラストラクチャが必要となるため、CSA が Windows ファイアウォールとともに展開されたときに、Windows ファイアウォールを有効にするグループ ポリシーを使用する必要があります。

Windows ファイアウォールが CSA とともにインストールされたときに、Windows ファイアウォールを有効にするための AD グループ ポリシー設定方法の詳細は、『*Field Notice: FN-62188 – Cisco Unified ICM Enterprise and Hosted Contact Center Products Notice for Cisco Security Agent 4.5.1.616 Policy 2.0.0*』を参照してください。この資料は、次の URL から入手できます。

http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_field_notices_list.html

例外の設定およびアプリケーションで必要となるポートのオープンは、Unified CCE アプリケーションに付属する Windows Firewall Configuration Utility を使用してローカルに設定されます。

Windows Firewall Configuration Utility（CiscoICMfwConfig）は、設定ファイル（CiscoICMfwConfig_exc.xml）を使用して、どのポート、アプリケーション、またはサービスを Windows ファイアウォールで有効にするかを決定します。管理モードで CSA を展開するときには、CSA Management Center（MC）との通信が必要となるため、MC を CSA Agent に接続するために使用するデフォルトの UDP ポートを追加するように、このファイルを変更することが重要です。この変更は、Configuration Utility を実行する前に行う必要があります。設定ファイルの Ports XML 要素には、必要に応じて次の行を追加します。

```
<Ports>
..
<Port Number="5401" Protocol="UDP" Name="ManagedCSA" />
</Ports>
```

Windows ファイアウォールは、Windows Firewall Control Panel Applet を使用するか、またはコマンドラインから次のコマンドを使用して、ポートの例外を直接追加して設定することもできます。

```
netsh firewall add portopening protocol = UDP port = 5401 name = ManagedCSA mode = ENABLE
scope = ALL profile = ALL
```

Windows ファイアウォールの詳細については、『*Windows Firewall Operations Guide*』を参照してください。このガイドは、次の URL から入手できます。

http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/Operations/c52a765e-5a62-4c28-9e3f-d5ed334cadf6.mspx

# サーバ セキュリティの設定

## Unified Contact Center セキュリティ ウィザード

Unified Contact Center セキュリティ ウィザードを使用すると、上述した自動セキュリティ強化、Windows ファイアウォール設定、および Network Isolation IPSec ポリシー展開の 3 つのセキュリティ機能を容易に設定できます。セキュリティ ウィザードは、これら 3 つのユーティリティの機能を使いやすいウィザード風のインターフェイスにカプセル化し、セキュリティ機能の設定に関する手順をユーザにガイドします。セキュリティ ウィザードは、Network Isolation IPSec ポリシーを展開する場合に特に便利であり、推奨されるアプローチでもあります。セキュリティ ウィザードは、すべての Unified CCE 7.5 サーバにデフォルトでインストールされ、Unified CCE 7.0、7.1、および 7.2 リリースではダウンロードして利用できます。『*Security Best Practices Guide*』には、セキュリティ ウィザードについて詳しく説明した章があります。

# ウイルス保護

## ウイルス対策アプリケーション

Unified CCE システムでは、多くのサードパーティのウイルス対策アプリケーションがサポートされます。Unified CCE ソフトウェアの特定のリリースでサポートされるアプリケーションおよびバージョンのリストについては、『*Hardware and System Software Specifications Guide*』（以前の『*Bill of Materials*』）および『*Cisco Voice Portal Bill of Materials*』、ならびにサポートされるアプリケーションに対応する Cisco Unified CCX および Unified CM の製品マニュアルを参照してください。

（注）　お客様の環境でサポートするアプリケーションだけを展開します。特に、Unified CCE システムに Cisco Security Agent などのアプリケーションがインストールされている場合、サポートしないアプリケーションを展開すると、ソフトウェアの競合が発生する場合があります。

## 設定ガイドライン

ウイルス対策アプリケーションには多数の設定オプションが用意されます。これらを使用すると、サーバ上でどのデータをどのようにスキャンするのかを詳細にコントロールできます。

どのウイルス対策製品を使用する場合でも、スキャンとサーバ パフォーマンスのバランスを取るために設定を行います。スキャンの実行を選択すればするほど、潜在的なパフォーマンス オーバーヘッドが大きくなります。システム管理者の役割は、特定の環境内でウイルス対策アプリケーションをインストールするための、最適な設定要件を判断することです。Unified ICM 環境における、より詳細な設定情報のために、『*Security Best Practices Guide*』および特定のウイルス対策製品マニュアルを参照してください。

次のリストでは、一般的なベスト プラクティスの一部を取り上げます。

- サードパーティ ウイルス対策アプリケーションの最新サポート バージョンへアップグレードします。前のバージョンと比較して、より新しいバージョンではスキャン速度が改善され、サーバでのオーバーヘッドはより小さくなります。

- リモート ドライブ（ネットワーク マッピングまたは UNC 接続など）からアクセスされているファイルに対するスキャンを回避します。可能な場合、これらの各リモート マシンにはそれぞれ独自のウイルス対策ソフトウェアをインストールして常にローカルでスキャンを実行するようにします。多層なウイルス対策戦略において、ネットワーク全体でのスキャンおよびネットワーク ロードへの追加は必須ではありません。
- 従来のウイルス対策スキャンと比較してヒューリスティックス スキャンではより大きなスキャン オーバーヘッドが発生するため、信頼性の保証のないネットワーク（電子メールおよびインターネット ゲートウェイなど）からのデータ入力における重要な状況でだけ、この先進のスキャン オプションを使用します。
- リアルタイムまたはアクセス時のスキャンを有効にすることは可能ですが、その対象を着信ファイルだけにします（ディスクへの書き込み時）。これは、ほとんどのウイルス対策アプリケーションにとってのデフォルト設定です。ファイルの読み出しへのアクセス時のスキャンの実装は、高パフォーマンス アプリケーション環境において、システム リソースに対して必要以上に大きな影響を与えます。
- すべてのファイルに対する手動およびリアルタイム スキャンでは、最適な保護が提供される一方、この設定では、悪意あるコード（たとえば、ASCII テキスト ファイル）のサポートが不可能なファイルに対するスキャンによるオーバーヘッドが発生します。すべてのスキャン モードにおいて、システムを危険にさらすことがないと認識されているファイルまたはファイルのディレクトリを除外することが推奨されます。次のリンクから入手できる『*Security Best Practices for Cisco Intelligent Contact Management Software*』内で説明されているように、Unified ICM または Unified CCE の実装において特定の Unified ICM ファイルを除外するための推奨事項にも従います。

  http://www.cisco.com/en/US/partner/products/sw/custcosw/ps1001/prod_technical_reference_list.html
- 使用状況が低い時、またアプリケーション アクティビティが最も低い時にだけ、定期的なディスク スキャンの予定を組みます。アプリケーションの削除アクティビティの予定を組むには、上記の項目に掲載された『*Security Best Practices Guide*』を参照してください。

Unified CM のウイルス対策アプリケーションを設定するためのガイドラインは、次のリンクから入手できます。

- http://cisco.com/en/US/partner/products/sw/voicesw/ps556/products_implementation_design_guides_list.html
- http://cisco.com/en/US/partner/products/sw/voicesw/ps556/products_user_guide_list.html

# 侵入防御

## Cisco Security Agent

Cisco Security Agent では、脅威に対する保護がサーバ（エンドポイントとしても知られる）に提供されます。悪意ある動作が識別され、回避されます。これにより、既知および未知（「デイ ゼロ」）のセキュリティ リスクが排除され、運用費の削減が促進されます。Cisco Security Agent では、ホスト侵入防御、分散型ファイアウォール機能、悪意あるモバイル コードに対する保護、オペレーティング システムの整合性保証、および監査ログ統合を（管理モードで）単一の製品内ですべて提供することにより、複数のエンドポイントのセキュリティ機能が集約され、拡張されます。

ウイルス対策アプリケーションとは異なり、Cisco Security Agent ではシグニチャの一致を信頼するのではなく、動作が解析されます。ただし、これらは両方とも、ホスト セキュリティに対する多層な対策のための常に重要なコンポーネントです。Cisco Security Agent は、ウイルス対策アプリケーションの代替としては認識されません。

Cisco Security Agent の Unified CCE コンポーネント上での展開には、多くのアプリケーション互換エージェントの取得と、希望するモードに従ったそれらの実装を伴います。

（注）　Unified CCE 用の Cisco Security Agent ポリシーは、サーバに限定されており、Agent Desktop においては展開しないでください。お客様は選択により、企業内に CSA 製品を展開し、展開された Agent Desktop ソフトウェアのアクティビティを含めて、デスクトップ エンドポイント上で正当なアプリケーション アクティビティを許可するように、Management Center 内のデフォルトのデスクトップ セキュリティ ポリシーを修正できます。

## エージェント モード

Cisco Security Agent は、次の 2 種類のモードで展開が可能です。

- スタンドアロン モード：スタンドアロン エージェントは、各音声アプリケーションの Cisco Software Center から直接的に取得できます。また、セントラルの Cisco Security Agent Management Center（MC）への通信機能を必要とせずに実装できます。
- 管理モード：エージェントに固有であり、展開されたソリューション内の各音声アプリケーションと互換性のある XML エクスポート ファイルを同じ場所からダウンロードし、Cisco Unified Operations VPN/Security Management Solution（VMS）バンドルの一部である Cisco Security Agent のための既存の Cisco Unified Operations Management Center にインポートできます。

Cisco Security Agent のための先進の Cisco Unified Operations Management Center では、エージェントのためのすべての管理機能がコアの管理用ソフトウェアに統合されます。このコアの管理用ソフトウェアでは、ポリシーの定義と配布、ソフトウェア アップデートの提供、およびエージェントへの通信の維持が一元化された手段が提供されます。この役割ベースの、Web ブラウザによる場所を選ばない管理アクセスを使用すると、管理センター 1 か所につき何千も存在するエージェントに対する管理者のコントロールが容易になります。

Cisco Unified ICM、Unified CCE、および Cisco Voice Portal のエージェントは、次の URL から入手できます。

http://www.cisco.com/kobayashi/sw-center/contact_center/csa/

その他の音声アプリケーション エージェントは、次の URL から入手できます。

http://www.cisco.com/public/sw-center/sw-voice.shtml

## サードパーティ アプリケーションの依存関係

Cisco Security Agent は、『*Hardware and System Software Specification Guide*』またはインストールしている Cisco Security Agent のインストール ガイドに記載されている、サポートされているアプリケーションと同じサーバ上にだけ配置できます。Cisco Unified ICM エージェントのインストールの詳細については、『*Cisco Security Agent Installation/Deployment Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*』を参照してください。この資料は、次のリンクから入手できます。

http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_installation_and_configuration_guides_list.html

（注）　シスコは、Sygate、McAfee などのベンダーが提供するその他の侵入防御製品についてはテストやサポートを行いません。これらの製品は、正当なアプリケーションをセキュリティに対する脅威として、もし誤って識別すると、アプリケーションの機能性をブロックすることがあります。CSA の場合と同様に、これらの製品は正しい動作を実行するように設定する必要があります。

# パッチ管理

## セキュリティ パッチ

コンタクト センター製品のためのセキュリティ アップデート認定プロセスは、次のリンクにおいて文書化されています。

http://www.cisco.com/en/US/prod/collateral/voicesw/custcosw/ps5693/ps1844/product_bulletin_c25-455396.html

この手順は、カスタマイズされた Cisco Unified Communications Operating System（CIPT OS）ではなく、標準の Windows オペレーティング システムを実行するアプリケーション サーバに適用されます。

Microsoft から重大または重要なセキュリティ アップデートがリリースされると、シスコは Unified ICM ベースのアプリケーションに対する影響を判断します。影響があると区分されたセキュリティ アップデートに対しては、シスコは自社の製品に対するテストを続け、潜在的な競合があるかどうかをより詳細に判断します。影響評価速報は、通常は Microsoft がセキュリティ アップデートをリリースした数日後に公開されます。この影響評価速報は、次の URL の IntelliShield Event Responses にあります。

http://www.cisco.com/security

これらのアップデートをいつどのように適用するのかについては、お客様は Microsoft のガイドラインに従う必要があります。Microsoft からリリースされたすべてのセキュリティ パッチをコンタクト センターのお客様が個別に判断し、お客様の環境に適切であると判断されたパッチをインストールすることが推奨されます。より深刻な重大度を持つセキュリティ パッチを個別に判断するサービス、また必要に応じて、これらのセキュリティ パッチを検証するサービスの提供をシスコは継続します。コンタクト センターのソフトウェア製品には、より深刻な重大度を持つセキュリティ パッチが適切な場合があります。

Unified CM Operating System で動作するすべてのアプリケーション サーバについては、『*Cisco Unified CallManager Security Patch Process*』を参照してください。この資料は、次の URL から入手できます。

http://www.cisco.com/application/pdf/en/us/guest/products/ps556/c1167/ccmigration_09186a0080157c73.pdf

シスコがサポートするオペレーティング システム ファイル、SQL Server、およびセキュリティ ファイルの追跡については、『*Cisco IP Telephony Operating System, SQL Server, Security Updates*』を参照してください。この資料は、次の URL から入手できます。

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/win_os/os_srv_sec/osbios.htm

Unified CM のセキュリティ パッチおよび Hotfixes ポリシーでは、重大度 1 または重大であると判断された適用可能なパッチは、Hotfixes として 24 時間以内にテストされ、http://www.cisco.com に掲載される必要があると指定されています。すべての適用可能なパッチは、1 か月に一度、増分のサービス リリースとして統合して掲載されます。

新規の修正ファイル、OS アップデート、および Unified CM と関連製品のためのパッチを自動的に通知する通知ツール（電子メール サービス）は、次のリンクから利用できます。

http://www.cisco.com/cgi-bin/Software/Newsbuilder/Builder/VOICE.cgi

## 自動パッチ管理

Unified CCE サーバ（CIPT OS にインストールされたアプリケーションを除く）では、Microsoft の Windows Server Update Services との統合がサポートされます。これにより、お客様はこれらのサーバにどのパッチをいつ展開できるかを管理します

アップデートは選択的に承認し、稼動中のサーバにいつ展開するか決定することをお勧めします。Windows Automatic Update Client（デフォルトですべての Windows ホストにインストールされる）は、デフォルトの Windows アップデート Web サイトの代わりに、Microsoft Window アップデート サービスが稼動するサーバとポーリングすることによって、アップデートを取得するように設定できます。

設定および展開の詳細な情報については、『*Deployment Guide*』および次のサイトでその他のステップ バイステップ ガイドを参照してください。

http://www.microsoft.com/windowsserversystem/updateservices/default.mspx

このトピックについては、『*Security Best Practices Guide for Cisco Unified ICM/CCE & Hosted Editions, Release 7.x*』で追加情報が入手できます。

（注）　現在、Cisco Unified Communications Operating System の設定およびパッチ プロセスでは、自動パッチ管理プロセスを使用できません。

# エンドポイント セキュリティ

## エージェント デスクトップ

CTI OS（C++/COM ツールキット）および CAD エージェント デスクトップはともに、サーバへの TLS 暗号化をサポートします。この暗号化によって、エージェントのログインおよび CTI データをスヌーピングから保護します。相互認証メカニズムは、認証、鍵交換、ストリーム暗号化に使用される暗号スイートで合意するために、CTI OS のサーバとクライアントに対して実装されました。使用される暗号スイートは、次のとおりです。

- プロトコル：SSLv3
- 鍵交換：DH
- 認証：RSA
- 暗号化：AES（128）
- メッセージ ダイジェスト アルゴリズム：SHA1

図 8-4 は、暗号化の実装における、エージェント デスクトップ上およびサーバ上での X.509 認証の使用を示しています。この実装は、最も強固にセキュリティで保護された展開のために、公開キー インフラストラクチャ（PKI）との統合をサポートしています。デフォルトでは、アプリケーションは、クライアントおよびサーバのリクエストの署名に使用される自己署名証明書（CA）をインストールし、

これを使用します。ただし、シスコはサードパーティの CA との統合をサポートしています。企業で管理する CA または Verisign などの外部認証局によってセキュリティが向上するため、このような統合が好ましい方法です。

**図 8-4　セキュア エージェント デスクトップ（証明書ベースの相互認証）**

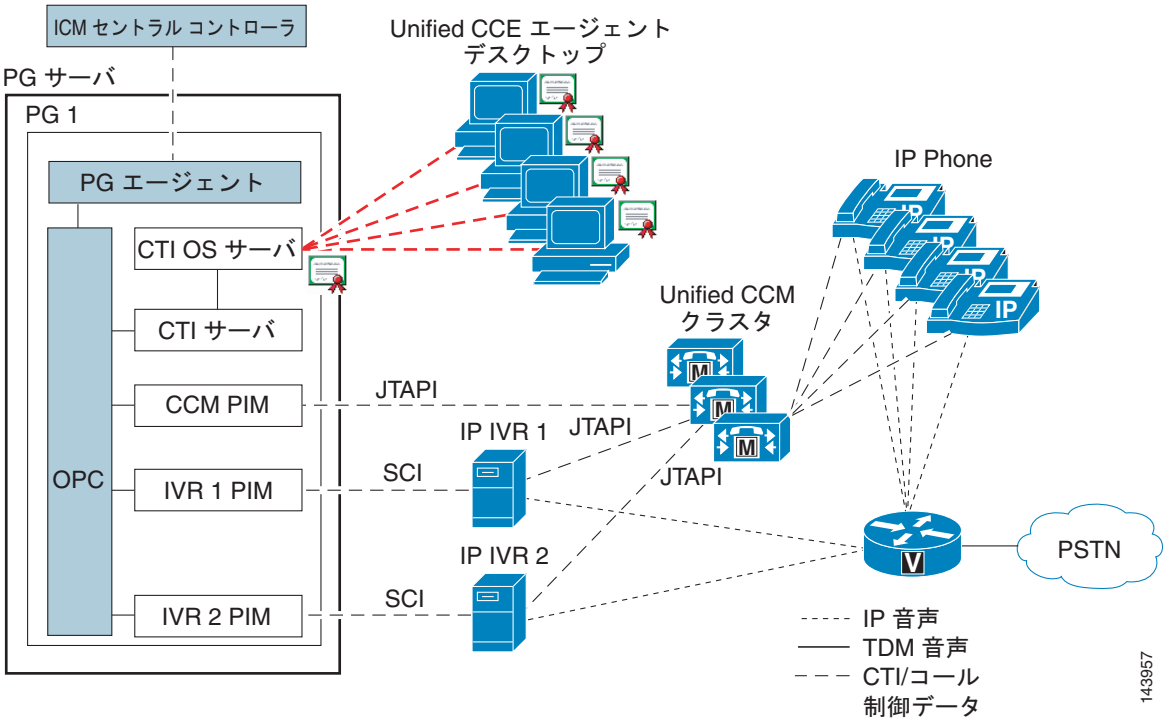
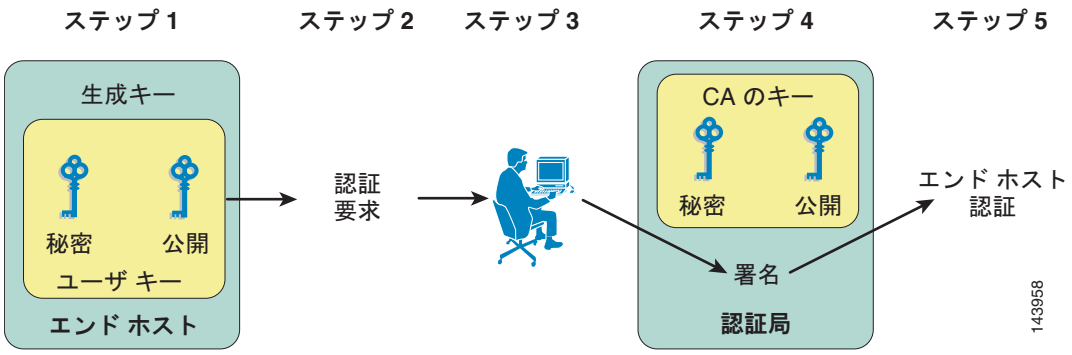



図 8-5 は、エージェントおよびサーバによって使用される証明書を生成する認証局の登録手順を示します。エージェント デスクトップ証明書の登録手順は手動で行われるため、各エンドポイントで証明書署名要求（CSR）を作成する必要があります。これらの証明書署名要求は、証明書の署名および生成を担当する認証局に転送されます。

**図 8-5　認証局の登録手順**



# Unified IP Phone デバイスの認証

Unified CM Release 4.*x* または 5.0 に基づいて Unified CCE ソリューションを設計する場合、お客様は Cisco Unified IP Phone 7940、7960、または 7970 に対するデバイス認証を選択して実装できます。Unified CCE 7.0 は、Unified CM の認証デバイス セキュリティ モードでテストされており、それによって次のことを保証します。

- デバイス アイデンティティ：RSA シグニチャを使用した相互認証
- シグナリング インテグリティ：HMAC-SHA-1 を使用して認証された SCCP メッセージ
- シグナリング プライバシー：AES-128-CBC を使用して暗号化された SCCP メッセージ コンテンツ

# Unified IP Phone のメディア暗号化

Unified CCE ではメディア暗号化を使用できます。ただし、サイレント モニタリング機能は使用できなくなります。また、録音システムを展開している場合は、録音システムのベンダーに連絡して、Secure Real-Time Transport Protocol（SRTP）を使用した環境での録音のサポートを確認してください。

# IP Phone の強化

Unified CM の IP Phone デバイス設定は、電話機の PC ポートを無効にしたり、PC から音声 Virtual Local Area Network（VLAN; バーチャル ローカル エリア ネットワーク）へのアクセスを制限するなど、電話機機能の多くを無効にして電話機を強化する機能を提供します。また、これらの設定の一部を変更しても、Unified CCE ソリューションのモニタリングまたは録音の機能が無効になります。設定は次のように定義されます。

- PC 音声 VLAN アクセス
  - PC ポートに接続されたデバイスによる音声 VLAN へのアクセスを許可するかどうかを示します。音声 VLAN アクセスを無効にすると、接続された PC による音声 VLAN 上でのデータの送受信が回避されます。また、電話によって送受信されるデータの PC による受信も回避されます。この機能を無効にすると、デスクトップベースのモニタリングおよび録音が無効になります。
  - 推奨設定：有効（デフォルト）
- PC ポートへのスパン
  - 電話機が、電話機ポート上で送信または受信したパケットを PC ポートに転送するかどうかを示します。この機能を使用するには、PC 音声 VLAN アクセスが有効になっていることが必要です。この機能を無効にすると、デスクトップベースのモニタリングおよび録音が無効になります。
  - 推奨設定：有効

展開されたサードパーティのモニタリングおよび/または録音アプリケーションが、音声ストリームの取り込みにこのメカニズムを使用している場合を除いて、次の設定を無効にして中間者（MITM）攻撃を防止する必要があります。CTI OS のサイレント モニタリング機能および CAD のサイレント モニタリングおよび録音は、Gratuitous ARP に依存しません。

- Gratuitous ARP
  - 電話機が Gratuitous ARP 応答から MAC アドレスを認識するかどうかを示します。
  - 推奨設定：無効