ソリューションのセキュリティ

セキュリティの概要

Contact Center Enterprise ソリューションのセキュリティを実現するには、アクセス、接続、要件そしてシステム管理を正確に定義する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により、使用可能なシスコの技術を使用して、データセンターのリソースを内部および外部の攻撃から保護できます。セキュリティ対策により、データプライバシー、整合性、およびシステムの可用性が確保されます。

Contact Center Enterprise ソリューションのセキュリティに関する考慮事項は、Cisco Unified Communications ソリューションの別のアプリケーションの考慮事項と類似しています。Contact Center Enterprise ソリューションは、非常にさまざまで、複雑なネットワーク設計を必要とすることがよくあります。これらの展開では、レイヤ 2 およびレイヤ 3 ネットワーキングまた、音声、VPN、QoS、Microsoft Windows Active Directory、その他のネットワーキングの問題への適性が必要です。この章では、これらのエリアについてのガイダンスの一部を説明します。ただし、これは安全なコンタクトセンターの展開に関してすべてが記載されたガイダンスではありません。

Unified Communications Security Solution ポータルと一緒に、http://www.cisco.com/c/en/us/solutions/enterprise/design-zone/index.html に記載されている「設計ゾーン」 の設計ドキュメントを使用します。これらのドキュメントは、Cisco Unified Communications 用のネットワーク インフラストラクチャの適切な構築に関する情報を提供します。特に、セキュリティおよび Cisco Unified Communications に関する関連ドキュメントを参照してください。

- *Cisco Unified Communications Manager* に基づいた *Cisco Unified Communications SRND*

- データセンターネットワーク：サーバファームセキュリティ *SRNDv2*
- サイト間 *IPSec VPN SRND*
- 音声およびビデオに対応した *IPSec VPN*（*V3PN*）*SRND*
- *Business Ready Teleworker SRND*

これらのドキュメントの更新や追加は定期的に行われるので,頻繁に「設計ゾーン」を参照してください。

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。詳細については、Microsoft の次のトピックを参照してください。

- 新しい Active Directory 論理構造の設計
- Active Directory の初回展開
- 既存の Windows 環境から Microsoft Windows サーバ 2012 R2 Active Directory へのアップグレード
- 現在の環境を Windows Active Directory 環境に強化

特に 、「Microsoft Windows サーバ 2012 R2」の「ディレクトリおよびセキュリティサービスの設計と展開」項を参照してください。この項は、組織のすべての Active Directory の設計と導入の目標を達成するために役立ちます。https://technet.microsoft.com/library/hh801901.aspx で Microsoft TechNet の項目を参照してください。

セキュリティレイヤ

適切に安全なソリューションを提供するには、さまざまな脅威から保護する多層化されたアプローチが必要です。

次のセキュリティ層を実装し、セキュリティ層のポリシーを確立します。

- **物理セキュリティ** —コンタクトセンターのアプリケーションをホストするサーバが物理的に安全であることを確認します。権限を持つ担当者のみがアクセスできるデータセンター内のサーバを見つけ出します。また、ケーブル接続用のプランタ、ルータ、スイッチへのアクセスも制御します。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のような技術も含まれます。
- **境界セキュリティ** —安全なデータネットワークの設計や展開は複雑な情報カテゴリです。このガイドでは、Contact Center Enterprise ソリューションに対して効果な境界セキュリティを確立するリソースへの参照を提供します。
- **データセキュリティ** — カスタマーの個人情報の盗聴を保護するレベルを向上させるため、Contact Center Enterprise ソリューションは、エージェントデスクトップで Transport Layer Security（TLS）をサポートします。また、サーバ間の通信チャネルを保護するための IPSec もサポートしています。

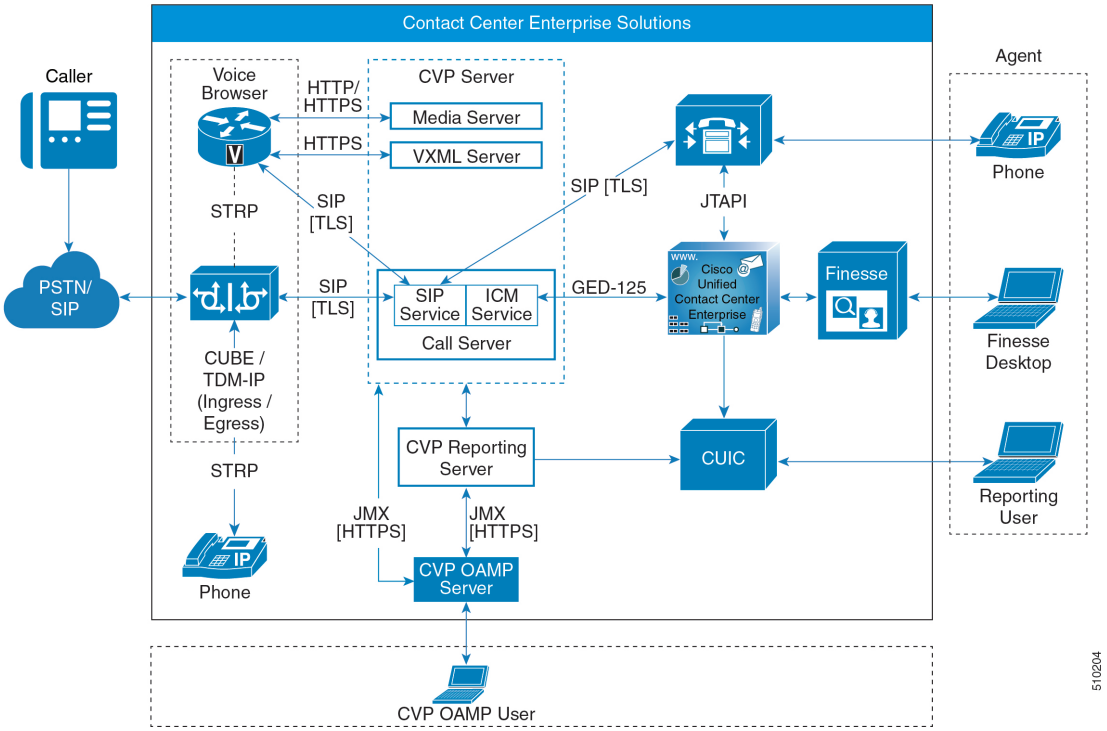
Note Contact Center Enterprise ソリューションは、デフォルトで TLS 1.2 を使用します。ほとんどのコンポーネントでは、必要に応じて以前のバージョンの TLS を有効にすることができます。

- **ホスト ベース ファイアウォール** — Windows ファイアウォールを使い、一方的な着信トラフィックで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します。VM の Windows ファイアウォール構成ユーティリティを使用して、Windows サーバ 2012 R2 のファイアウォール コンポーネントと統合します。
- **ウイルス保護**—最新のウイルス定義ファイル（日次更新がスケジュールされている）を備えたウイルス対策アプリケーションをすべての VM で実行します。テスト済みおよびサポートされているすべてのウイルス対策アプリケーションの一覧については、ソリューションの「互換性マトリックス」を参照してください。
- **パッチ管理**—すべてのセキュリティ更新を適用せずにソリューションをライブネットワークに接続しないでください。Microsoft（Windows、SQL サーバ、Internet Explorer など）およびその他のサードパーティ製のセキュリティパッチを使用して、すべてのホストを最新の状態に保ちます。http://www.cisco.com/c/en/us/products/collateral/customer-collaboration/unified-contact-center-enterprise/product_bulletin_c25-455396.htmlで、サードパーティ製のパッチ管理ポリシーを参照してください。

これらのセキュリティ層の大半については、Contact Center Enterprise ソリューションが複数の機能をサポートしています。ただしシスコは、企業ポリシー、安全なソリューションの展開や維持の手順に関して、管理または強制はできません。

セキュアなシグナリングおよびメディアの設計と構成

TLS-SRTP は、CallServer で SIP 信号と RTP の暗号化をサポートします。この図は、包括的な展開モデルを説明しています。



導入モデル

1. **Unsecured**

   この展開モデルは、CVP および VVB の以前のリリースのモデルです。操作は以前と同じようにレンダリングされます。これは、既存のソリューションに対して影響のない展開です。

2. **セキュア シグナリングのみ**

   この展開モデルでは、セキュリティで保護されていないモデルにシグナリング セキュリティが導入されます。操作が強化され、コール セットアップ用の SIP が保護されます。これにより、音声が聞こえる前のすべてのデータ交換がセキュアな方法で行われます。

3. **エージェント コールのメディア セキュリティを使用したセキュア シグナリング**

   この展開モデルは、シグナリング セキュリティをサポートし、発信者とエージェント間のメディアとオーディオのセキュリティをさらに追加します。発信者と企業内の IP ネットワークを介して伝送されるエージェント間の音声コンテンツは、ハッキングやスヌーピングに対して耐性があります。

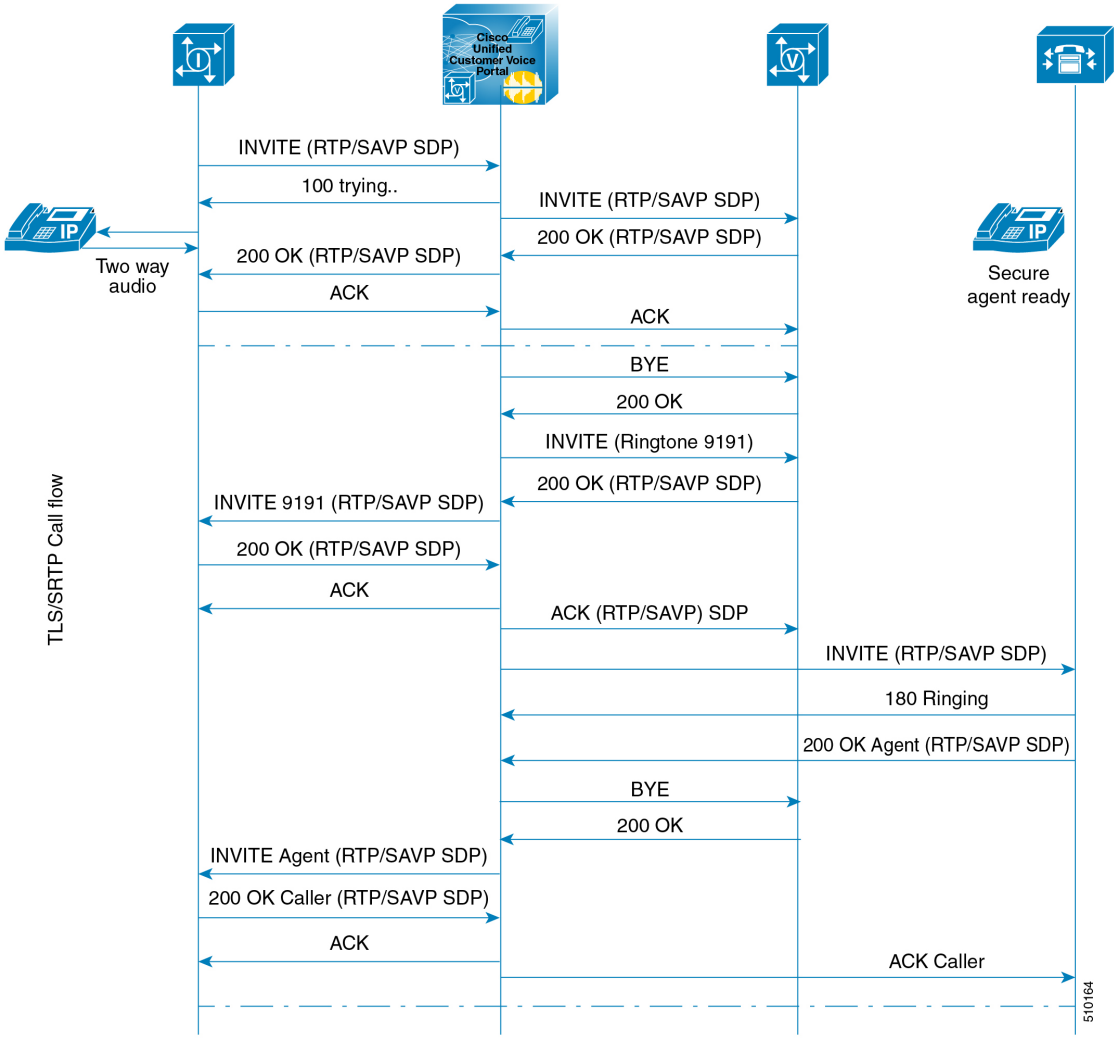
4. **IVR およびエージェント コールのエンドツーエンド メディア セキュリティを使用したシグナリング**

   この展開モードは、コールに対する完全なセキュリティ保護を提供します。これにより、シグナリングが保護されるだけでなく、発信者から IVR へのメディアと音声、およびエージェントも保護されます。

Note

- TLS / SRTP展開の場合：
  - CVP と VVB が G711 mu-law であり、すべてのエージェントが G729 である場合、Unified CM は、ウィスパー アナウンス レッグでのセキュアなトランスコーディングをサポートしません。セキュアなトランスコーディングをサポートする回避策として、G729 の VVB を使用してアナウンスを再生します。

通話フロー



メディア暗号化（SRTP）の考慮事項

展開で SRTP を有効にする前に以下を考慮してください。

- エージェントレグで安全なメディアを使用するには、インストール済みの IP 電話が SRTP と互換性があることを確認してください。
- 仮想化音声ブラウザは、VRU レグの SRTP をサポートします。
- IOS VXML ゲートウェイは SRTP をサポートしません。
- モバイルエージェントは SRTP を使用できません。
- Cisco アウトバウンドオプション ダイヤラは SRTP をサポートしません。コールがダイヤラに接続されている間、コールは SRTP を使用できません。ただし、コールがダイヤラに接続されなくなると SRTP とネゴシエートできます。

プラットフォームの違い

Contact Center Enterprise ソリューションは、管理方法が異なる複数のアプリケーションサーバで構成されています。プライマリサーバは、中核的なコンポーネント向けです。これらサーバは、標準規格の（デフォルト）オペレーティングシステムのインストレーションのみにインストールします。Windows サーバ 2012 R2 にインストールしたコンポーネントには、Windows サーバソフトウェアのデフォルトリテールバージョンのみを使用します。最新のデバイスドライバ、セキュリティアップデートなどによって、オペレーティングシステムを最新の状態に保ちます。

Unified Communications Manager（Unified CM）などの一部のサーバは、Cisco Voice Operating System（VOS）で実行されます。シスコから該当するすべてのパッチオペレーティングシステムの更新を入手します。このオペレーティングシステムのセキュリティ強化仕様に関しては、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html の「『*Cisco Collaboration System Solution Reference Network Designs*』」および別の Unified CM 製品ドキュメントを参照してください。

適切なセキュリティはサーバによって異なります。これらのサーバを環境内で設計、導入、および保守する場合は、次の点に留意します。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。

セキュリティ設計要素

Unified CCE には http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-configuration-examples-list.html で *Cisco Unified ICM/Contact Center Enterprise* セキュリティ ガイドがあります。そのガイドでは、この章の情報について説明されています。このガイドでは、セキュリティの実装の詳細と、Unified CCE 展開のセキュリティ確保に関する一般的なガイダンスについて説明します。セキュリティ機能には、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構成

- 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
- Microsoft Baseline Security Analysis
- 監査
- ウイルス対策ガイドライン
- セキュアなリモート管理
- シングル サインオン

ガイドラインは、Microsoft や他のサードパーティベンダーによって発表された強化ガイドラインの一部に基づいています。このガイドは、製品内のほとんどのセキュリティ機能の基準点として機能します。このガイドでは、さまざまな Contact Center Enterprise ツールにバンドルされている Automated OS および SQL Security Hardening のインストレーションに関して説明します。

その他のセキュリティ機能

Table 1: その他のセキュリティドキュメント

セキュリティに関するトピック	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	*Cisco Unified ICM/Contact Center Enterprise* ステージング ガイド at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html
SNMPv3 の認証および暗号化	*Cisco Unified ICM/Contact Center Enterprise SNMP* ガイド at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-configuration-examples-list.html
機能制御（ソフトウェアアクセス制御）	*Cisco Unified ICM/Contact Center Enterprise* コンフィギュレーション ガイド at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-configuration-examples-list.html
リアルタイムクライアントの検証	*Cisco Unified ICM* セットアップおよびコンフィグレーション ガイド at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html

ネットワーク ファイアウォール

ソリューション用のファイアウォールを展開する際は、いくつかの検討すべき要素があります。Demilitarized Zone（DMZ; 緩衝地帯）ではコアコンポーネントに対してアプリケーションサーバをインストールしないでください。外部から見えるネットワークや企業のネットワークからサーバをセグメント化します。VM をデータセンターに配置し、適切なファイアウォールまたはルータをアクセス制御リスト（ACL）で設定して、トラフィックを制御します。

ファイアウォールを適切に使用するには、どの TCP/UDP IP ポートが使用されるのか、ファイアウォールの導入とトポロジを検討し、ネットワークアドレス変換（NAT）の影響を知るネットワーク管理者が必要です。

TCP/IP ポート

Contact Center Enterprise ソリューションで使用するポートのインベントリについては、http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-configuration-examples-list.html の「*Cisco Unified Contact Center Enterprise Solutions* ポート使用状況ガイド」を参照してください。

Unified CM が使用するポートについては、の『*Cisco Unified Communications Manager* の *TCP* および *UDP* ポートの使用ガイド』を参照してください。http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

ファイアウォールの構成を支援するため、このガイドには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。

ネットワーク ファイアウォール トポロジ

AD 管理者が OU を作成する Active Directory モデルでは、次を実行します。

- 企業境界ファイアウォールで次のポートをブロック
  - UDP ポート 135、137、138、および 445
  - TCP ポート 135、139、445 および 593
- 適切に設定されたレイヤ 3 およびレイヤ 4 ACL を展開します。
- 専用の Historical Data サーバをインストールすることで、データベースと Web サービスを分離します。
- Administration & Data サーバ（ADS）の数を最小限にし、管理クライアント（データベース不要）とインターネット スクリプト エディタ クライアントを使用します。
- イントラサーバ通信を暗号化するために、Windows IPSec（ESP）を展開します。

- 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

ネットワークアドレス変換（NAT）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では、IP パケットペイロード内の IP アドレスが置き換えられない問題が発生します。IP ヘッダー内の IP アドレスだけが置き換えられます。

この問題を解決するため、Cisco IOS ベースのルータおよび PIX/JT ファイアウォールでは、CT-JTBE（TAPI/JTAPI）を含むさまざまなプロトコルおよびアプリケーションに対する *fix-ups* を実装します。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。このプロセスが動作するには、Cisco IOS または PIX/ASA のバージョンと Unified CM バージョンとの互換性が必要です。

Unified CCE は、NAT を介した接続をサポートしています。詳細については、http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-configuration-examples-list.html の「*Cisco Unified ICM/Contact Center Enterprise* セキュリティ ガイド」に記載されている『“IPSec および NAT サポート”』の項を参照してください。

ASA NAT とファイアウォール

Cisco 適応型セキュリティアプライアンス（ASA）ファイアウォールは、単一のセキュリティアプライアンスを、セキュリティコンテキストと呼ばれる複数の仮想デバイスに分割します。各コンテキストは、独自のセキュリティ ポリシー、インターフェイス、および管理者を持つ独立したデバイスです。マルチコンテキストは、複数のスタンドアロンデバイスを使用することに似ています。各コンテキストにより、カスタマートラフィックは分離され、安全になり、構成が容易になります。すべてのカスタマートラフィックが最初にファイアウォールに送信された後、コンピュータリソースに転送されます。

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 ファイアウォールを保護することで、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。Contact Center Enterprise ソリューションは、VM の Windows ファイアウォールの展開をサポートします。 *Cisco Unified ICM/Contact Center Enterprise* セキュリティ ガイド には、本機能の実装および構成に関する章が記載されています。

Windows ファイアウォール構成ユーティリティを使用して例外を構成すると、アプリケーションに必要なポートを開くことができます。

Windows ファイアウォールは、Unified CCE のインストール中に設定され、必要なポートが開きます。

Windows ファイアウォールの詳細については、Microsoft のマニュアルを参照してください。

Active Directory の展開

この項では、Active Directory の展開トポロジについて説明します。Active Directory（AD）展開ガイダンスの詳細は、https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html の *Cisco Unified ICM/Contact Center Enterprise* ステージング ガイド を参照してください。

専用の Windows Active Directory ドメインにソリューションを展開できますが、要件ではありません。代わりに、組織単位を使用してセキュリティの基本理念を展開できます。これは 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（ドメインメンバーシップ用）、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。

グローバル カタログの要件

Contact Center Enterprise ソリューションは、Active Directory のグローバルカタログを使用します。Unified CCE Hosts が格納されている AD フォレスト内のすべてのドメインは、そのドメインのグローバルカタログを公開する必要があります。これには、ソリューションが通信を行う認証、ユーザルックアップ、グループ検索などのすべてのドメインが含まれます。

Note これは、フォレスト間の操作を意味するものではありません。フォレスト間操作はサポートされていません。

Active Directory サイトトポロジ

地理的に分散された Contact Center Enterprise ソリューションでは、各サイトで冗長ドメインコントローラを配置します。各サイトでグローバルカタログを確立し、サイト間複製接続を適切に構成します。Contact Center Enterprise ソリューションは、サイト内の Active Directory サーバと通信します。これには、Microsoft のガイドラインに従って適切に実装されたサイトトポロジが必要です。

組織

アプリケーションによって作成された OU

ソリューションソフトウェアをインストールする場合、VM がメンバーである AD ドメインはネイティブモードである必要があります。インストールすると、ソリューションに複数の OU 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をインストールするには、AD の組織単位に対する代理制御が必要です。ドメイン階層の任意の場所に OU を配置します。AD 管理者は、Contact Center Enterprise ソリューション OU 階層をどの程度深くネストして作成し、データを入力するかを決定します。

Note 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。

Contact Center Enterprise のインストールによって、Domain Manager ツールと統合されます。このツールは OU 階層およびソフトウェアが必要とするオブジェクトを事前インストールする際にスタンドアロンで使用できます。また、設定プログラムが呼び出され、AD で同じオブジェクトを作成するときにも使用できます。AD/OU は、実行中の VM 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。

Active Directory 管理者が作成した OU

管理者は、特定の AD オブジェクトを作成できます。主な例は、Unified CCE サーバの OU コンテナです。この OU コンテナは、特定のドメインのメンバーである VM を含めるよう手動で追加されます。ドメインに参加したら、この OU にこれら VM を移動します。この分離は、サーバを管理できる人とできない人（制御の分離）を制御します。最も重要なのは、分離が、OU 内のアプリケーションサーバが継承できる、または継承できない AD ドメイン セキュリティ ポリシーを制御する点です。

Active Directory から CCE 認証を分離する

リリース 12.0(1) 以前は、Unified CCE は、Microsoft Active Directory Security Groups を使用して、設定や構成タスクを実行するユーザのアクセス権を制御していました。Microsoft AD は、システムコンポーネントが対話する権限も付与します。たとえば、このデータベースは、Logger データベースを読み取る権限をディストリビュータに付与します。Microsoft AD は、セキュリティグループ - 設定、構成、およびサービスに関連付けられているユーザ権限を管理します。したがって、Microsoft AD は、認証と承認の両方を処理しました。このような場合、Microsoft AD はセキュリティグループにユーザ権限を割り当てる必要があります。これを実現するには、Unified CCE ソリューション管理で、承認のために Microsoft AD に対する書き込み権限が必要です。

デフォルトでは 、Unified CCE により 、現在、認証および承認機能が切り離されています。

認証と認可を切り離すと、Microsoft AD を使用して、Unified CCE コンポーネントの許可を管理する必要がなくなります。Unified CCE ソリューションでは、承認のために、各ローカルマシン上のローカルユーザグループにユーザ ID を追加する必要があります。ユーザ権限は、ローカル マシンのローカル ユーザ グループへのメンバーシップによって提供されます。Microsoft AD は認証にのみ使用されます。

Microsoft AD にすでに存在するユーザ ID を承認するには、ユーザ ID を関連付けるか、ローカルユーザグループに追加します。

- ユーザ ID をローカルの `UcceService` セキュリティグループに関連付け、SQL データベースでの読み取り/書き込み操作用の SQL サーバの承認をユーザ ID に提供します。Service Account Manager ツールを使用して、ドメインユーザをサービス アカウント ユーザとして割り当てます。
- Unified CCE 設定操作用のローカル管理者グループにユーザ ID を追加します。Unified CCE 構成操作用のローカル `UcceService` セキュリティグループにユーザ ID を追加します。ユーザ ID がローカル管理者グループに追加されている場合は、**User List** ツールで、[**設定**（**`Setup`**）] チェックボックスをオンにします。ユーザ ID がローカル `UcceService` グループに追加されている場合、[**構成**（**Config**）] をオンにしすると、ユーザのセキュリティ グループ メンバーシップ（**管理者**グループまたは**構成**グループ）が、データベーススキーマにあるユーザグループテーブル内の **User_Role** コラムに表示されます。

ADSecurityGroupUpdate レジストリ キー

このレジストリキーは、インスタンスの組織単位（OU）の下で、ドメイン内の設定および設定セキュリティ グループの更新を許可または拒否します。

キーは、次の 2 つの値があります。

- 0 — User List ツールが、インスタンス OU のドメイン内の構成および設定セキュリティグループ更新していないことを示します。
- 1 — User List ツールが、インスタンス OU のドメイン内の構成および設定セキュリティグループ更新していることを示します。

デフォルト値は 0 です。

サービス アカウント マネージャのユーザ ヘルス

アップグレード後、Service Account Manager は `UcceService` ローカルグループ内のユーザを確認します。ユーザが、`UcceService` ローカルグループに存在しない場合、Service Account Manager は、[動作不良（*Unhealthy*）] というステータスを表示します。このような場合は、**Fix Group Membership** を実行してステータスを正常にします。または、Service Account Manager（SAM）ツールまたは、`Websetup` に新規ドメインユーザを提供します。

機能拡張の詳細については、次のガイドを参照してください。

- Cisco Unified ICM/Contact Center Enterprise ステージング ガイド の Service Account Manager に関する章。

- Unified CCE インスタンスへのコンポーネントの追加、ローカルマシンでの権限構成、および Cisco Unified Contact Center Enterprise インストールおよびアップグレードガイドにデータベースを移行の項。

Active Directory と Customer Collaboration Platform ユーザアカウント

Customer Collaboration Platform は、侵害を受けたシステムのリスクを軽減するためにエージェントのログイン情報の保管を最小限に抑えます。Customer Collaboration Platform は、システム設定の管理アカウントのみを保持しています。Customer Collaboration Platform は、Active Directory（AD）認証をすべてのエージェントアクセスに使用します。Customer Collaboration Platform サーバは、エージェントのログイン情報を保存しません。

Customer Collaboration Platform でエージェントアカウントを作成することはできません。AD が認証するすべてのアカウントで Customer Collaboration Platform を使用できます。アプリケーションを使用できるユーザを制限するには、AD グループを設定したら、Customer Collaboration Platform を構成して、そのグループへのアクセスのみを許可します。

一般に、AD が認証するエージェントは、すべての Customer Collaboration Platform 機能にアクセスできます。特定の URL をブロックすることで、パネルへのアクセスをブロックできます。

IPSec の展開

Contact Center Enterprise ソリューションは、VM とサイト間の重要なリンクを保護するために、Microsoft Windows ISec と Cisco IOS ISec の 1 つまたは両方に依存しています。次の方法でソリューションを保護できます。

- VM とサイト間にピアツーピア ISec トンネルを展開する方法
- より制限が厳しく、事前設定済みのネットワーク分離 ISec ポリシーを展開する方法
- 併用する場合

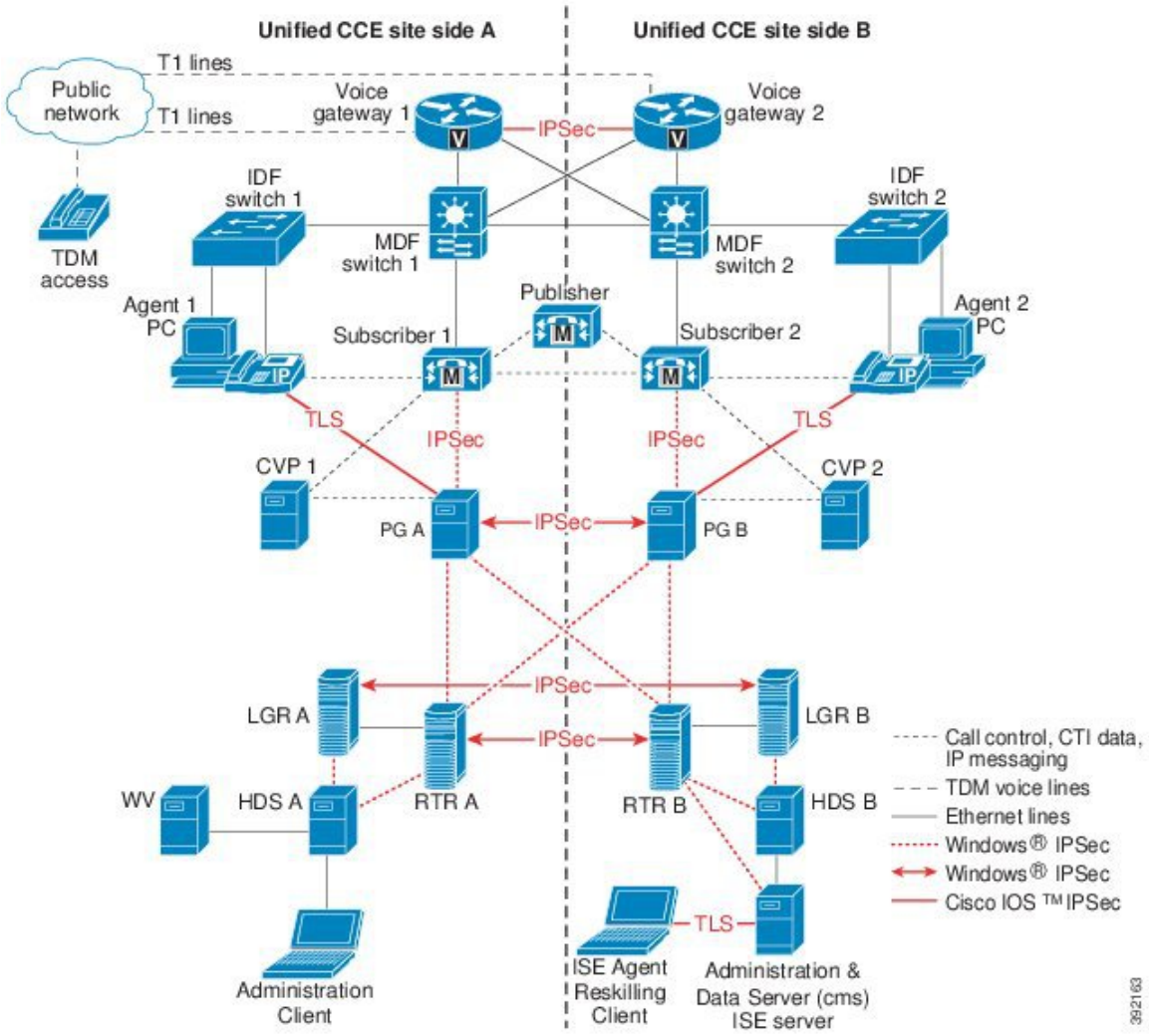
ピアツーピア ISec の導入では、Microsoft によって提供されるツールを使用して、セキュリティで保護されている各通信パスを手動で構成する必要があります。ただし、ネットワーク分離 IPSec ユーティリティを使用すると、各 VM にネットワーク分離 IPSec ポリシーを自動で展開できます。このユーティリティは、例外が発生しない限り、その VM との間のすべての通信パスを保護します。ネットワーク分離 IPSec ユーティリティは、すべての Contact Center Enterprise サーバにデフォルトでインストールされます。

Cisco Unified ICM/Contact Center Enterprise セキュリティ ガイドは、適切な設定などを含む Windows IPSec の展開に役立つサポートされているパスと情報を一覧します。

Note IPSec を有効にすると、いくつかの重要なエリアで、拡張性に影響を与えます。

Contact Center Enterprise ソリューションでの接続パスの一部は IPSec をサポートします。次の図は、Windows IPSec または Cisco IOS IPSec で保護する必要があるさまざまなサーバ相互接続を示しています。この図は、TLS をサポートする複数のパスも示しています。

***Figure 1: IPSec* の展開例**



サーバセキュリティ設定

ユニファイド コンタクト センター セキュリティ ウィザード

ユニファイドコンタクトセンターセキュリティウィザードにより、SQL サーバの強化、Windows ファイアウォールの構成、ネットワークの分離 ISec ポリシーの導入など、これらのセキュリティ機能を簡単に構成できます。セキュリティウィザードは、これらユーティリティの機能を使いやすいインターフェイスでカプセル化し、セキュリティ機能の構成に関連する手順でユーザを導き

ます。（これは、ネットワーク分離 IPSec ポリシーの展開時に役立ちます）。Unified CCE のインストールには、デフォルトでセキュリティウィザードが含まれます。

ウイルス対策

ウイルス対策アプリケーション

Contact Center Enterprise ソリューションは、いくつかのサードパーティ製のウイルス対策アプリケーションをサポートしています。ソリューションとソリューションで対応するバージョンの一覧に関しては、ソリューション向けの「互換性マトリックス」を、サポート済みのアプリケーションに関しては、Unified Communications Manager 製品関連のドキュメントを参照してください。

ソフトウェアの競合を避けるため、お使いの環境にはサポートされているアプリケーションだけを展開してください。

設定のガイドライン

ウイルス対策アプリケーションには、スキャンするデータとそのスキャン方法を詳細に制御できる多数の構成オプションがあります。

どのウイルス対策製品を使用する場合でも、スキャンと VM パフォーマンスのバランスを取るために構成を行います。スキャンを選択するほど、パフォーマンスのオーバーヘッドが大きくなります。システム管理者は、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に最適な構成要件を決定します。より詳細な Contact Center Enterprise ソリューションに関する構成情報は、http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html の *Cisco Unified ICM/Contact Center Enterprise* セキュリティ ガイドおよび、特定のウイルス対策製品に関する書類を参照してください。

次のリストでは、一般的なルールについて説明します。

- サポートされている最新バージョンのウイルス対策アプリケーションにアップグレードします。バージョンが新しいと、以前のバージョンよりもスキャン速度が向上し、VMのオーバーヘッドが軽減されます。
- 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のスキャンを回避します。すべてのスキャンをローカルに保持するために、すべてのマシンにウイルス対策ソフトウェアがインストールされているのが理想です。多層構成のウイルス対策戦略では、ネットワーク全体のスキャンやネットワーク負荷の追加は必要ありません。
- ヒューリスティックスキャンは、従来のウイルス対策スキャンよりもオーバーヘッドが大きくなります。この高度なスキャンオプションは、信頼できないネットワーク（電子メールやインターネットゲートウェイなど）からのデータエントリの重要なポイントでのみ使用します。
- 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。ファイルと読み取りのオンアクセススキャンは、高性能アプリケーション環境におけるシステムリソースに必要以上の影響を与えます。

- すべてのファイルを必要時にリアルタイムでスキャンすることで最適に保護できます。ただし、この構成により、悪意のあるコード（ASCII テキストファイルなど）をサポートできないファイルをスキャンする不必要なオーバーヘッドが発生します。システムにリスクを与えないと分かっているすべてのスキャンモードのファイルまたはファイルのディレクトリを除外します。また、ソリューションで除外する特定の Contact Center Enterprise ファイルのガイドラインに従います。これに関しては、 *Cisco Unified ICM/Contact Center Enterprise* セキュリティ ガイドを参照してください。
- 使用時間が低い、またはアプリケーションアクティビティが最も低い際は、定期的なディスク スキャンをスケジュールします。アプリケーションの削除アクティビティをいつスケジュールするかを決定するには、 *Cisco Unified ICM/Contact Center Enterprise* セキュリティ ガイドを参照してください。

侵入防御

シスコには、Sygate や McAfee などのベンダーによる、侵入防止製品のテストやサポートはありません。このような製品は、そのアプリケーションをセキュリティ脅威として誤って識別した場合、正当なアプリケーション機能をブロックする可能性があります。これらの製品を慎重に構成して、正当な操作を実行できるようにします。

パッチ管理

セキュリティパッチ

Contact Center Enterprise 製品へののセキュリティ更新資格認定プロセスについては、http://www.cisco.com/c/en/us/products/collateral/customer-collaboration/unified-contact-center-enterprise/product_bulletin_c25-455396.html に記載されています。このプロセスは、標準規格の Windows オペレーティングシステムを実行している VM に適用されます。

更新プログラムを適用するタイミングと方法に関する Microsoft のガイドラインに従ってください。Microsoft がリリースしたすべてのセキュリティパッチを評価し、環境に適していると判断したパッチをインストールします。

自動パッチ管理

Contact Center Enterprise サーバ（VOS にインストールされているアプリケーションは除く）は、Microsoft の Windows Server Update Services との統合をサポートしています。このサービスを使用すると、更新が選択的に承認され、実稼働 VM への展開時期が決定されます。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働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。承認されたメンテナンス期間中に更新が実行されるようスケジュールします。

構成と展開の詳細については、Microsoft のマニュアルを参照してください。

Cisco Unified Communications VOS の構成およびパッチプロセスでは、現在、自動パッチ管理プロセスは許可されません。

エンドポイント セキュリティ

Unified IP Phone デバイスの認証

Contact Center Enterprise ソリューションを設計する際、Cisco Unified IP Phone 向けにデバイス認証を実装できます。Contact Center Enterprise ソリューションは、以下を保証する Unified Communications Manager の 認証済みデバイスセキュリティモードをサポートしています。

- **デバイス ID** — X.509 証明書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 SIP 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 SIP メッセージコンテンツ

IP Phone の強化

Unified CM の IP Phone デバイス構成では、特定の電話機の機能を無効にすることで電話機を強化できます。たとえば、電話機の PC ポートを無効にしたり、PC による音声 VLAN へのアクセスを制限できます。これら設定の一部を変更すると、Contact Center Enterprise ソリューションの監視機能や録音機能が無効になります。設定は次のように定義されています。

- **PC 音声 VLAN アクセス** — PC ポートに接続されているデバイスを音声 VLAN にアクセスさせるかどうかを電話機が許可しているかを示します。ボイス VLAN アクセスを無効にすると、接続されている PC でボイス VLAN 上のデータを送受信できなくなります。また、電話によって送受信されたデータを PC で受信することもできなくなります。この機能を無効にすると、デスクトップベースの監視と録音が無効されます。

  この設定は有効（デフォルト）です。

- **PC ポートへのスパン** — 電話機が電話機ポートから PC ポートへ送受信されたパケットを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 アクセスを有効にします。この機能を無効にすると、デスクトップベースの監視と録音が無効されます。

  この設定は有効です。

次の設定を無効にすることで、中間者攻撃（MITM）を防ぎます。一部のサードパーティ製のモニタリングおよび録音アプリケーションでは、このメカニズムを音声ストリームのキャプチャに使用します。

- **無償 ARP** — 無償 ARP 応答から、電話機が MAC アドレスを学習するかどうかを示します。

  この設定は無効です。

転送中の安全な PII

Contact Center Enterprise ソリューションは、内部および外部からの攻撃を受けやすい個人情報（PII）などのカスタマーの機密情報を処理します。

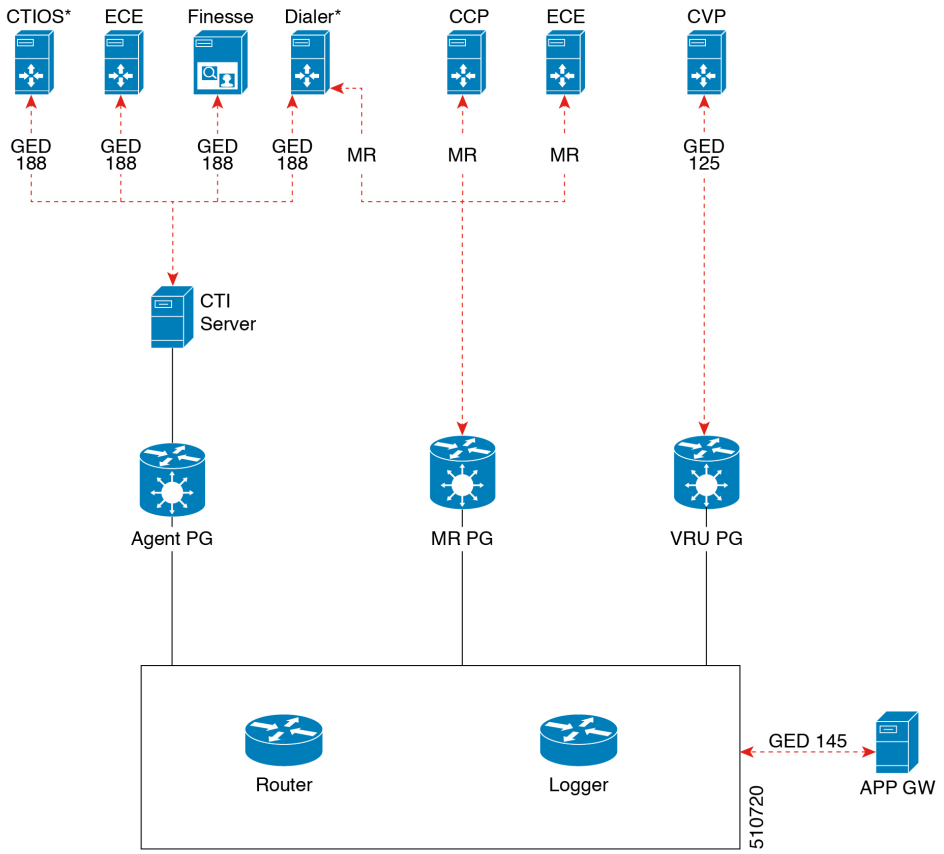
GED 188、GED 125、GED 145、および MR carry PII などのトランスポートチャネルは、攻撃を受けやすいです。CCE ソリューションは、TLS プロトコルを使用して、PII を転送するトランスポートチャネルを保護します。

これらのトランスポートチャネルの保護に使用される設計上の理念を次に示します。

- 自己署名証明書またはサードパーティ CA 署名付き証明書のいずれかを使用して、クライアントとサーバコンポーネント間のセキュアな通信チャネルを有効にします。
- 接続に失敗した場合、非セキュアモードにフォールバックするオプションはありません。
- VM ごとに 1 つのセキュリティ証明書を使用する。

セキュリティで保護された接続と証明書管理に関しては、https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html の「Cisco Unified ICM/Contact Center Enterprise セキュリティ ガイド」を参照してください。

Figure 2: セキュリティで保護された接続の例



Note セントラルコントローラと PG 間の通信チャネルは安全ではありません。エンドツーエンドのソリューションのセキュリティについては、IPSec ネットワーク分離ゾーンを使用します。