# Cisco Unified ICM/Contact Center 企業向けセキュリティガイド、リリース 12.6 (1)

**初版**：2021 年 5 月 14 日

**シスコシステムズ合同会社**
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

# 目 次

# はじめに



## 変更履歴

次の表に、このガイドで行われた変更のリストを示します。最新の変更が上部に表示されます。

| 変更 | 参照先 | 日付 |
|---|---|---|
| **リリース 12.6(1) のマニュアル 初回リリース** | | |
| OpenJDK の移行 | Java のアップグレード | |
| | アップグレード Tomcat | |
| | Tomcat を元に戻す | |

## このガイドについて

このドキュメントでは、Windows Server の Cisco Unified Intelligent Contact Management（Unified ICM）のセキュリティ強化設定ガイドラインについて説明します。「Unified ICM」 という用語には、Unified Contact Center Enterprise/Hosted（Unified CCE/CCH）、および Cisco Unified Intelligent Contact Management Enterprise/Hosted が含まれます。これらのサーバ設定に適用されるオプションの Unified ICM アプリケーションについては、以下を除き、こちらでも扱います。

- ビジネス チャットおよび E メール
- Dynamic Content Adapter

このマニュアルを通じて、「Unified ICM/Cisco Unified Contact Center Enterprise（Unified CCE）」への参照は、これらの設定を想定しています。セキュリティを強化したシスコパートナーやシスコが提供するソリューション（PSO アプリケーションなど）に関して、お客様の特定のソリューションに付属するアプリケーションでセキュリティを強化して使用することはできません。セキュリティの設定がそれらのアプリケーションの動作を妨害しないことを確認するために、特別なテストと認証を検討してください。

このマニュアルで示す設定は、シスコがアプリケーションの開発とテストに対して内部で使用するパラメータを表しています。基本のオペレーティングシステムとアプリケーションのインストール以外に、このセットからの誤差は、互換性のある動作環境の提供を保証することはできません。このマニュアルの設定を常に均等に実装することはできません。導入環境では、特定の企業ポリシー、特定の IT ユーティリティ（バックアップアカウントなど）、または他の外部ガイドラインに準拠するために、これらのガイドラインの適用を変更または制限できます。

# 対象読者

このドキュメントは、主にサーバ管理者および OS およびアプリケーションのインストーラを対象にしています。

このドキュメントのターゲットリーダーは、SQL サーバと Windows Server のインストールに精通している経験豊富な管理者です。リーダーは、Unified ICM/Unified CCE ソリューションのアプリケーション、およびこれらのシステムのインストールと管理にも精通しています。これらのガイドラインの目的は、シスコ のコンタクト センター アプリケーションが依存するさまざまなサードパーティ製アプリケーションのセキュリティ保護に関する統合ビューを追加的に提供することにあります。

# 関連資料

Cisco Unified ICM/Contact Center Enterprise のマニュアルおよび関連資料は、https://www.cisco.com/cisco/web/psa/default.html の Cisco.com からアクセスできます。

関連ドキュメントには、Cisco Unified Contact Center Management Portal、Cisco Unified Customer Voice Portal（CVP）、Cisco Unified IP IVR、Cisco Unified Intelligence Center のマニュアルセットが含まれます。次のリストには、さらなる詳細が記載されています。

- Cisco Unified Contact Center 製品のマニュアルについては、https://www.cisco.com/cisco/web/psa/default.html にアクセスし、**[音声およびユニファイド コミュニケーション（Voice and Unified Communications）] > [Customer Collaboration] > [Cisco Unified Contact Center 製品（Cisco Unified Contact Center Products）]** または **[Cisco Unified Voice Self-Service 製品（Cisco Unified Voice Self-Service Products）]** を選択します。次に、関心のある製品またはオプションを選択します。

- Cisco Unified Communications Manager のマニュアルは、https://www.cisco.com/cisco/web/psa/default.html からアクセスできます。

# 通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、シスコ サービスにアクセスしてください。
- サービス リクエストを送信するには、シスコ サポートにアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

### Cisco バグ検索ツール

Cisco バグ検索ツール（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

# フィールド通知

シスコでは、シスコ製品に関する重要な問題についてカスタマーとパートナーに通知するために、Field Notice を発行しています。通常それらの問題については、アップグレード、回避策、またはその他のユーザ アクションが必要になります。詳細については、https://www.cisco.com/c/en/us/support/web/tsd-products-field-notice-summary.html の「製品フィールド通知の概要」を参照してください。

次の通知で新しいアナウンスがリリースされた場合、シスコ製品、シリーズ、またはソフトウェアのカスタムサブスクリプションを作成して、電子メールアラートを受信したり、RSS フィードを利用できます。

- Cisco セキュリティ アドバイザリ
- Field Notice
- 販売終了またはサポートに関するアナウンス
- ソフトウェアアップデート

- 既知のバグの更新

カスタムサブスクリプションの作成の詳細については、https://cway.cisco.com/mynotifications の「マイ通知（*My Notifications*）」を参照してください。

# マニュアルに関するフィードバック

このドキュメントに関するご意見は、contactcenterproducts_docfeedback@cisco.com まで電子メールでご共有ください。

ご意見をお待ちしています。

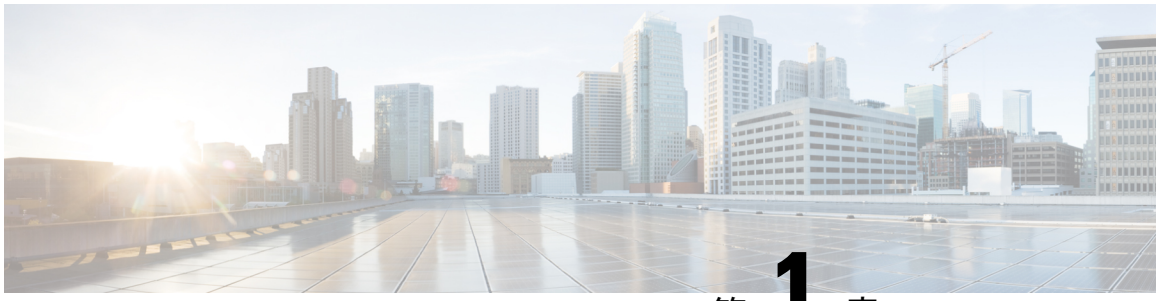
# 表記法

このマニュアルでは、以下の表記法を使用しています。

| 表記法 | 説明 |
|---|---|
| ▿太字▵ | 太字は、ユーザエントリ、キー、ボタン、フォルダ名およびサブメニュー名などのコマンドを表すときに使用されます。<br>次に例を示します。<br>• **[編集（Edit）]** > **[検索（Find）]** を選択します。<br>• [完了（Finish）] をクリックします。 |
| イタリック体 | イタリック体は、次の内容を表すときに使用されます。<br>• 新しい用語の紹介。例：スキル グループとは、類似したスキルを持つエージェントの集合です。<br>• ユーザが置き換える必要のある構文値。例：IF (*condition, true-value, false-value*)<br>• ドキュメントのタイトル。例： *Cisco Unified Contact Center Enterprise* インストールおよびアップグレード ガイドを参照してください。 |
| ウィンドウ フォント | Courier などのウィンドウ フォントは、次の場合に使用されます。<br>• コード中のテキストや、ウィンドウに表示されるテキスト。例：`<html><title>Cisco Systems, Inc. </title></html>` |

| 表記法 | 説明 |
| --- | --- |
| < > | 山カッコは、次の場合に使用されます。<br>• コンテキストでイタリックが許可されない引数（ASCII 出力など）。<br>• ユーザが入力する文字列で、ウィンドウには表示されないもの（パスワードなど）。 |

はじめに



第 1 章

# セキュリティ戦略と Unified CCE



## 絶え間ないセキュリティの向上

セキュリティを取り巻く状況は、日々の脅威と共に常に変化しています。新しい脅威により、高度な技術とイノベーションメカニズムがビジネスに大きく影響を及ぼす可能性があります。セキュリティ戦略は、データとシステムリソースの機密性、整合性、可用性を保護するというビジネス上の支援において必要なものです。

この章では、Contact Center Enterprise 製品とシスコのセキュリティプロセスのセキュリティアーキテクチャが、セキュリティ戦略をどのようにサポートしているのかについて説明します。また、セキュリティ戦略に関する当社のビジョンをカプセル化するコラボレーション セキュリティ制御フレームワーク（SCF）についても説明します。

## セキュリティ戦略をサポートする方法

セキュリティ戦略を、セキュリティプロセス、技術とツール、および Contact Center Enterprise ソリューションにおけるコンプライアンスに関するセキュリティポリシーの間のシナジーでサポートします。これらは、次から直接派生します。

- シスコの製品セキュリティ要件
- 市場ベースのセキュリティとコンプライアンスの要件
- 必須の規制、セキュリティ、およびコンプライアンスの要件

- コラボレーション セキュリティ制御フレームワーク

セキュリティを強化するには、コラボレーションセキュリティ制御フレームワーク（SCF）の目標を組み込む必要があります。シスコのセキュアな開発ライフサイクル（CSDL）プロセスは、シスコの開発作業と SCF の調整を行います。

**関連トピック**

安全な開発プロセス （19 ページ）

# コラボレーション セキュリティ制御フレームワーク

コラボレーションセキュリティ制御フレームワークは、安全で信頼性の高いコラボレーションインフラストラクチャを構築するための設計と実装のガイドラインを提供します。これらのインフラストラクチャは、既知の攻撃および新しい形式の攻撃のどちらに対しても耐障害性に優れています。SCF は、インフラストラクチャ アーキテクチャにおける技術的リスクの評価をサポートするモデル、手法、制御構造、および制御セットの組み合わせです。SCF は継続的な改善プロセスに統合されます。このプロセスにより、インフラストラクチャ アーキテクチャのセキュリティ強化が段階的に改善されます。これらの改善により、現在の重要な脅威に対処し、新しく脅威や発生しつつある脅威を識別し、追跡し、防御します。

SCF には、セキュリティポリシーの強化や、可視性と制御性の向上に役立つ 6 つのセキュリティアクションが定義されています。SCF は、次の 2 つのセキュリティ理想を中心に、それぞれをサポートする 3 つの柱を使用して展開します。

- 完全な可視化
  - 特定
  - 監視
  - 相関
- 包括的な制御
  - 強化
  - 分離
  - 措置

SCF には、Contact Center Enterprise のソリューションに対するアーキテクチャの復元力の基盤が必要です。

# セキュリティ アーキテクチャの原理

シスコのセキュアな開発ライフサイクルは、高度にセキュアなソリューションアーキテクチャの作成において、業界の一部の分野をリードし、対応しています。シスコのセキュアなコーディング標準規格は、すべての Unified CCE リリースに CSDL の原則を設計しています。これらの標準は,製品に対する影響を防ぐための機能です。また、プログラムの予期せぬ動作や、既

知のエクスプロイト可能な脆弱性を引き起こす可能性のある、未定義の動作を排除しています。

セキュリティアーキテクチャの原則では、既知のセキュリティ脆弱性に対する対策を展開する必要があります。たとえば、次のような対策があります。

- 信頼だけでなく、検証も必要
- 弱いエンティティと重要なエンティティのセキュリティ保護
- 必須プラットフォームの強化
- 安全な失敗と安全な失敗
- 詳細を防御する（各エンティティが入力を検証）
- 明示的に承認されていない限り、デフォルトは常に「最小権限」
- 権限の分離（役割の分離と義務の分離）
- すべてのエンティティは、環境システムに入る前にトライパーティによって承認（Ops、リリース、およびセキュリティ）
- PII データとセンシティブデータ（保存時と送信中の両方）の保護
- すべての失敗とすべての CRUD（作成、読み取り、更新、および削除）のアクションを記録し、ログを保護

# Unified CCE ソリューションのセキュリティ アーキテクチャ

当社のセキュリティアーキテクチャは、複数の階層化されたセキュリティオプションと制御で構成されています。これらのセキュリティ機能は、個々のセキュリティ要件を満たして導入できます。これらの機能を組み合わせて、攻撃に対する強力なセキュリティポスチャを実現できます。

Contact Center Enterprise のソリューションには、Windows OS 上で実行されるサーバと、Linux ベースの Cisco Voice OS（VOS）上で実行されるサーバが含まれます。セキュリティアーキテクチャは、特定のサーバが実行されている OS のリソースを利用します。

Windows OS では、Unified CCE サーバは、Windows ファイアウォール、Windows NT LAN Manager バージョン 2（NTLMv2）、Windows 強化ポリシー、および Active Directory を利用します。これらのサーバには、以下が含まれます。

- ルータとロガー
- 周辺機器ゲートウェイ
- 管理 & データサーバ
- Cisco Voice Portal
- Unified Contact Center Management Portal

Cisco VOS プラットフォームは、Linux（シェル）OS アーキテクチャ内で動作する閉じたアプライアンスベースのモデルです。VOS 上で実行されるサーバには、次のものが含まれます。

- Cisco Finesse
- Cisco Unified Intelligence Center
- 仮想音声ブラウザ
- Unified Communications Manager
- Cisco Unity Connection
- Cisco Identity Service
- ライブ データ
- Customer Collaboration Platform

次の図は、Unified CCE インスタンスの中核的な要素を示しています。

デスクトップや電話機などのアプリケーション エンドポイントには、コンピュータ テレフォニー インテグレーション（CTI）、JTAPI、および TAPI アプリケーションが関係します。これらのエンドポイントは、TLS と SRTP を活用してセキュリティで保護されています。このソリューションでは、作成した証明書信頼リスト（CTL）を使用して、クライアントとサーバ間のシグナリング認証を確立します。

### ネットワーク セキュリティ アーキテクチャ

Contact Center Enterprise のソリューションは、柔軟なネットワーク セキュリティ モデルを提供します。ネットワーク上には、固有のニーズとコンプライアンス要件に基づいてソリューションにセキュリティを適用できる領域が多数用意されています。これには、ファイアウォール、アクセス制御リスト（ACL）、プライベート ネットワーク アドレッシング、ネットワークアドレス変換（NAT）、DMZ、SRTP、およびインターネット プロトコル セキュリティ（ISec）の設定が含まれます。

IPSec を導入することで、移動中のデータを保護できます。IPSec は、Internet Protocol（IP）ネットワークを使った、プライベートで安全な通信を確保するために設計されたオープン標準のインターネットレイヤ 3 フレームワークです。暗号セキュリティサービスとポリシーを使用すると、セキュリティが提供されます。IPSec は、次に対する攻撃に役立ちます。

- 信頼されていないコンピュータからのネットワークベースの攻撃により、アプリケーション、サービス、またはネットワークのサービス拒否が発生する可能性があります
- データ破損
- データの盗難
- ユーザ資格情報の窃盗
- 重要なサーバ、他のコンピュータ、ネットワークに対するネットワークセキュリティ攻撃（IP スプーフィング、DNS ハイジャック）

IPSec は、Contact Center Enterprise のソリューションに 2 つのモードで導入できます。LAN または WAN ネットワークエンドポイントは、トランスポートモードとトンネルモードのいずれかの導入をサポートします。コンタクトセンターノード（周辺機器ゲートウェイ、ルータ、およびロガーなど）は、トランスポートモードの IPSec のみをサポートします。

音声およびビデオストリームを提供する Real-Time Transport Protocol（RTP）に暗号化を直接適用することで、ソリューション内の音声トラフィックを保護します。RTP ストリームは、中核的な Contact Center Enterprise ソリューション内では終了しません。Unified CM や音声ゲートウェイなどの付加デバイスは、ソリューション内にメディアターミネーションを提供します。

Secure Real-Time Transport Protocol（SRTP）は、音声とビデオのトラフィックを保護する方法です。

Unified CCE Web サーバは、Web サーバの応答に Microsoft Internet Information Services（IIS）、クライアント認証には Apache Tomcat を使用します。Web サーバと Web ベースのユーザ間の通信は、HTTPS および Transport Layer Security（TLS）プロトコルを使用して信頼され、暗号化されます。

Contact Center Enterprise のソリューションを構成するサーバは、保護されたデータセンターに存在します。通常、これらはオープン インターネット トラフィックにさらされません。これらのサーバは、ファイアウォールまたはDMZの背後に置かれています。唯一の例外は、Microsoft Active Directory ドメインコントローラ、Customer Collaboration Platform サーバ、および DMZ 内に存在する電子メールおよびチャット Web サーバです。

このガイドは、オンプレミスに基づくソリューションの導入に焦点を当てています。シスコは、Customer Journey Platform などのクラウドベースのコンタクト センター アプリケーションも提供しています。クラウドデータ処理に関する国際標準要件の順守を十分に確認しています。シスコは、クラウドデータ処理と国境を越えた転送に関する EU、EU-US プライバシー シールドおよび APEC 合意との間で拘束力のある企業ルールを締結しています。Cisco Trust Center の Web サイト（https://www.cisco.com/c/en/us/about/trust-center.html）では、次の保護機能の詳細を提供しています。

# 完全な可視化の目標

SCF モデルは、セキュリティの目的と、セキュリティ制御を整理するためのセキュリティアクションをサポートする構造を定義します。SCF モデルは、実証済みの業界プラクティスとセキュリティアーキテクチャの原理に基づいています。このモデルは、シスコのエンジニアが、サービスプロバイダー、企業、および中小規模のビジネス（SMB）インフラストラクチャの設計、実装、評価、および管理を行うことで培った経験から成長しています。

SCF モデルを使用すると、包括的な可視性を目的としたシステムのアクティビティに対するインサイトを把握できます。SCF は、システムが次を知っていることを義務付けています。

- システムへのアクセス者
- 実行されるアクション
- 異常、機能のずれ、または不審なアクティビティについて通知する人

包括的な可視性の目標に関する主な検討事項には、次のようなものがあります。

- 識別して、ユーザー、トラフィック、アプリケーション、プロトコル、および利用行動の分類
- 監視および活動およびパターンを記録
- 複数のソースから収集し、データの相関することで、傾向およびシステム全体のイベントを識別
- 検出および異常トラフィックや脅威を識別します。

# システムのすべてを特定する

Contact Center Enterprise のソリューションは、ユーザの認証と承認に 2 つの一般的な方法を利用します。Unified CCE は、サーバ間認証に NTLMv2 を利用します。管理ユーザ カウントは、認証および承認に Active Directory（AD）を使用して、ステージング、導入、および操作に関連するタスクを実行します。

デフォルトでは、Unified CCE エージェントは、Unified CCE 設定 SQL データベースを介して認証されます。必要に応じて、シングルサインオン（SSO）を導入して、適格な ID プロバイダー（IdP）を使用してエージェントを認証できます。IdP は内部または外部に使用できますが、認証には SAMLLv2 アサーションを提供する必要があります。SSO の導入では、アプリケーションの構成データベースにユーザパスワードは保存されません。認証に成功すると、Unified CCE はアイデンティティサービス（IdS）によって、アイデンティティサービス（IdS）によって、保護されたリソースに対する認証のために OAuth トークンを提供します。

## ユーザの特定

Contact Center Enterprise のソリューションは、次のユーザクラスを認識します。

- 管理者
- エージェントとスーパーバイザ
- API ユーザ

Contact Center Enterprise は、管理者（ドメイン管理者とローカル管理者）の 2 つの機能を認識しています。AD は、すべての管理者の ID と認証を保持します。AD ステージングなどのドメイン管理者特権を必要とするセットアップ関連タスクには、ドメイン管理者アカウントを使用します。AD では、ローカルの管理者特権だけが必要なタスクには、ローカルの管理者アカウントを使用します。このようなタスクには、AD ルート組織ユニット（OU）インスタンスへのバインドや診断ツールへのアクセスが含まれます。

エージェントは、Contact Center Enterprise のソリューションの中核的なユーザです。設定データベースを介してエージェントアカウントを作成および認証します。

スーパーバイザには、エージェントのスキル変更やレポートの実行などのタスクに対する追加の権限が必要です。この理由から、AD ではスーパーバイザアカウントを作成します。

Contact Center Enterprise のソリューションには、サードパーティ製ツールで機能する API がいくつか含まれています。Unified CCE REST API コールはすべてステートレス（セッション固定ではない）ですが、HTTPS 経由の認証済みコールです。承認された API ユーザは、最初のシステム導入時に定義します。

## デバイスの識別

Unified CCE ソリューションには、認証と承認のためにユーザ関連のデータ管理で中心的な役割を果たすデバイスが含まれています。これらのデバイスは、変更制御履歴を通じて簡単な監査を実行する機能も提供します。

Unified CCE 管理およびデータサーバには、SQL データベース内の Unified CCE 設定スキーマのコピーが含まれています。この情報は、コンタクトセンターエージェントを認証するデフォルト（非 SSO）方式を提供します。また、システム管理者が Unified CCE の機能制御セットを使用して、最小権限のアクセス制御を許可する権限のマッピングも提供しています。

エージェントおよびスーパーバイザのシングルサインオン（SSO）をサポートするために、このソリューションは VOS ベースのアプライアンスである Cisco Identity Service（IdS）を導入します。Cisco IdS は、IdP と信頼関係を持ち、Cisco Finesse や Cisco Unified Intelligence Center などの保護されたリソース全体にわたって内部の OAuth トークン管理を担当します。コンタクトセンターで SSO を有効にした場合、関連するエージェントおよびスーパーバイザ認証データは IdP に存在し、Unified CCE データベースには存在しません。

Unified CCE 自動記録機能には、Unified CCE 設定全体の冗長なマスターコピーが含まれています。Unified CCE ルータ は、ダイナミックキー生成メソッドを使用して、すべての設定トランザクションとその関連履歴を同じデータベースに同期および保存します。Unified CCE ツールでは、これらの設定およびリカバリ キーを使用して、コール ルーティング スクリプトの履歴と一般的な Unified CCE 設定トランザクションの変更を追跡および元に戻します。

Active Directory は、コアな Windows ベースの Unified CCE コンポーネント全体でセキュリティポリシーを管理し、管理ユーザに認証を提供する中心的な役割を果たします。AD に保存されるユーザパスワードは、ローカルの Security Accounts Manager（SAM）データベースに存在し、Unicode Pwdattribute のハッシュ値の一部です。Windows は、このハッシュ値が LAN Manager と Windows NT ハッシュの製品として生成されます。Unified CCE は、Web セットアップと Web 管理者が AD ユーザアカウントで認証を行う場合に使用するために作成します。

## サービスとアプリケーションの特定

Unified CCE サーバは、信頼できる Microsoft Active Directory ドメインで動作します。Unified CCE コンポーネントをインストールする前に、最初に必要な AD ステージングを実行する必要があります。Unified CCE サーバが存在するターゲット AD ドメインにルート OU（部門）を作成します。ルート OU「Cisco_ICM」は、ドメインルートに配置するか、別の OU 内に配置できます。ドメインルートの下にルート OU を複数の層でネストしないでください。ルート OU を作成するには、Unified CCE の Domain Manager を実行します。ドメイン管理者権限または委任（完全な制御）権限を、ルート OU がネストされたサブ OU に対して提供します。Domain Manager がルート OU を作成すると、残りのインストールに対するドメイン管理者権限は不要です。

中核的なソフトウェアをインストールした後、WebSetup を実行して、Unified CCE データベースサービスに必要な AD サービスアカウントを作成します。デフォルトでは、AD ルート OU 内にこれらのアカウントを作成するために、WebSetup はハードコードされています。ただし、これが完了すると、Service Account Manager（SAM）ユーティリティを実行して、DB サービスを事前設定された AD アカウントにマップすることができます。このサービスアカウントユーザのカスタムマッピングを実行する場合は、Unified CCE WebSetup が作成したデフォルトのサービスアカウントを削除できます。

Unified CCE Web サーバは、安全なアクセス（HTTPS）用に設定されています。シスコは、TLS で使用する Web サーバの設定に役立つ SSL 暗号化ユーティリティ（SSLUtil.exe）のアプリケーションを提供しています。このユーティリティにより、次の機能を実行して TLS 暗号化を構成するタスクが簡単になります。

- SSL の設定（SSL Configuration）
- SSL 証明書の管理

ユニファイド コンタクト センター セキュリティ ウィザードは、スタンドアロンサーバの強化型導入ツールで、セキュリティの設定を簡単にします。セキュリティウィザードでは、次のタスクを実行できます。

- Windows ファイアウォールポリシーの定義
- SQL 強化の適用
- IPSec を使用したネットワーク分離の実行

また、OS ツールを使用して、IIS で見つかったセキュリティタスクなどを実行することもできます。

各ソフトウェアリリースを対象に、特定のバージョンのサードパーティ製のウイルス対策ソフトウェアを使用する必要があります。お使いのソリューションが、適格なウイルス対策ソフトウェアを使用しているかを確認します。

# システムのすべてをモニタリング

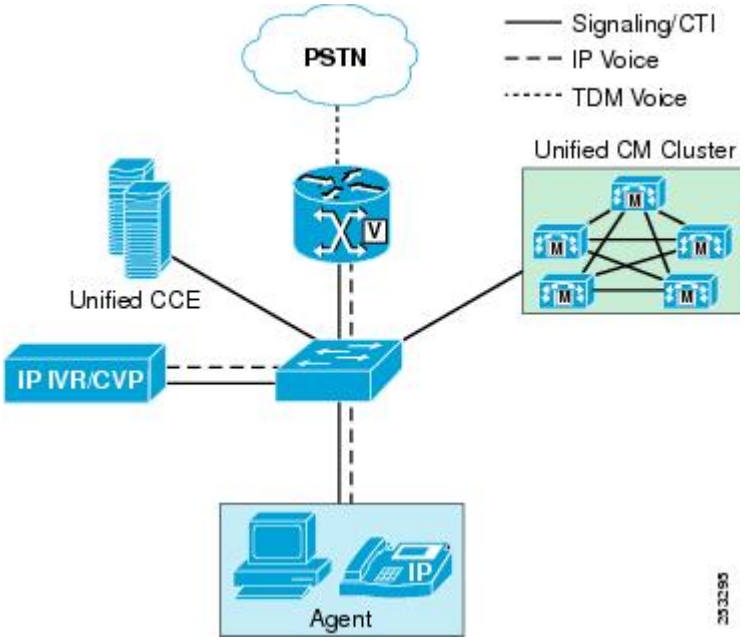
モニタリングは、製品アーキテクチャのすべての重要なコンポーネントをカバーする必要がある業務を効果的に管理する上で重要な役割を果たします。モニタリングは、セキュリティ上の問題を検出し、その重大度に基づいて分析と緩和を可能な限り早く行うのに役立ちます。

セキュリティの問題は、ネットワーク攻撃、ネットワークの破損、アプリケーションセキュリティ攻撃、およびトランザクションの失敗によって発生し、サービス拒否が発生する可能性があります。

## ネットワークのモニタリング

Unified Communications Manager Real-Time Monitoring Tool（RTMT）を使用して、Contact Center Enterprise ソリューションをモニタできます。RTMT は、診断情報を収集し、プラットフォームおよびアプリケーション設定データも収集します。RTMT は、ネットワークトポロジ内のす

べてのデバイスの正常性およびステータス情報と要求を収集する管理インターフェイスを提供します。RTMT を設定すると、他のセキュリティツールを使用して、ネットワークベースの攻撃（ゆっくりとした TCP 攻撃、「Slowloris」、または「ping of death」などのパケット攻撃）などのセキュリティ問題についてデータを解析できます。次の図は、RTMT がネットワークのやりとりをモニタするソリューション コンポーネントを示しています。




Contact Center Enterprise のソリューションは、特定のネットワークイベントをキャプチャします。ネットワーク要求の異常を報告します。各コンポーネントは、インターフェイスする他のコンポーネントの変更を確認します。当社のソリューションは、次のネットワークイベントを追跡できます。

- ホストが到達不能
- TCP タイムアウト
- 過剰な応答遅延

Contact Center Enterprise のソリューションには、ネットワークの異常に関するレポートを支援し、サードパーティ製のセキュリティ インテリジェンス ツールと統合するための機能が組み込まれています。

- コンタクトセンターデバイスのリアルタイムパフォーマンスのモニタリング
- デバイスインベントリ管理と検出
- ビルド済みおよびカスタムなしきい値、Syslog、相互関係、およびシステムルール
- リンクステータス、デバイスステータス、デバイスパフォーマンス、デバイス 360
- ユーザが設定したしきい値に対する電子メールメッセージ形式のイベントアラート生成
- RTMT に存在するデフォルトビューアでの収集と表示のトレース

セキュリティ戦略には、Contact Center Enterprise のソリューションに統合し、このデータを分析できるセキュリティインテリジェンスツールを含める必要があります。この役割を担うサードパーティ製ツールを検索できます。シスコには、次のセキュリティ インテリジェンス ツールも用意されています。

**Cisco AMP**

https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html

Cisco AMP（Advanced Malware Protection）では、グローバルな脅威インテリジェンス、高度なサンドボックス、リアルタイムのマルウェアブロックを提供することで、侵害が防止されます。ただし、予防だけに依存することはできません。AMP は拡張ネットワーク全体でファイルアクティビティを連続的に分析し、高度なマルウェアを迅速に検出し、阻止し、削除できます。

**Cisco Stealthwatch**

https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html

Cisco Stealthwatch は、業界大手の機械学習と行動モデリングを使用して、新たな脅威を識別し、迅速に対応するために役立ちます。ネットワークをモニタして、ネットワークインフラストラクチャからのテレメトリを使用して、オンの人と、その人が何をしているのかを確認できます。この機能により、ネットワークをセグメント化して重要なデータを保護できます。

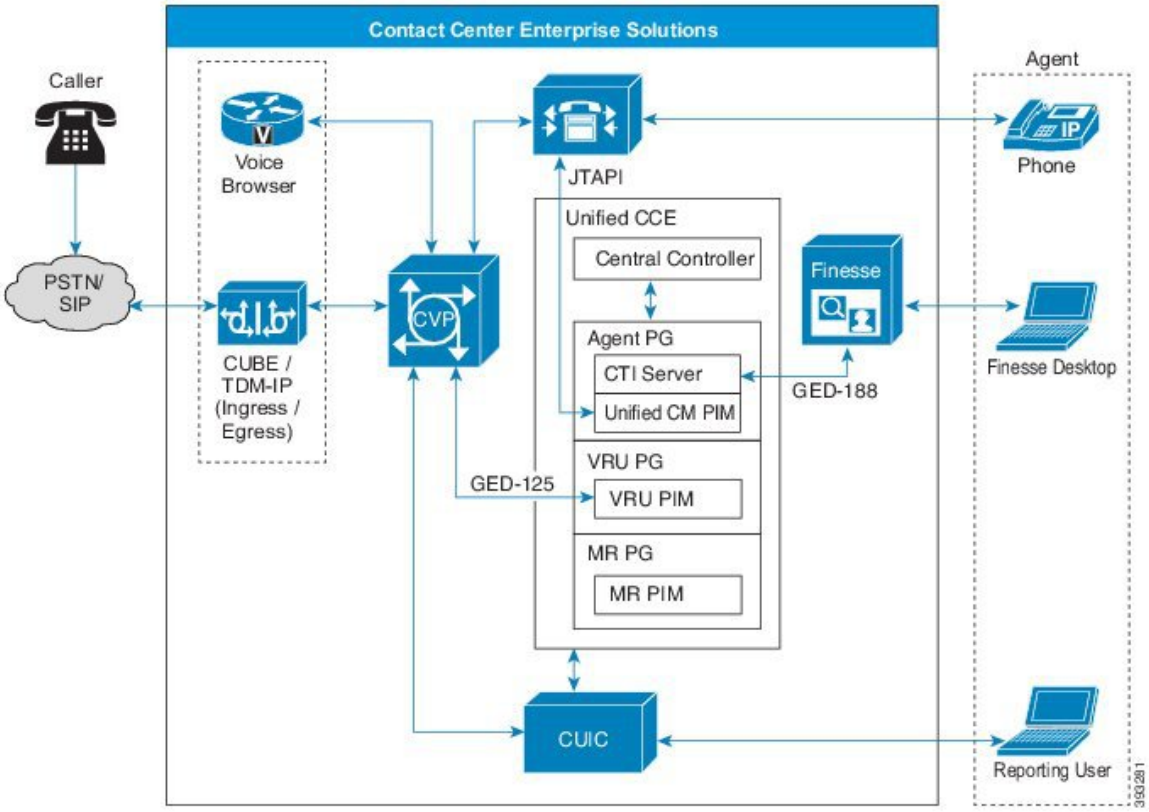
**Cisco Prime Assurance**

https://www.cisco.com/c/en/us/products/cloud-systems-management/prime-collaboration/index.html

Cisco Prime Assurance は、自動で迅速にプロビジョニング、リアルタイムモニタリング、プロアクティブなトラブルシューティング、およびシスコのインストールに関する長時間のトレンドと分析を提供します。

## データのモニタリング

コンタクトセンター企業ソリューションのコンポーネントは、ビジネストランザクションの一部として他のコンポーネントと通信します。コンポーネントは、この図に示すセグメントの主要なデータ転送をモニタします。




### 着信コール数（Incoming Calls）

Unified CCE は、2 つの主要な方法でコールを受信します。着信コールは、VoIP テクノロジーを使用してメディアサービスをテレフォニーエンドポイントにストリーミングする PSTN または IP ベースの SIP トランクを介して着信できます。いずれの場合も、物理メディアは、入力キャリア、音声ゲートウェイ、および Unified CM メディア ターミネーション エンドポイントの間を移動します。物理メディアストリームは、コアの Unified CCE コンポーネント内では終了しません。しかし、Unified CCE と Unified CVP は、コールの処理と取り扱いに重要なリアルタイムシグナリングを提供します。

Contact Center Enterprise ソリューションには、次に関連する着信コール攻撃をアクティブに検出し、防止するように設計されたセキュリティ機能が含まれています。

- 不正通話
- 電話によるサービス妨害行為（TDoS）

料金の不正使用は、テレフォニーシステムを使用して、アカウンタビリティを持たずに長距離（国際）コールを行う不正な使用です。シスコ コラボレーション ネットワークでの料金の不正利用を防ぐため、次のさまざまなツールを使用できます。

- Unified Communications Manager サービスクラス（CoS）
- 音声ゲートウェイの料金の不正利用防止アプリケーション

- 音声ゲートウェイクラスの制限（CoR）
- Cisco Unity Connection の制限ルール

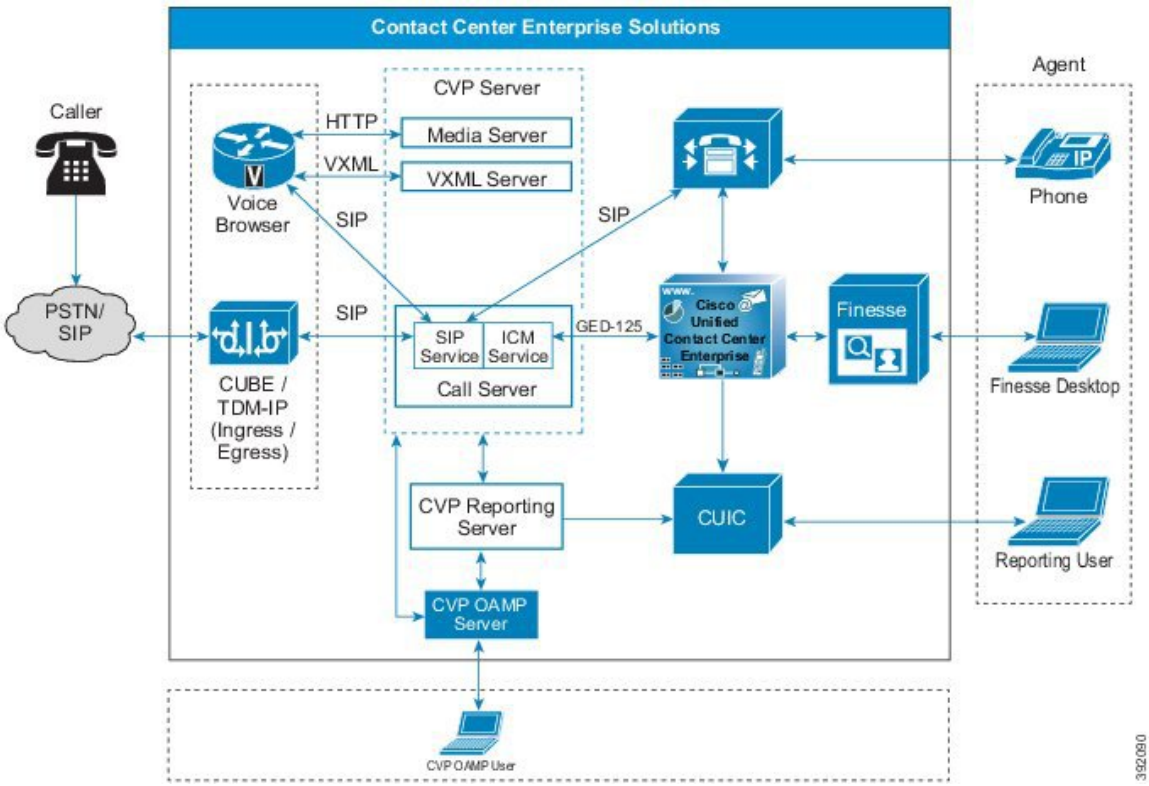
TDoS 攻撃は一般に、データネットワークのサービス妨害（DoS）と同じモデルに従います。不正なユーザがシステムにフラッディングしすぎてアクセス要求が多くなると、権限を持つユーザがシステムにアクセスできなくなります。Unified CCE には、輻輳制御機能が搭載されています。輻輳制御を使用すると、着信コールのコール/秒（CPS）パターンをモニタし、コンタクトセンターにアラートしてTDoS 攻撃から保護できます。

### ビジネストランザクション

以下は、当社のソリューションがデータをキャプチャし、診断データと障害をモニタするビジネストランザクションの一部です。

- **ルーティング制御**：Unified CM クラスタがルーティング命令の要求を可能にするメッセージ
- **デバイスとコールのモニタリング**：クラスタが Unified CCE の状態変更を通知できるメッセージ
- **デバイスとコール の制御**：Unified CCE から手順を受信する Unified CM クラスタを有効にするメッセージ

図 *1 : Unified CCE* ビジネストランザクション（コンポーネント間のコールフロー）



## モニタリング対象の録音

ほとんどのアプリケーション ロギング フレームワークは、技術的な障害が発生した場合の識別に焦点を当てています。Unified CCE ソリューションは、カスタムの診断フレームワーク API と業界標準の SNMP プロトコルと Syslog プロトコルを組み合わせて、プラットフォームとプロセスロギングの両方の機能を提供します。

セキュリティの監査では、システムの正常性に影響を及ぼす可能性のある問題の発生を防ぐため、反応ロギングをプロアクティブツールと分析にブレンドするという、緊密に統合された方法が必要です。当社のソリューションは、次の機能を組み込んでいます。

- 全コール期間のコールレポート
- Unified Intelligence Center とオープン データベース スキーマによる詳細なエージェントレポート
- エージェントと顧客間のブレンドタスクルーティングの監査証跡
- t_Event とリカバリテーブルを活用して管理変更の追跡を可能にする、オープンなデータベーススキーマのサポート
- 自動アラート用 RTMT

Syslog と中央リポジトリ サービス ログ ビジネス トランザクションとその他のデータ送信。Unified Intelligence Center は、監査のレポートおよび分析機能を提供します。

RTMT は、設定されている侵害（インシデント）に対するアラートを電子メールメッセージとして送信します。また、特に SNMP トラップでシステムの重大な侵害（インシデント）も設定します。RTMT は、次のタイプのイベントについてレポートできます。

- デバイス インベントリ管理
- 音声およびビデオのエンドポイント モニタリング
- 診断
- 障害管理
- コンタクトセンターデバイスのリアルタイムパフォーマンスのモニタリング
- 根本原因の分析に伴うイベントおよびアラーム
- コンタクトセンターのデバイスダッシュボード：ビルド済みおよびカスタム
- しきい値、Syslog、相互関係、およびシステムルール：ビルド済みおよびカスタム
- マルチテナントおよびログイン エージェントのライセンス情報

# システム内のすべてを関連付ける

情報セキュリティにコンテキストと意味を適用するには、アプリケーションロギングと編集によって記録されたイベント、インシデント、および失敗の相関関係が必要です。相関関係によ

り、さまざまな情報サイロ間の関係を評価することで重要な情報値が追加されます。Unified CCEは、ソリューション内のリアルタイムイベントと履歴イベントを関連付け、セキュリティ情報の値を増やします。

イベント、インシデント、および失敗の相関関係は、システムの障害や問題を特定、理解、およびトラブルシューティングするのに役立ちます。相関関係は、個別の方法で個々の根本原因を特定するよりも効果的です。

## アラートと通知を利用する

アラート、通知、およびアラームは、イベントのシステム管理者に通知するシステム機能です。システムは、これらのアラートに基づいて修正または予防措置を取り、事業運営をスムーズに行うことができます。このソリューションを使用すると、アカウントのサインイン試行などの重要なイベントを追跡できます。

Contact Center Enterprise のソリューションで使用可能なアラート機能の一部は次のとおりです。

- SNMP イベントトランスレータ機能は、Windows のイベントをリアルタイムで SNMP トラップに変換します。
- Microsoft SQL サーバには、新しい監査機能を使用したイベントのキャプチャとレポート機能が含まれています。詳細については、Microsoft の「https://docs.microsoft.com/en-us/sql/relational-databases/security/auditing/sql-server-audit-database-engine?view=sql-server-2017」の項目を参照してください。

  （注） シスコは、トランザクションパフォーマンスの低下により、Contact Center Enterprise のソリューション内の Microsoft SQL サーバでの監査に対する C2 イベントのキャプチャをサポートしません。

- イベント ログ モニタリング システムのアラートメカニズムは、AD の設計にとって重要な要素です。このメカニズムを使用すると、管理者の望ましくないインシデントに対する注意をチャネル化して、AD のセキュリティが低下しないようにすることができます。

  AD セキュリティモニタリングおよびアラートの詳細については、https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/monitoring-active-directory-for-signs-of-compromise を参照してください。

- Contact Center Enterprise のソリューションにより、Unified CCE サーバを Windows リモートデスクトップでリモート管理できます。ソリューションは、このような管理アクティビティのすべてのセキュリティイベントを記録します。Windows リモートデスクトップの集中ロギング機能を使用すると、Windows サーバイベントログまたは SNMP イベントモニタでイベントを記録できます。

  Unified CCE ソリューションがシステムイベントをキャプチャする方法の詳細については、このガイドの「監査」の章を参照してください。

### 関連トピック

監査（Auditing）

## イベントとセキュリティ インシデントの関連付け

ビジネスイベントは、何でもインシデントになる可能性があります。ビジネスでは、一部のシステムイベントをデフォルトでインシデントとして分類する必要があります。運用マニュアルまたは標準的な運用手順で、それらのイベントの修正措置と予防措置に対処します。コンタクト センター エンタープライズでは、次のビジネスイベントを、管理上の通知と修正措置を必要とするインシデントとして定義します。

- ホストが到達不能
- TCP タイムアウト
- 過剰な応答遅延
- 不明なリンクステータス
- 不明なデバイスステータス
- デバイス & コール制御 & メッセージ障害のモニタリング
- ルーティング制御メッセージの失敗

当社のソリューションは、これらのインシデントにアラートおよび通知機能を提供します。定義済みの修正措置を取った場合、これらの重大な失敗の情報を管理者に送信します。

詳細については、このガイドの「監査」の章を参照してください。

**関連トピック**

監査（Auditing）

# 完全な制御の目標

コラボレーションセキュリティ制御フレームワークは、完全に制御するという目的を通じてシステムの復元力を強化します。SCF には、システムをデフォルトで安全に強化できる十分なパラメータが提供され、既知のセキュリティ上の脆弱性が軽減されています。

# 可能なことを強化する

強化とは、ハードウェアとソフトウェアのデフォルト設定を変更することで、攻撃が発生する可能性がある手段を遮断するプロセスです。

### システムの強化

すべてのシステムに、一連のデフォルトリソースが有効化されています。システムの強化の目的は、システムの未使用リソースを無効にし、ビジネスニーズに必要なリソースのみを有効に活用する方法です。システムの強化は、ベンダーやメーカーに関係なく、オペレーティングシステム、Web サーバ、アプリケーションサーバ、データベースサーバ、ミドルウェア、ファイアウォール、ルータ、およびそれらを実行するハードウェアに適用されます。

詳細については、このガイドの「強化および準拠」のセクションを参照してください。

Contact center enterprise ソリューションには、強化手順が必要です。システムの強化手順とガイドラインは、Center for Internet Security、NIST セキュリティ標準 SP-800-123 など、複数の業界標準に基づいています。組織のセキュリティポリシーとプラクティスの一部として、すべての製品展開でシステムを強化する必要があります。

### OS の強化

OS の強化により、OS にデフォルトで含まれる不要なサービス、アプリケーション、およびポートを削除または無効化することで、オペレーティングシステムの安全性が強化されます。強化すると、アプリケーション、ファイルシステム、ネットワーク設定に対して正しく関連する許可と権限が適切に設定されます。また、未使用のファイルも削除され、最新のパッチが適用されます。

### データベースの強化

データベースの強化は、権限の少ない原則に従います。これは、ユーザが不要で、誤使用の可能性がある機能をロックダウンすることでユーザのアクセスを制限します。データベースの強化には、権限の分離や、適切で関連したユーザについてのみ、異なるスキーマや表へのアクセス制限が含まれます。データベースの強化の原則を適用することで、システム管理者とデータベース管理者の「役割分離特権」により、セキュリティが向上します。

### ファイアウォールの強化

ファイアウォールでは、企業または内部インフラストラクチャの周囲レベルのセキュリティを定義します。ファイアウォールは、ネットワークまたはホストがサービスとアプリケーションを保護する最初の防御メカニズムの 1 つです。

業界標準のファイアウォール強化の原則に従うのは、セキュリティ戦略にとって重要です。

詳細については、https://www.cisco.com/c/en/us/about/security-center/firewall-best-practices.html にある「*Cisco Firewall Best Practices Guide*」を参照してください。

### サーバ強化

サーバまたはインフラストラクチャを強化すると、Web サーバ、アプリケーションサーバ、その他のアプリケーションまたはサービスを含む各ネットワークコンポーネントに適切なセキュリティが適用されます。サーバの強化は、製品やサイトに影響を与える可能性のあるリスクをモデル化するセキュリティ調査から始まります。安全ではない可能性のある環境のすべての側面（Web 層のコンポーネントなど）を特定します。製品またはサービスを導入する前に、構成の変更によって既知の問題を取り除く必要があります。

詳細については、Center for Internet Security のサイト（https://www.cisecurity.org/cis-benchmarks/）を参照してください。

### ミドルウェア、その他のソフトウェア、およびハードウェアの強化

SNMP は、ネットワークデバイスの正常性に関する豊富な情報を備え、シンプルなアーキテクチャを提供します。ただし、SNMP は 2 台のコンピュータ間で交換されるデータを保護するた

めに、コミュニティストリングに依存しているため、セキュリティはほとんど提供されません。このコミュニティストリングは明確なテキストで表されています。これにより、多くのセキュリティ対策が効果的に無効になります。ネットワークデータとネットワークデバイスの両方の機密性、整合性、可用性を保護するために、SNMP を適切に保護します。

詳細については、次のソースを参照してください。

- 次のリンクにある「*Cisco IOS* デバイスの強化ガイド」の SNMP 強化のセクション https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html#anc54
- *Cisco Unified ICM/Contact Center Enterprise SNMP* ガイド at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html

AD の強化には、Microsoft Windows 環境全体で権限を付与されたユーザを完全に調査する必要があります。これらの設定を再設定して、すべてのユーザが適切なアクセス権を得る必要があります。これは、次をカバーするマルチステップの、けれども単純なプロセスです。

- ローカルユーザとグループ
- ADユーザ
- AD グループのユーザ権利
- AD の委任
- グループポリシーの委任
- パスワードの管理
- AD の監査とモニタリング
- サービス アカウント

詳細については、https://docs.microsoft.com/en-us/previous-versions/technet-magazine/cc160982(v=msdn.10) にある AD のセキュリティ保護に関する Microsoft TechNetの項目を参照してください。

**関連トピック**

SQL サーバの強化
Windows セキュリティの強化

# 可能なものの分離

分離の焦点は、攻撃の範囲と脆弱性を制限する追加の制御を加える方法です。分離によって、ユーザ、サービス、およびシステムへの影響を最小限に抑えます。論理セキュリティゾーンと物理セキュリティゾーンを作成することで、インフラストラクチャ内の機能ブロック間のアクセスを回避できます。この方法は、セキュリティ違反攻撃の範囲を制限します。

### システムとアーキテクチャの分離

Contact Center Enterprise のソリューションは、多層防御のアプローチに従います。このアプローチにより、すべての主要コンポーネントの機能をセグメント化し、ファイアウォールを階層化された機能セキュリティ管理用にセグメント化します。

### ユーザのセグメンテーション

Contact Center Enterprise は、ユーザを管理者、スーパーバイザ、およびエージェントとして分類します。各役割には、割り当てられた特定のタスクがあります。エージェントと管理者は、サインイン機能、場所に適用される制限、およびエージェントに対するその他の機能制限によって分離されています。スーパーバイザと管理者は、任意の端末またはアプリケーションからサインインして、システムをモニタおよび管理できます。

### アプリケーションの分離

Contact Center Enterprise は、その機能の役割に基づいてアプリケーションを分離します。ファイアウォールの分類によって、アプリケーションが保護され、関連するコンポーネントだけがアプリケーションに接続できます。

システム管理者は、NAT 対応のサインイン資格情報を使用して、これらの個々のコンポーネントを SSH 端末または Windows 上のセキュアなリモート画面共有プロトコルでリモートで管理します。このような分離により、攻撃が他のシステム機能に広がるリスクを最小限に抑えます。

# 可能なことを適用する

SCF の主な焦点は、可視性と制御の強化です。セキュリティポリシーの成功は、最終的には可視性と制御がどの程度強化されるのかによります。スマート企業は、ポリシー認識、慎重なモニタリング、および強制の組み合わせを使用して、ポリシーの適用に対する計画的な方法を取ります。この方法には、以下が含まれます。

- リスクの特定と伝達：問題点
- 受け入れ可能なポリシーとガイダンスインフラストラクチャの作成：責任を持つ関係者に期待される操作
- ポリシーへの準拠を監視するプロセスの開発：成功を知る方法
- コントロールが失敗した場合の応答機能の準備：侵害が発生した場合、誰が軽減するのか

効果的なガバナンスを行うのは、不作為の結果に直接関連しています。ポリシーによって期待が設定され、説明責任が割り当てられます。ポリシーは法律、規制、および技術的なセキュリティ要件を遵守し、許可または許可しないことを挙げています。ポリシーでは、管理がセキュリティ戦略とアーキテクチャを管理し、方向性を提供する方法を定義します。

シスコは、開発から導入および運用まで、デフォルトで Contact Center Enterprise の製品に内部のセキュリティポリシーと手順（CSDL など）を適用します。

# 安全な開発プロセス

シスコの Security and Trust Engineering グループは、次のような方法で、シスコの製品およびソリューション全体にわたって信頼できるプロセス、ポリシー、および技術を支持し、強化します。

- シスコのセキュアな開発ライフサイクル（CSDL）
- シスコのセキュリティ実施マネージャ
- シスコのセキュリティ サポート プログラム
- シスコの高度なセキュリティ イニシアチブ グループ（ASIG）

これらのプロセス、グループ、および専門チームは、シスコの製品およびサービスを評価し、セキュリティの脆弱性と弱点を特定します。協力しながら、緩和と改善の計画を作成し、継続的な改善周期でシスコの製品およびサービスに関するセキュリティ分析を実行します。また、CSDL をサポートするための安全な開発要件とツールも定義します。

CSDL は、高い手法と技術によって一貫性のある製品のセキュリティを確保し、ソフトウェアの脆弱性の数と深刻度を減少させます。CSDL は、ISO 27034 の「情報技術 - セキュリティ技術 - アプリケーション セキュリティ」のガイドラインに準拠しています。CSDL の強制適用と必須実装は、シスコの ISO コンプライアンス プロセスの一部です。シスコは、2013 年から ISO/27034-1 を基準として CSDL を評価しています。2011 年に発行された ISO/IEC 27034–1 のガイダンスを満たすか、このガイダンスをサポートする人、プロセス、ツールと共に、すべての現在のアプリケーションセキュリティ関連ポリシー、標準、および手順をサポートしています。

詳細については、https://www.cisco.com/c/en/us/about/trust-center/technology-built-in-security.html にある CSDL のセクションを参照してください。

シスコの内部セキュリティポリシーにより、リリースのステージング環境と FCS のサンドボックス環境は、実稼働環境のセキュリティ標準と手順と同等に強化されます。

シスコは、自動強化スクリプト、Web サーバ、アプリケーションサーバ、データベースサーバ、ミドルウェアソフトウェア、オペレーティングシステムなど、ソフトウェアスタックの強化されたイメージを適用します。この強化により、導入を迅速化し、強化システムで人的エラーが発生する可能性を回避できます。

リリーステストと FCS テストを社内に導入するには、開発周期内に導入されるセキュリティ スキャン ツールをすべてクリアする必要があります。

# 導入および運用のセキュリティ プロセス

Cisco Product Security Incident Response Team（PSIRT）は、シスコ製品やネットワークに対するセキュリティの脆弱性情報の受信、調査、および公開レポートを管理する専門のグローバルチームです。

Cisco PSIRT は、24 時間年中無休で、シスコのお客様、シスコのエンジニアとサポート、独立したセキュリティ研究者、コンサルタント、業界組織、その他のベンダーと協力して、シスコ製品やネットワークに関するセキュリティ上の問題が生じ得る可能性を特定します。

PSIRT のお知らせは、https://tools.cisco.com/security/center/publicationListing.x にある『シスコのセキュリティアドバイザリおよびアラート』から参照できます。

# コンプライアンス、データセキュリティ、およびプライバシープロセス

シスコ内部のセキュリティプロセスでは、セキュリティへの準拠が製品とサービスの設計の一部である必要があります。Contact Center Enterprise のソリューションは、これらのプロセスに従います。

社内のセキュリティおよびコンプライアンスプロセスは厳格です。当社のサービスにはサードパーティ製のソフトウェアコンポーネントが含まれているので、当社のソリューションは、セキュリティが侵害ないように、技術的、法律的、およびサプライチェーンのセキュリティ検証プロセスを繰り返します。これらのプロセスは、当社の製品開発のライフサイクルと完全に不可欠で、リリースのエントリ基準として機能します。

ただし、ビルトインされたセキュリティは、包括的なセキュリティ戦略の一部のみをカバーしています。ソリューションのセキュリティ戦略を設計する間、適切なセキュリティ、ビジネス、およびローカルのセキュリティ要件に準拠していることを確認するための手順を独自に追加します。

### セキュリティの標準、慣習、およびコンプライアンス

当社製品の製品のセキュリティ要件をリリース基準として定義します。これらの要件は、既知のリスク、顧客の期待、業界の慣行に基づいて、内部および外部のソースからコンパイルされます。業種や地域ごとに固有の要件があります。

当社は、これらのセキュリティおよびプライバシーの要件を遵守するために、お客様を支援する製品の開発に取り組んでいます。複数の地域や組織に共通する要件に優先順位を付けています。Contact Center Enterprise のソリューションに関する当社のセキュリティ要件は、該当する業界の標準要件を反映しています。

- 一般データ保護規制（EU 規制 2016/679）PII データ保護（欧州連合の個人識別情報）
- 米国 Sarbanes-Oxley 法
- 米国医療保険の相互運用性と説明責任に関する法令（HIPPA）
- ISO27001
- 情報技術セキュリティ評価のコモンクライテリア
- 米国政府の認証および標準：
    - Federal Information Processing Standards（FIPS）

- 国立標準技術研究所（NIST）SP 800 シリーズ
- Federal Information Security Management Act（FISMA）
- 連邦リスク・認証管理プログラム（FedRAMP）

- その他の市場要求に基づくセキュリティおよびコンプライアンスの要件：
  - SysAdmin、監査、ネットワーク、セキュリティ（SANS）の上位 20
  - オープン Web アプリケーション セキュリティ プロジェクト（OWASP）の上位 10
  - クレジットカード データ保護基準（PCI DSS）

標準規格と要件が重複する場合が多いため、共通のコンプライアンスシートを作成することで、当社の製品が要件を満たしていることを確認できます。これらのコンプライアンスシートの例については、https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Compliance/HIPAA/default/HIP_AppD.html にある「*Simplified Crosswalk—HIPAA*、*PCI* および *SOX*」を参照してください。

### データセキュリティとプライバシー

データセキュリティとプライバシーは、コンタクトセンターで最優先されます。Contact Center Enterprise の製品は、データ分類の標準とポリシーを適用して、個人識別情報（PII）を含む、特定されたセンシティブデータをコンタクト センター ソリューション内で保護します。

組織は一般に、必要な場合に限り、PII データまたはクレジットカードデータをローカルシステムに保存しないことを選択できます。Unified CCE ソリューションでは、コール スクリプト アプリケーション内の PII データに拡張コールコンテキスト（ECC）変数を使用します。Unified CCE では、これらの変数は履歴データベースに書き込まず、保存されません。

オーディオ録音がカスタマーケアポリシーの一部である場合は、クレジットカード情報を録音しません。多くの組織は、クレジットカード情報が話題に上がっている時はエージェントに録音を一時停止するようにしています。他のユーザは、デスクトップ分析や、自動一時停止と再開機能を提供するサードパーティ製アプリケーションとの統合を使用して、より自動化されたを方式を探しています。データソースへのパスがインターネットと同様に「オープンなパブリックネットワーク」を通過する場合は、データの転送中は暗号化してください。

### PII その他のセンシティブデータのセキュリティ

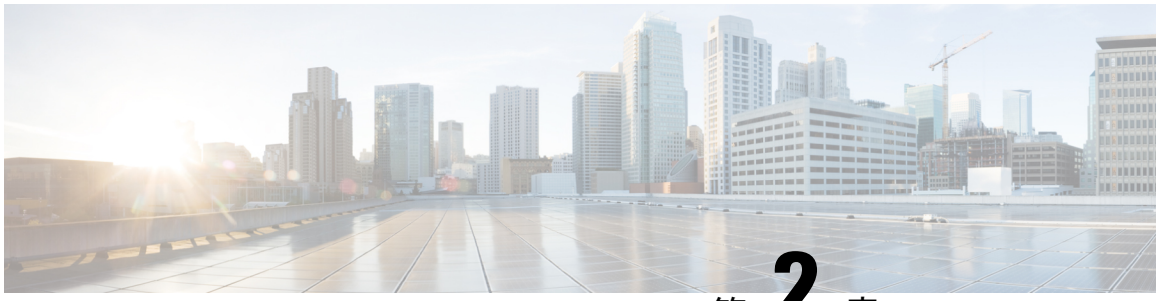
Contact Center Enterprise の製品は、シスコのセンシティブな個人情報の内部定義を使用します。その定義は複数のセキュリティ要件に基づいています。

Contact Center Enterprise の製品は、社内でセキュアなチャネルを使用して、ユーザ ID、パスワード、セッション情報、PII などの機密情報を通信します。サードパーティのアプリケーションサービスに接続する場合は、データ通信用のセキュアなプロトコルを使用して接続する必要があります。

PII には以下が含まれます。

- 連絡先情報（名前、電子メール、電話番号、住所）

- 識別情報の形式（SSN、運転免許証、パスポート、指紋）
- デモグラフィック情報（年齢、性別）
- 職業情報（職位、会社名、業界、従業員の電子メール、電話番号、ポケベル）
- ヘルスケア情報（医療制度、プロバイダ、履歴、保険、遺伝情報)
- 金融情報（銀行、クレジットカードおよびデビットカードのアカウント番号、購入履歴、取引記録)
- オンラインアクティビティ（IP アドレス、Cookie、フラッシュクッキー、ログイン情報）
- 顧客アカウントへのアクセスを許可するデータ（パスワード、個人識別番号）
- 電気通信およびトラフィックデータ（通話の詳細レコード、インターネットトラフィック、請求、通話履歴）
- 顧客のリアルタイムロケーション
- クレジットカード番号と銀行アカウント情報
- ソーシャルセキュリティ番号や運転免許証などの政府発行の識別子
- 差別につながる可能性があるデータ（たとえば、人種、種族的出身、宗教的または哲学的な信条、政治的意見、労働組合員であること、性的嗜好、身体的または精神的な健康状態）
- 身元窃盗に使用できるデータ（母親の旧姓など）



第 2 章

# 暗号化のサポート



## ユーザとエージェントのパスワード

シングルサインオン（SSO）が有効の場合、エージェントとスーパーバイザの認証をサードパーティのアイデンティティ プロバイダー（IDP）に渡します。このような場合、エージェントパスワードとスーパーバイザパスワードは Unified CCE データベースに保存されません。

SSO が有効になっていない場合、エージェントパスワードとスーパーバイザパスワードは SHA-256 ハッシュを含む設定データベースに保存されます。Unified CCE には、転送中のデータを保護するメカニズムと、保存中のデータを保護するためのオプションがあります。

管理者ユーザと設定ユーザのログインでは、Active Directory に保存されているログイン情報を使用します。これらのパスワードは、Unified CCE データベースには保存されません。例外として、システムインベントリは CCE 管理 Web ページを介して、中央の場所から Unified CCE サービスの中央の設定と管理を可能にするシステムインベントリです。システムインベントリでは、Unified CCE ソリューション内の他のサブシステムを管理し、診断情報を取得するためのログイン情報が必要です。これらのパスワードは、AW データベースに AES 256 ビット暗号化で保存されます。

CCE 管理 Web ページのユーザは、Active Directory のログイン情報を使用して認証されます。

CUIC レポート ユーザは、SSO が有効かどうかに応じて、SSO または AD のログイン情報を使用してログインできます。SSO が有効になっていない場合、スーパーバイザ レポート ユーザは Active Directory 認証を使用してレポートにアクセスし、設定データベースに保存されているローカルの SHA-256 パスワードにはアクセスしません。

（注） Unified CCE では、Active Directory のユーザパスワードの読み取り、設定、または変更ができません。スーパーバイザ レポート ユーザが、設定管理者が設定したエージェントパスワードとは異なる CUIC にログインするために、パスワード（AD パスワード）を使用する可能性があります。

# コール変数と拡張コール変数

Unified CCE のコールコンテキスト変数には、システム周辺機器内の設定とスクリプトの方法に応じて、センシティブデータが含まれている場合があります。終話コール詳細レコードに 1 ~10 の変数が格納され、**[永続（Persistent）]** チェックボックスがオンの場合、拡張コールコンテキスト（ECC）変数は、履歴データサーバ（HDS）の終端コール変数およびルータコール変数のレコードに保存されます。

これらの変数は、メモリ内でも、データベースに保存されている場合でも暗号化されません。したがって、これらの変数に保存するデータについては慎重にしてください。これらの変数は通常、診断とカスタムレポートにのみ使用されます。

Unified CCE は、トランスポート中に変数を暗号化し、格納されているドライブを暗号化するための戦略を持っています。

詳細については、「IPSec の概要 （27 ページ）」および「転送中の安全な PII （85 ページ）」を参照してください。

# Internet Script Editor

インターネット スクリプト エディタ Web アプリケーションは、TLS v1.2 プロトコルのみを使用し、エンドポイントがネゴシエートする暗号を使用して暗号化を行います。スーパーバイザのサインイン、ユーザのサインイン、および交換されたデータは、ネットワーク全体で保護されます。

IIS 内の特定の暗号スイートの有効化の詳細については、https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings にある項目を参照してください。

**関連トピック**

CCE 証明書管理ユーティリティ （81 ページ）

# Cisco Contact Center の SNMP 管理サービス

Unified ICM と Unified CCE には、*SNMP* リサーチ インターナショナルによって提供される認証と暗号化（プライバシー）をサポートする簡易ネットワーク管理プロトコル（SNMP v3）エージェントが含まれます。この実装では、管理ステーションとの通信の設定を、SHA-256 ダ

イジェストアルゴリズムを使用して認証されます。すべてのSNMPメッセージの暗号化に対して、この実装では次のいずれかのプロトコルが使用されます。

- aes-192
- AES-256

詳細については、https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html にある「*Cisco Unified ICM/Contact Center Enterprise SNMP* ガイド」を参照してください。

# TLS 暗号化のサポート

データ センター インターフェイスや、Cisco Finesse、Customer Collaboration Platform、CVP、アプリケーション ゲートウェイなどの外部コンポーネントは、TLSを使用した暗号化をサポートします。

## サポート対象の暗号方式

暗号化に使用される AES 暗号を次に示します。

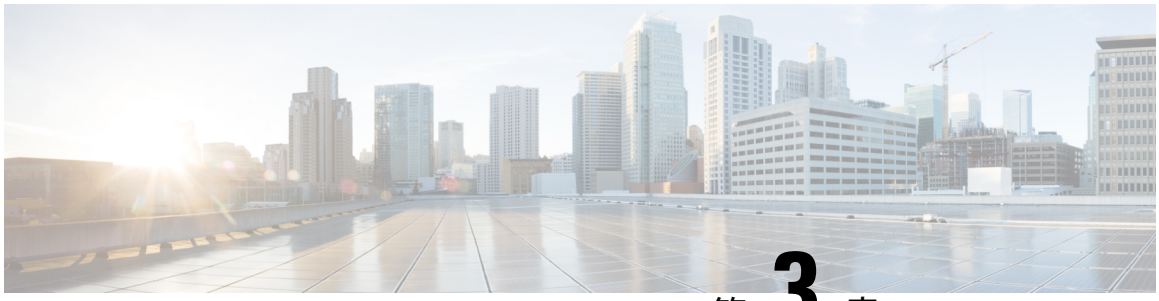
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA
- ECDHE-RSA-AES256-SHA384
- AES128-GCM-SHA256
- AES256-GCM-SHA384
- AES128-SHA256
- AES128-SHA
- AES256-SHA256
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES128-SHA256
- DHE-RSA-AES128-SHA
- DHE-RSA-AES256-SHA256

# 暗号スイートの管理

サーバとクライアントについて、サポートされている暗号をそれぞれ次のレジストリから追加または削除できます。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\Cisco SSL Configuration\ServerCiphers
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\Cisco SSL Configuration\ClientCiphers
```



第 3 章

# IPSec および NAT のサポート



## IPSec の概要

Internet Protocol Security（IPSec）は、暗号セキュリティサービスを使用して、Internet Protocol（IP）ネットワーク上のプライベートで安全な通信を確保するためのオープンスタンダードのフレームワークです。

（注） IPSec はさまざまな方法で導入できます。この章では、IPSec が何であり、IPSec を使用して選択した通信パスを保護する方法について説明します。「ネットワーク分離ユーティリティを使用した IPSec」の章では、サーバとの間のトラフィック**全体**を保護するための、より制限された、けれど自動化された IPSec のアプリケーションについて説明します。ネットワーク分離ユーティリティでは、IPSec の適用作業も保存されます。このユーティリティを使用して IPSec を適用する場合でも、この章を読んで IPSec 導入オプションを理解してください。その後、お使いの環境に対して最もメリットの高いツールを使用できます。

詳細については、https://docs.microsoft.com/en-us/windows/desktop/fwp/ipsec-configurationを参照してください。

コンタクトセンター環境に IPSec を実装すると、導入の容易さ、使いやすさ、および不正なアクセスから機密情報を保護するバランスを見つけ出すことを意味します。

適切なバランスを見つけ出すには、次の条件が必要です。

- リスクを評価し、組織に適したレベルのセキュリティを判断します。
- 機密情報を識別します。
- リスク管理基準を使用し、特定の情報を保護するセキュリティポリシーを定義します。
- 既存の組織内でポリシーを最適に実装する方法を決定します。
- 管理と技術の要件を確実に満たすようにします。

アプリケーションの使用または導入方法は、セキュリティに関する検討事項に影響します。たとえば、必要なセキュリティは、単一のメインサイトの導入と、信頼されたネットワークをまたがって通信できない複数のサイトにわたる導入の間で異なります。Windows Server のセキュリティ フレームワークは、厳格なセキュリティ要件を満たすように設計されています。ただし、慎重な計画とアセスメント、効果的なセキュリティガイドライン、実施、監査、および適切なセキュリティポリシーの設計と割り当てなしには、ソフトウェア単独では効果的ではありません。

IPSec を有効にした場合、パフォーマンスに影響を及ぼす影響は無視できると予想されます。コール処理レートに影響はありません。：

**関連トピック**

ネットワーク分離ユーティリティを使用した IPSec

# トンネルモードでの IPSec のサポート

データおよび音声ネットワークの導入におけるセキュリティ上の懸念が高いため、Unified ICM と Unified CCE は、セントラル コントローラ サイトとリモート周辺機器（PG）サイト間で IPSec をサポートしています。この安全なネットワーク実装は、WAN 接続が IPSec のトンネルで保護される分散モデルを意味します。トンネルモードの Cisco IOS IPsec の設定とは、2 つのサイト間の Cisco IP ルータ（IPSec ピア）だけが安全なチャネル確立の一部であることを意味します。すべてのデータトラフィックは WAN リンクを通して暗号化されますが、ローカルエリアネットワークでは暗号化されません。トンネルモードは、IPSec ピア間のトラフィックフローの機密性を保証します。これは、IOS ルータが、セントラルサイトをリモートサイトに接続しています。

IPSec 設定の適格な仕様は次のとおりです。

- AES 128
- AES 256

一般に、QoS ネットワークでは、トラフィックがトンネルにカプセル化され、暗号化される前に、パケットヘッダー情報に基づいて QoS 機能を分類および適用します。

# 転送モードでの IPSec のサポート

## システム要件

トランスポートモードでの IPSec のサポートについては、Microsoft Windows Server をインストールする必要があります。

## サポートされる通信パス

Unified ICM リリース は、サーバ間の通信を保護するために、Window サーバのオペレーティング環境での IPSec の導入をサポートしています。サポートは、顧客センシティブデータを交換する次のノードリストに制限されています。

1. NAM ルータと CICM ルータ間の接続
2. 冗長な Unified ICM ルータ/ロガーペア間のパブリック接続
3. 冗長な Unified ICM ルータ/ロガーペア間のプライベート接続
4. Unified ICM ルータと Unified ICM 周辺機器ゲートウェイ（PG）間のすべての接続
5. 冗長な Unified ICM ルータ/ロガーのペアと管理者 & データサーバ（プライマリ/セカンダリ）と履歴データサーバ（HDS）間のすべての接続
6. 冗長な Unified ICM ルータ/ロガーペアと管理サーバ、リアルタイムおよび履歴データサーバ、および詳細データサーバ（プライマリ/セカンダリ）間のすべての接続
7. 冗長な Unified ICM PG ペア間のパブリック接続とプライベート接続
8. Unified CCE 導入における冗長な Unified ICM PG ペアと Unified Communications Manager 間の接続

これらすべてのサーバ通信パスについて、IPSec 導入を計画する際の一般的な基盤として高いセキュリティレベルを検討してください。

## IPSec ポリシーの設定

Windows Server IPSec ポリシー設定は、セキュリティ要件を 1 つ以上の IPSec ポリシーに変換することです。

各 IPSec ポリシーは、1 つ以上の IPSec ルールで構成されています。各 IPSec ルールは、次で構成されます。

- 選択したフィルタリスト
- 選択したフィルタアクション
- 選択した認証方式

- 選択した接続タイプ
- 選択したトンネル設定

IPSecポリシーを設定するには複数の方法がありますが、最も直接的な方法は次のとおりです。

新しいポリシーを作成し、必要に応じてフィルタリストとフィルタアクションを追加し、ポリシーのルールを定義します。この方式では、最初にIPSecポリシーを作成してから、ルールを追加および設定します。ルールの作成中に、フィルタリスト（トラフィックタイプの指定）とフィルタアクション（トラフィックの処理方法を指定）を追加します。

各通信パスと各端（各サーバ）に対して、IPSecセキュリティポリシーを作成する必要があります。IP セキュリティ ポリシー ウィザードを使用して各 IPSec ポリシーのプロパティを作成および編集する場合は、次の情報を入力します。

1. 名前
2. [説明（Description）]（任意）
3. デフォルトの応答ルールをアクティブ化しない
4. IP セキュリティルール（追加ウィザードを使用したルールの追加）
   - トンネルのエンドポイント（トンネルを指定しない）
   - ネットワークタイプ：すべてのネットワーク接続
5. IPフィルタリスト
   - 名前
   - [説明（Description）]（任意）
   - 追加ウィザードを使用して IP フィルタを追加します。

     [説明（Description）]（任意）

     送信元アドレス：特定の IP アドレス（パスによって異なります）

     宛先アドレス：特定の IP アドレス（パスによって異なります）

     IP プロトコル の種類：任意
   - 追加ウィザードを使用して IP フィルタアクションを追加します。

     名前

     [説明（Description）]（任意）

     フィルタアクションの一般オプション：セキュリティのネゴシエート

     IPSec をサポートしていないコンピュータと通信しない

     IP トラフィックセキュリティ：整合性と暗号化 - 整合性アルゴリズム：SHA1 - 暗号化アルゴリズム：3DES
   - 認証方法：Active Directory _Kerberos V5 プロトコル（デフォルト）

（注）

- X.509 証明書は、顧客の設定に応じて実稼働環境でも使用できます。Unified ICM がすべての導入モデルで Active Directory を要求する場合、認証方式として Kerberos を使用する場合に、追加のセキュリティ資格情報管理は不要です。PG を介した Unified CM 接続の場合は、事前共有キー（PSK）を使用します。
- セキュリティを強化する際、PSK 認証は相対的に弱い認証方式なので使用しないでください。また、PSK はプレーンテキストで保存されます。テストには PSK のみを使用します。詳細については、事前共有キー認証に関する Microsoft Technet の項目を参照してください。
- IPSec ポリシーをカスタマイズする場合は、IPSec 設定を変更してカスタマイズできます。詳細については、データ保護の設定（クイックモード）設定に関する Microsoft のドキュメントを参照してください。

6. キー交換のセキュリティ方式：IKE セキュリティアルゴリズム（デフォルト）
   - 整合性アルゴリズム：SHA1
   - 暗号化アルゴリズム：3DES
   - Diffie-Hellman グループ：中（DH グループ 2、1024 ビットキー）

（注）

- セキュリティを強化するには、2048 ビット以上の Diffie-Hellman キーを使用して LogJam の脆弱性攻撃による脅威を軽減します（CVE - CVE-2015-4000）。詳細については、https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000を参照してください。強力な Diffie-Hellman グループと長いキー長を組み合わせると、秘密鍵の計算上の困難さが増します。詳細については、キー交換方法に関する Microsoft Technet の項目を参照してください。
- 長いキー長を使用すると、CPU 処理のオーバーヘッドが大きくなります。

# Unified Communications Manager への IPSec 接続

Unified Communications Manager が Unified ICM システムと同じドメインにはない Unified CCE システムでは、認証に Kerberos を使用できません。このようなシステムには、X.509 証明書を使用します。

# IPSec アクティビティ

## IPSec モニタ

Windows Server オペレーティングシステム上の IPSec をモニタするには、IP Security モニタ（ipsecmon）を使用できます。IPSec モニタの詳細については、Microsoft Technet の項目を参照してください。

## IPSec ロギングの有効化

ポリシーが正常に動作しない場合は、IPSec セキュリティ関連プロセスのロギングを有効にできます。このログは、Oakley ログと呼ばれます。ログは読みにくいですが、プロセスの失敗の場所を追跡するのに役立ちます。次の手順では、IPSec ロギングを有効にします。

### 手順

**ステップ 1** **[開始（Start）]** > **[実行（Run）]** の順に選択します。

**ステップ 2** **Regedt32** と入力 して **[OK]** をクリックして、登録エディタに入ります。

**ステップ 3** **HKEY_LOCAL_MACHINE** をダブルクリックします。

**ステップ 4** `System\CurrentControlSet\Services\PolicyAgent` に移動します。

**ステップ 5** **[ポリシーエージェント（Policy Agent）]** をダブルクリックします。

**ステップ 6** 右側のペインを右クリックし、**[編集（Edit）]** > **[キーの追加（Add Key）]** を選択します。

**ステップ 7** キー名として**Oakley**を入力します（大文字と小文字が区別されます）。

**ステップ 8** **[Oakley]** をダブルクリックします。

**ステップ 9** 左側のペインを右クリックし、**[新規（New）]** > **[DWORD 値（DWORD Value）]** を選択します。

**ステップ 10** 値の名前 **EnableLogging** を入力します（大文字と小文字が区別されます）。

**ステップ 11** 値をダブルクリックして、DWORD を **1** に設定します。

**ステップ 12** [OK] をクリックします。

**ステップ 13** コマンドプロンプトに移動し、**net stop policyagent & net start policyagent** と入力します。

**ステップ 14** `%windir%\debug\Oakley.log` でログを検索します。

# Message Analyzer

Message Analyzer を使用すると、プロトコル メッセージング トラフィックをキャプチャ、表示、および解析できます。さらに、Windows コンポーネントからのシステムイベントおよび他のメッセージのトレースと評価を行います。

Message Analyzer のダウンロードおよび詳細については、https://www.microsoft.com/en-in/download/details.aspx?id=44226 を参照してください。

# システム モニタリング

組み込みのパフォーマンス コンソール（perfmon）を使用すると、ネットワーク アクティビティを他のシステム パフォーマンス データと一緒にモニタできます。ネットワーク コンポーネントは別のハードウェアリソースとして取り扱い、通常のパフォーマンスモニタリングルーチンの一部として確認します。

ネットワーク アクティビティは、ネットワーク コンポーネントだけでなく、システム全体のパフォーマンスにも影響を及ぼす可能性があります。ディスク、メモリ、プロセッサアクティビティなどのネットワーク アクティビティと共に、他のリソースを必ずモニタしてください。システムモニタを使用すると、単一のツールを使用してネットワークとシステムのアクティビティを追跡できます。通常のモニタリング設定の一部として、次のカウンタを使用します。

- Cache\Data Map Hits %
- Cache\Fast Reads/sec
- Cache\Lazy Write Pages/sec
- Logical Disk\% Disk Space
- Memory\Available Bytes
- Memory\Nonpaged Pool Allocs
- Memory\Nonpaged Pool Bytes
- Memory\Paged Pool Allocs
- Memory\Paged Pool Bytes
- Processor(_Total)\% Processor Time
- System\Context Switches/sec
- System\Processor Queue Length
- Processor(_Total)\Interrupts/sec

# NAT のサポート

ネットワークアドレス変換（NAT）は、大規模ネットワーク内の登録済み IP アドレスを保存し、IP アドレッシング管理タスクをシンプル化するためのメカニズムです。NAT は、プライベート内部ネットワーク内の IP アドレスを、パブリック外部ネットワーク（インターネットなど）を通じて転送する法律上の IP アドレスに変換します。NAT はさらに、着信トラフィックの法律上 の 配信アドレスを内部ネットワーク内の IP アドレスに変換します。

NAT 全体にわたって Unified CCE 環境に IP 電話を導入できます。リモート周辺機器（PG）サーバは、NAT ネットワークリモートの中央コントローラサーバ（ルータおよびロガー）から見つけ出すことができます。PG サーバの NAT サポート資格は、NAT 機能を備える Cisco IP ルータを実装するネットワーク インフラストラクチャに限定されています。

エージェントデスクトップは、サイレントモニタリングが使用される場合を除き、NAT 環境でサポートされます。サイレントモニタリングは、NAT ではサポートされていません。

NAT の設定方法の詳細については、https://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080094e77.shtml を参照してください。

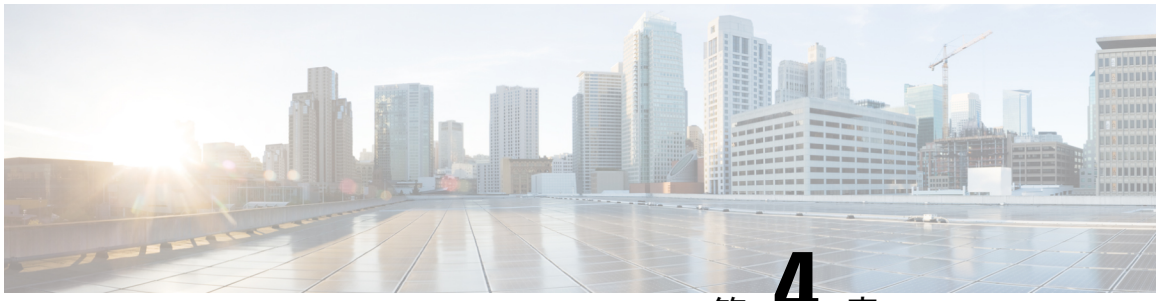
NAT 全体に IP 電話を導入する方法の詳細については、https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/12-4t/nat-12-4t-book.pdf を参照してください。

# IPSec と NAT の透過性

IPSec NAT の透過表示機能では、NAT と IPSec の間で既知の多くの非互換性に対処することで、ネットワーク内の NAT またはポートアドレス変換（PAT）ポイントを経由する IPSec トラフィックのサポートが導入されます。VPN デバイスは、NAT トラバーサル（NAT-T）を自動的に検出します。両方の VPN デバイスが NAT-T に対応している場合、NAT-T は自動的に検出され、自動的にネゴシエートされます。

# その他の IPSec リファレンス

- IPSec アーキテクチャ：https://technet.microsoft.com/en-us/library/bb726946.aspx
- Windows Server：https://docs.microsoft.com/en-us/windows-server/get-started/server-basics
- Windows ファイアウォールおよび IPSec：https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/windows-firewall-with-advanced-security



第 4 章

# 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ついて

ユニファイド コンタクト センター セキュリティ ウィザードは、ステップバイステップのウィザードベースの方法でセキュリティ設定をシンプル化する Unified ICM/CCE 用のセキュリティ導入ツールです。

セキュリティウィザードでは、次の Unified ICM/CCE セキュリティ コマンドライン ユーティリティを実行できます。

- Windows ファイアウォール ユーティリティ
- ネットワーク分離ユーティリティ
- SQL 強化ユーティリティ

### 関連トピック

自動 SQL サーバの強化 （77 ページ）
ネットワーク分離ユーティリティを使用した IPSec
ウィンドウ サーバのファイアウォールの設定

# 設定と制約事項

次に、セキュリティウィザードの制限事項を示します。

- セキュリティウィザードは、ネットワーク上で実行されているアプリケーションに干渉しません。セキュリティウィザードは、アプリケーションのメンテナンスウィンドウでのみ実行します。これは、ネットワークセキュリティをセットアップするときに接続が中断される可能性があるからです。
- Unified ICM をネットワークにインストールした後は、ファイアウォールの設定ユーティリティとネットワーク分離ユーティリティを設定する必要があります。
- セキュリティウィザードでは、セキュリティを設定するために、コマンドラインユーティリティがシステム上にある必要があります。ウィザードは、ユーティリティがインストールされていない場合を検出し、ユーザに通知します。
- セキュリティウィザードは、すべての Unified ICM または Unified CCE サーバで実行できますが、ドメインコントローラ上では実行できません。

**関連トピック**

ネットワーク分離ユーティリティを使用した IPSec
ウィンドウ サーバのファイアウォールの設定

# ウィザードの実行

ICM-CCE-CCH のインストーラはセキュリティウィザードをインストールし、「%SYSTEMDRIVE%\CiscoUtils\UCCSecurityWizard」 ディレクトリに配置します。セキュリティウィザードの機能を使用するには、サーバ管理者である必要があります。

ウィザードは、**[開始（Start）]** > **[プログラム（Programs）]** > **[Cisco Unified CCE ツール（Cisco Unified CCE Tools）]** > **[セキュリティウィザード（Security Wizard）]** の下にインストールされたショートカットを使用して実行できます。

（注） ウィザードを使用する前に、ウィザードに含まれる各ユーティリティに関するこのガイドの章を読み、ユーティリティの機能を理解します。

セキュリティウィザードには、セキュリティユーティリティ（セキュリティ強化、Windows ファイアウォール、ネットワーク分離ユーティリティ、および SQL ユーティリティ）のメニューリストが表示されます。各ユーティリティは、1 回ずつ実行します。

メニューの選択を行き来して、各メニューの内容を理解できます。ただし、特定の機能の **[次へ（Next）]** ボタンをクリックした後、設定を完了するか **[キャンセル（Cancel）]** をクリックして **[ようこそ（Welcome）]** ページに戻ります。セキュリティウィザードには追加の説明があ

りません。各ユーティリティには、導入パネル、設定、確認パネル、およびステータスパネルがあります。

### 次のタスク

問題の原因となるデフォルトとは異なる値を選択すると、ウィザードに警告が表示されます。

まれに、バックエンドユーティリティ スクリプトが終了した場合は、UCCSecurityWizard フォルダに作成された一時テキストファイルは削除されません。このテキストファイルにはコマンドライン出力が含まれています。このファイルを使用して問題をデバッグできます。

# Windows ファイアウォールの構成

セキュリティ ウィザードのファイアウォールの設定パネルでは、次の操作を実行できます。

- Unified ICM または Unified CCE システム用 に Windows ファイアウォールを設定 します。
- 以前に適用したファイアウォール設定を元に戻します。
- Windows デフォルトに復元します。

> **警告** デフォルトの Windows ファイアウォール設定では、Unified ICM アプリケーションとの互換性 がありません。

- Windows ファイアウォールを無効にします。
- Unified ICM ファイアウォール 例外 XML ファイルを編集します。**[ICM ファイアウォール例外 XML の編集（Edit ICM Firewall Exceptions XML）]** ボタンをクリックすると、その XML ファイルがメモ帳で開きます。ファイルを保存し、ウィザードを続行する前に閉じてください。

Windows ファイアウォールの設定ユーティリティ：

- Unified ICM アプリケーションのインストール後に実行する必要があります。
- インストールされている Unified ICM コンポーネントを自動的に検出し、必要に応じて Windows ファイアウォールを設定します。
- VNC の例外などのカスタム例外を追加できます。
- すべての Unified ICM および Unified CCE サーバにデフォルトでインストールされます。

# ネットワーク分離設定パネル

セキュリティウィザードは、ネットワーク分離ユーティリティを初めて構成する場合、または既存のポリシーを編集する場合に、ネットワーク分離ユーティリティの導入に最適です。

セキュリティ ウィザード インターフェイスには、次の利点があります。

- 設定パネルは、入力に応じて動的に変更されます。
- 現在のポリシーを参照できます。
- 現在のネットワーク分離設定を表示し、必要に応じて編集できます。
- 単一のセキュリティ ウィザード パネルで複数の境界デバイスを追加できます。CLI に複数の境界デバイスを追加するには、追加するデバイスごとに別個のコマンドを作成します。

信頼済みデバイスとして設定されている各サーバでネットワーク分離ユーティリティを実行します。境界デバイスでユーティリティを実行する必要はありません。

使用可能な場合は、設定パネルには、XML ネットワーク分離構成ファイルに保存された最後の構成（Windows IPSec ポリシーストアではない）が表示されます。

信頼済みデバイスパネル：

- ポリシーのステータスを表示します。
- ポリシーを有効化、変更、参照、または無効化するために使用できます。

（注） 信頼済みとしてデバイスを有効化または変更するには、36 文字以上の事前共有キーを入力します。入力したキーの長さは、入力に伴い、正しい長さが入力されるように更新されます。

（注） ネットワーク分離ユーティリティポリシーは、コマンドラインでのみ完全に削除できます。

すべての信頼済みデバイスで同じ事前共有キーを使用しない場合は、信頼済みデバイス間のネットワーク接続が失敗します。

境界デバイスパネルで、次の操作を実行できます。

- 前のパネルでの選択に基づいて、パネルを動的に修正します。
  - 前のパネルでポリシーを無効にした場合、このパネルの要素は無効になります。
  - 前のパネルで参照オプションを選択した場合は、ブラウズ目的でデバイスの境界リストだけが有効になります。
- 複数の境界デバイスを追加または削除できます。
- チェックボックスを使用して、動的に検出されたデバイスを追加できます。

- ポート、IPアドレス、またはサブネットを介して、手動で指定されたデバイスを追加できます。デバイスの指定後、**[デバイスの追加（Add Device）]** をクリックしてデバイスを追加します。

  [追加（Add）] ボタンはデータを検証し、重複エントリをチェックしてから、詳細を確認します。

- デバイスリストでデバイスを選択し、**[選択項目の削除（Remove Selected）]** をクリックして、境界デバイスからデバイスを削除できます。

次に基づいて例外を絞り込みできます。

- トラフィックの方向：アウトバウンドまたはインバウンド
- プロトコル：TCP、UDP、ICMP
- 任意のポート（TCP または UDP が選択されている場合のみ）
- 特定のポートまたはすべてのポート

# SQL の強化

SQL 強化ウィザードを使用すると、次の処理を実行できます。

- SQL サーバのセキュリティ強化を適用します。
- 以前に適用した強化からアップグレードします。
- 以前に適用した強化をロールバックします。

[SQL 強化セキュリティ アクション パネルでは、次の操作を実行できます。

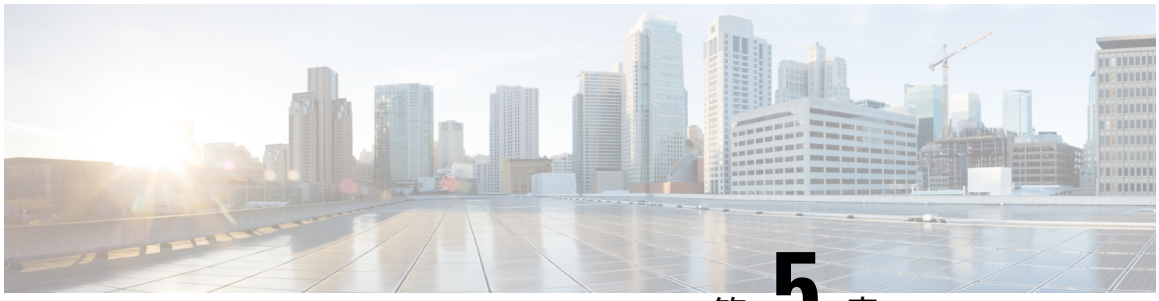
- SQL サーバのセキュリティ強化の適用またはアップグレード
- 以前に適用された SQL サーバのセキュリティ強化のロールバック

（注） SQL サーバのセキュリティ強化の履歴がない場合、または強化がすでにロールバックされている場合、このロールバックは無効になります。

パネルの上部にあるステータスバーは、設定の完了を示します。

**関連トピック**

自動 SQL サーバの強化 （77 ページ）



第 5 章

# ネットワーク分離ユーティリティを使用した IPSec



## IPsec

インターネット プロトコル セキュリティ（IPSec）は、Microsoft、Cisco およびその他の多くのインターネット技術特別調査委員会（IETF）の貢献企業によって共同で開発されたセキュリティ標準です。エンドポイントやゲートウェイなど、任意の2つのノード間で整合性（認証）と暗号化を提供します。IPSec は、ネットワークのレイヤ 3 で動作するため、アプリケーションに依存しません。IPSec は、アプリケーションに依存しないアプリケーションノード間でセキュリティを提供する Unified ICM のような大規模で分散されたアプリケーションに役立ちます。

詳細については、https://docs.microsoft.com/en-us/windows/desktop/fwp/ipsec-configurationを参照してください。

## 手動導入またはネットワーク分離ユーティリティ

ネットワーク分離ユーティリティは、IPSec を使用して Unified ICM/Unified CCE 環境を保護するための作業の大半を自動化します。ネットワーク分離ユーティリティは、Unified ICM/Unified

CCE サーバとの間でネットワークトラフィック全体を保護する事前設定済みの IPSec ポリシーを導入します。ネットワーク接続は、同じポリシーを共有するサーバ、または例外として明示的にリストされているサーバにのみ制限されます。

選択した通信パス間でのみネットワークトラフィックを保護する場合は、ネットワーク分離ユーティリティを使用しません。

**関連トピック**

ネットワーク分離ユーティリティを使用した IPSec

# シスコのネットワーク分離ユーティリティ

シスコネットワーク分離ユーティリティは、Windows IPSec 機能を使用して、Unified ICM デバイスをネットワークの他の部分から分離します。Unified ICM デバイスの例には、ルータ、ロガー、および周辺ゲートウェイデバイスが含まれます。このユーティリティは、ネットワーク分離 IPSec ポリシーを作成し、Unified ICM デバイスを信頼済みとして設定し、信頼済みデバイス間のすべてのトラフィックを認証およびオプションで暗号化します。信頼済みデバイス間のトラフィックは、設定を追加することなく通常通り継続して流れます。境界デバイス間のトラフィックとして分類されていない限り、信頼済みデバイス以外のデバイス間のすべてのトラフィックは拒否されます。

境界デバイスは、信頼済みデバイスへのアクセスが許可されている IPSec ポリシーを持つデバイスです。通常、これらのデバイスには、ドメインコントローラ、Unified CM、デフォルト ゲートウェイ デバイス、有用性デバイス、リモート アクセス コンピュータが含まれます。

信頼済みデバイスごとに、境界デバイスのリストが用意されています。個別の IP アドレスまたはサブネットまたはポートが、境界デバイスを定義します。

ネットワーク分離ポリシーでは、整合性と暗号化に IPsec ESP（カプセル化セキュリティ ペイロード）プロトコルが使用されます。導入される暗号スイートは次のとおりです。

- IP トラフィックセキュリティ：
  - 整合性アルゴリズム：SHA1
  - 暗号化アルゴリズム：3DES
- キー交換セキュリティ：
  - 整合性アルゴリズム：SHA1
  - 暗号化アルゴリズム：3DES（オプション）
  - Diffie-Hellman グループ：高（2048 ビットキー）

# ネットワーク分離ユーティリティ情報

次のセクションでは、ネットワーク分離ユーティリティの設計と動作について説明します。

# IPSec 用語

次のリストには、IPSec の基本用語の定義が含まれます。

**ポリシー**

IPSec ポリシーは、IPSec の動作を決定する 1 つ以上のルールの集大集です。Windows Server では複数のポリシーを作成できますが、一度に割り当てられるポリシー（アクティブ）は 1 つのみです。

**ルール**

各ルールは、FilterList、FilterAction、認証方式、TunnelSetting、および ConnectionType の各ルールで構成されます。

**フィルタリスト**

フィルタリストは、送信元および宛先の IP アドレス、プロトコル、およびポートに基づいて IP パケットと一致するフィルタのセットです。

**フィルタ アクション**

フィルタアクションは、フィルタリストで識別され、データ送信のセキュリティ要件を定義します。

**認証方式**

認証方式では、関連付けられたルールを適用する通信で ID を検証する方法の要件を定義します。

Microsoft Windows IPSec に関する用語の詳細については、次を参照してください。

https://docs.microsoft.com/en-us/windows/desktop/fwp/ipsec-configuration.

# ネットワーク分離ユーティリティプロセス

信頼済みデバイスごとにネットワーク分離ユーティリティを個別に実行します。境界デバイスでこのユーティリティを実行**しないでください**。

境界デバイス間のトラフィックを許可するには、信頼済みデバイスごとに [境界デバイス（Boundary Device）] リストを手動で設定します。

デバイスへのネットワーク分離 IPSec ポリシーの導入後、そのデバイスは [信頼済み（Trusted）] に設定されます。トラフィックは、設定を追加することなく、そのデバイスと他の信頼済みデバイスとの間で自由にフローします。

ネットワーク分離ユーティリティを実行すると、次の動作が実行されます。

1. そのコンピュータ上にすでに存在する IPSec ポリシーを削除します。この削除により競合が回避され、新しいポリシーがすべての Unified ICM デバイスと一致して導入が成功します。
2. Windows IPSec ポリシーストアに Cisco Unified Contact Center（ネットワーク分離）IPSec ポリシーを作成します。

3. ポリシーに対して次の 2 つのルールを作成します。

   1. **信頼済みデバイスのルール**

      このルールには、次の項目が含まれます。

      - **信頼済みデバイスのフィルタリスト**：すべてのトラフィック。すべてのトラフィックに一致する 1 つのフィルタ。
      - **信頼済みデバイスのフィルタアクション**：セキュリティが必要です。整合性アルゴリズム SHA1 を使用して認証し、必要に応じて暗号化アルゴリズム 3DES を使用して暗号化します。
      - **認証方法**：コンピュータ間の信頼を作成するために使用される認証方法は、事前共有キーです。

        事前共有キーは、二重引用符を除く一文字列の単語、数字、または文字を使用できます。このキーの最小長は 36 文字です。

   2. **境界デバイスルール**

      このルールには、次の項目が含まれます。

      - **境界デバイスフィルタリスト**：（デフォルトでは空）
      - **境界デバイスフィルタアクション**：IPSecポリシーなしでトラフィックを許可します。境界デバイスでは、信頼済みデバイスとの通信に IPSec が必要ではありません。

4. ネットワーク 分離ユーティリティは、Cisco Unified Contact Center の IPSec ポリシーのコピーをネットワーク分離ユーティリティフォルダ（`<system drive>:\CiscoUtils\NetworkIsolation\CiscoICMIPsecConfig.XML`）にある XML ファイルに保存します。

   XML ファイルには、ポリシーの状態と境界デバイスのリストが格納されます。事前共有キーは保存されません。

5. ネットワーク分離ユーティリティは、`<SystemDrive>:\CiscoUtils\NetworkIsolation\Logs\CiscoICMNetworkIsolation.log` にあるログファイルに、すべてのコマンドとアクションを記録します。

   このユーティリティは、ログファイルのコピーを 1 つ保持し、すべてのコマンドとアクションを以前に作成したログに追加します。

# トラフィックの暗号化とネットワーク分離ポリシー

ネットワーク分離ポリシーでは、同じ事前共有キーを持つコンピュータのみを操作できます。ネットワーク分離機能を使用すると、外部のハッカーは信頼できるコンピュータにアクセスできません。ただし、暗号化を有効にしない場合は、ハッカーはそのコンピュータからトラフィッ

クが行き来しているのを見ることができます。したがって、そのトラフィックを暗号化することを検討してください。

（注）
- 1 つの信頼済みデバイスに対するトラフィックは、単独では暗号化できません。すべての信頼済みデバイス上、またはデバイス上ではないトラフィックを暗号化します。1 つのコンピュータだけがトラフィックを暗号化している場合は、他の信頼済みデバイスのいずれもトラフィックを理解しません。
- 暗号化で IPSec が有効になっている場合は、暗号化オフロード NIC を使用します。そうすることで、暗号化ソフトウェアがパフォーマンスに影響を与えるのを防ぐことができます。

**関連トピック**

IPSec の概要 （27 ページ）
IPSec および NAT のサポート

# ネットワーク分離機能の導入

次のセクションでは、展開プランの設計時に注意する必要がある問題について説明します。

**関連トピック**

境界デバイスと Unified CCE （49 ページ）
デバイスの双方向の通信 （48 ページ）
重要な導入のヒント （45 ページ）
導入例 （45 ページ）

## 重要な導入のヒント

境界デバイスの設定は不要です。すべての設定は信頼済みデバイスで行われます。ネットワーク分離ユーティリティは、信頼済みデバイスを他の信頼済みデバイスや境界デバイスとやり取りするために設定します。ネットワーク分離機能は、一度に 1 つのデバイスに適用されます。この機能により、適用後に他のデバイスとの通信が瞬時に制限されます。したがって、この機能を使用する前に、この機能の導入方法を慎重に計画しないと、ネットワークの動作を誤って停止する可能性があります。ネットワーク分離機能を実装する前に、導入計画を作成します。このため、この機能はメンテナンスウィンドウでのみ導入し、導入計画を作成する前に警告を確認してください。

**関連トピック**

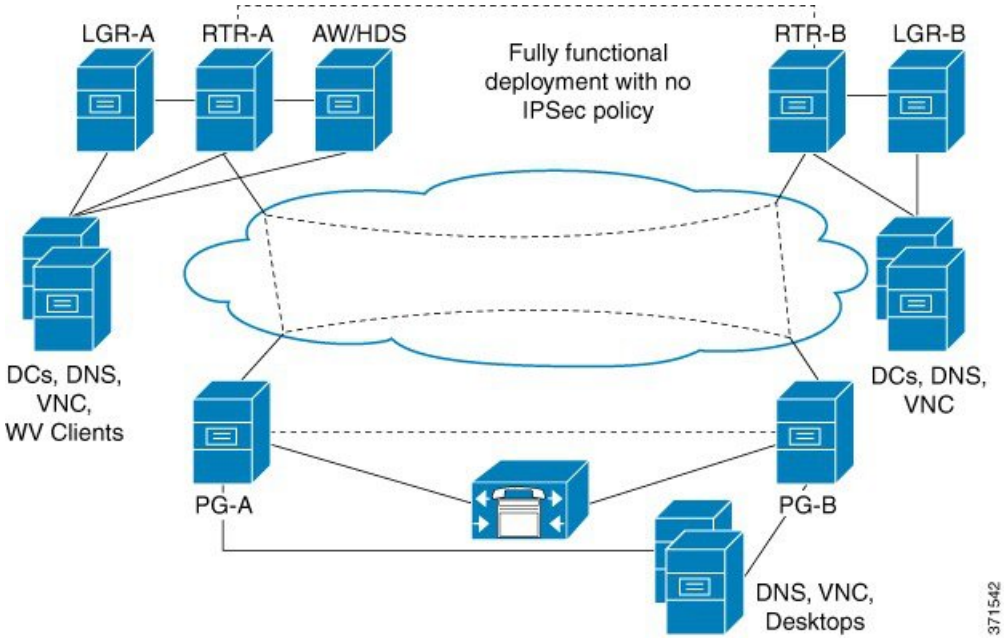
注意事項 （50 ページ）

## 導入例

導入例の 1 つを以下に示します。

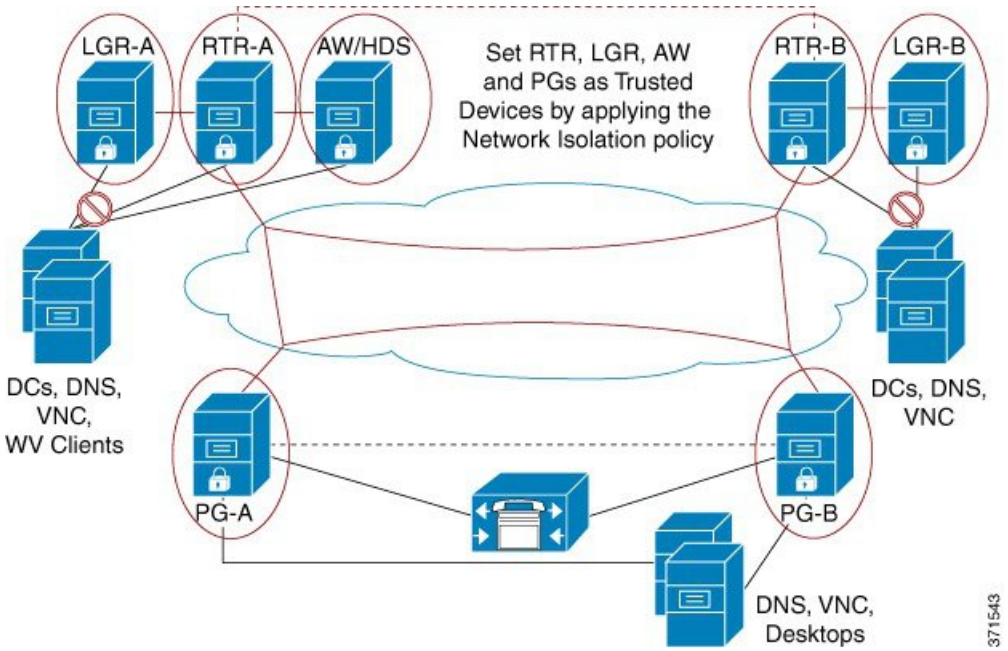
1. IPSec ポリシーを導入できる、完全に機能する Unified ICM または Unified CCE システムから開始します。

**図 *2:* ユニファイド コンタクト センターのシステムの例**



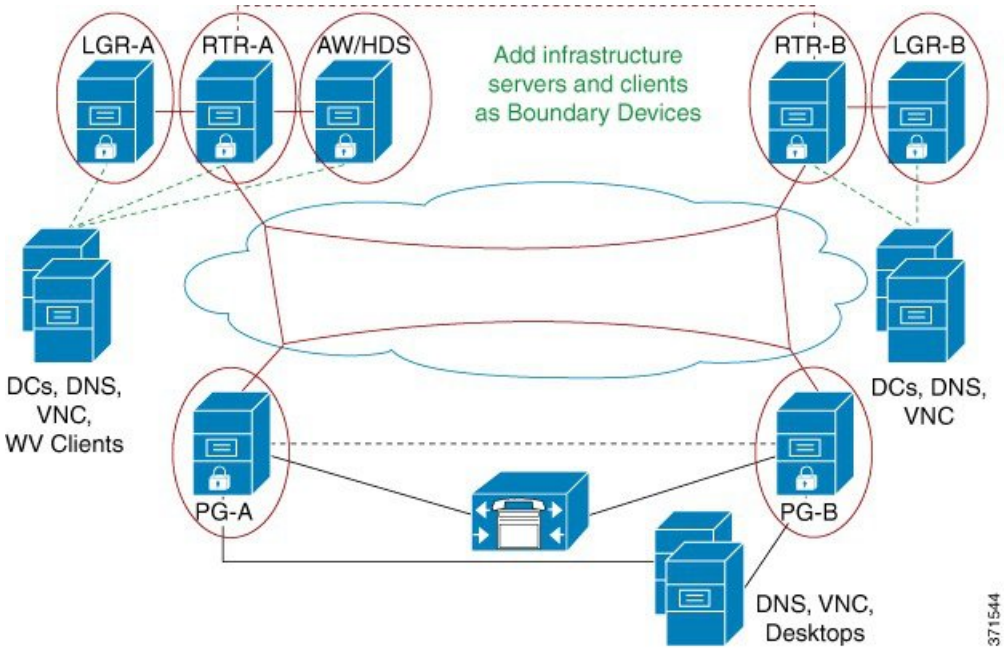

2. ネットワーク分離ユーティリティを CallRouter、ロガー、管理 & データサーバおよび PG に実行することで、それぞれを信頼済みデバイスとして設定します。

**図 *3:* 例：信頼済みデバイスの追加**



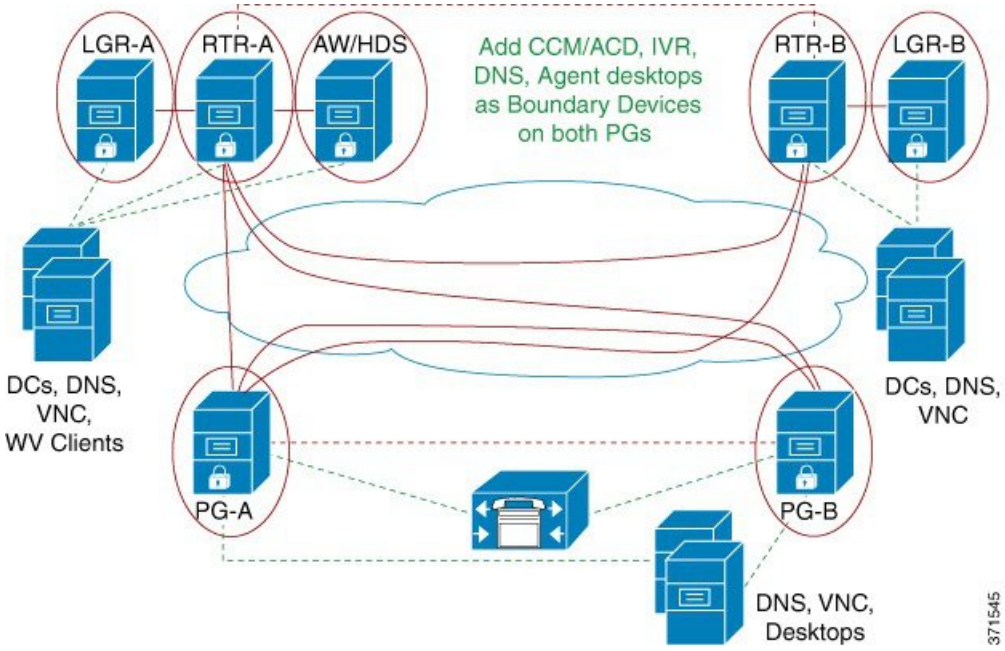
3. インフラストラクチャサーバとクライアントを境界デバイスとして追加します。

**図 *4*：例：境界デバイスの追加**




4. Unified Communications Manager または ACD サーバ、DNS、およびエージェントデスクトップを両方の PG に境界デバイスとして追加します。

**図 *5*：例：*PG* への境界デバイスの追加**



完了すると、すべてのユニファイド コンタクト センターの信頼済みデバイスが相互にのみ通信し、それぞれの境界デバイス（ドメインコントローラ、DNS、Unified Communications Managerなど）と通信します。外部からのネットワーク攻撃は、境界デバイスを介してルーティングされていない限り、信頼済みデバイスに到達できません。

# デバイスの双方向の通信

この表は、Unified CCE 導入での 2 者間通信の要件を示します。対象のデバイスを信頼済みデバイスまたは境界デバイスとして設定できます。

| **Unified CCE コンポーネント** | **対象デバイス** |
|---|---|
| CallRouter | CallRouter（冗長システムのもう一方の側） |
| | ロガー |
| | 管理&データサーバ/履歴データベースサーバ |
| | NAM ルータ |
| | 周辺機器ゲートウェイ（冗長システムの両側） |
| | アプリケーション ゲートウェイ |
| | データベースサーバー |
| | ネットワークゲートウェイ（Network Gateway） |
| ロガー | 履歴データベースサーバ/管理&データサーバ |
| | CallRouter |
| | Campaign Manager |
| | ダイヤラ |
| Peripheral Gateway | マルチチャネル/マルチメディアサーバ |
| | CallRouter（冗長システムの両側） |
| | 周辺機器ゲートウェイ（冗長システムのもう一方の側） |
| | Unified Communications Manager |
| | 管理&データサーバレガシーの PIMS/スイッチ |

| Unified CCE コンポーネント | 対象デバイス |
|---|---|
| 管理&データサーバ/履歴データベースサーバ | マルチチャネル/マルチメディアサーバ |
| | ルータ |
| | Logger |
| | カスタム アプリケーション サーバ |
| | CON API クライアント |
| | インターネット スクリプト エディタ クライアント/Web スキリング |
| | サードパーティ クライアント/SQL パーティ |
| 管理サーバ、リアルタイムおよび履歴データサーバ、および詳細データサーバ（AW-HDS-DDS） | マルチチャネル/マルチメディアサーバ |
| | ルータ |
| | Logger |
| | カスタム アプリケーション サーバ |
| | インターネット スクリプト エディタ クライアント/Web スキリング |
| | サードパーティ クライアント/SOL パーティ |

# 境界デバイスと Unified CCE

この表は、Unified CCE 導入で通常必要な境界デバイスの一覧を示します。

| 境界デバイス | 設定例 |
|---|---|
| ドメインコントローラ：RTR、LGR、管理 & データサーバまたは HDS、PG | • 境界デバイス：ドメインコントローラの IP アドレス<br>• トラフィックの方向：アウトバウンド<br>• プロトコル；任意<br>• ポート：適用されない |
| DNS、WINS、デフォルトゲートウェイ | — |

| 境界デバイス | 設定例 |
|---|---|
| リモートアクセスまたはリモート管理ソフトウェア：信頼済みのすべてのデバイス（VNC、pcAnywhere、リモートデスクトップ接続、SNMP）など | *VNC*：<br>• 境界デバイス：任意のホスト<br>• トラフィックの方向：インバウンド<br>• [プロトコル（Protocol）]：TCP<br>• ポート：5900 |
| PG の Unified Communications Manager クラスタ | • 境界デバイス：特定の IP アドレス（またはサブネット）<br>• トラフィックの方向：アウトバウンド<br>• [プロトコル（Protocol）]：TCP<br>• ポート：すべてのポート |
| [エージェントのデスクトップ（Agent Desktops）] | *Finesse* サーバ：<br>• 境界デバイス：サブネット<br>• トラフィックの方向：インバウンド<br>• [プロトコル（Protocol）]：TCP<br>• ポート：42028 |

# 注意事項

ポリシーがすべてのマシンに同時に適用されるよう、導入を慎重に計画します。そうでないと、誤ってデバイスを分離する場合があります。

注意点は次のとおりです。

- 

**重要** ポリシーをリモートで有効にすると、リモートアクセス用の境界デバイスリストにプロビジョニングが行なわれていない限り、リモートアクセスがブロックされます。リモートでポリシーを有効にする前に、リモートアクセス用の境界デバイスを追加します。

- 

**重要** 境界デバイスとしてすべてのドメインコントローラを追加しないと、ドメインログインが失敗します。ドメインログインが失敗した場合は、Unified ICM サービスも開始に失敗するか、ログイン時間の遅延を確認できます。ドメインコントローラのこのリストには、Unified ICM がインストールされているすべてのドメインが含まれます。このリストには、Web セットアップツール、設定ユーザ、およびスーパーバイザが存在するすべてのドメインも含まれています。

- 境界デバイスとして新しいデバイスを追加するには、IPSec を使用せずにこの新しいデバイスにアクセスする必要があるすべての信頼済みデバイスのポリシーを変更する必要があります。
- すべての信頼済みデバイスで事前共有キーの変更を呼び出す必要があります。
- 1 つの信頼済みデバイスだけで暗号化を有効にした場合、ネットワークトラフィックが暗号化されているため、そのデバイスは他の信頼済みデバイスと通信できません。信頼済みデバイスのすべてで暗号化を有効または無効にします。
- Windows IPSec ポリシー MMC プラグインを使用して IPSec ポリシーを変更することはできません。ネットワーク分離ユーティリティは、ポリシーの独自のコピーを保持します。ネットワーク分離ユーティリティを実行すると、ユーティリティ以外（またはセキュリティウィザード）で行われた変更を無視して、ユーティリティは最後に保存された設定に戻ります。
- ネットワーク分離ユーティリティは、ネットワーク上で実行されるアプリケーションに干渉しません。ただし、ユーティリティはアプリケーションのメンテナンスウィンドウでのみ実行します。このユーティリティは、ネットワークセキュリティを設定するときに接続が中断される可能性があるからです。
- ネットワークがファイアウォールの背後にある場合は、次の方法でファイアウォールを設定します。
  - IP プロトコル番号として、ESP（カプセル化セキュリティプロトコル）である 50 を許可します。
  - IKE プロトコルに対して、ポート 500 で UDP の送信元と宛先のトラフィックを許可します。
- NAT プロトコルを使用している場合は、ファイアウォールを設定して、UDP-ESP のカプセル化用に UDP 送信元と宛先ポート 4500 でトラフィックを転送します。
- Web サーバポートなど、アプリケーションポートの使用法に加えた変更は、ポリシーにも反映する必要があります。
- Unified ICM またはユニファイドコンタクトセンターアプリケーションが設定され、動作を確認した後に、ネットワーク分離ポリシーを導入します。

- 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インベントリについては、次のドキュメントを参照してください。
  - *Cisco Unified Contact Center Enterprise Solutions* ポート使用状況ガイド https://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_installation_and_configuration_guides_list.html
  - https://www.cisco.com/en/us/products/sw/voicesw/ps556/prod_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。

# バッチ導入

すべての信頼済みデバイスに共通の境界デバイスを追加する必要が生じた場合、導入の迅速化に役立つ次の XML ファイルを使用できます。

```
<system drive>:\CiscoUtils\NetworkIsolation\CiscoICMIPsecConfig.XML
```

この XML ファイルには、1 つの信頼済みデバイスに対する境界デバイスのリストとポリシー状態が含まれています。このファイルを使用すると、他の信頼済みデバイス上でポリシーを複製できます。

たとえば、信頼済みデバイスとして PG を設定する場合は、最初に 1 つの Unified ICM PG の設定を完了できます。次に、その PG から他の Unified ICM PG に XML ファイルをコピーできます。その後、他の PG で分離ユーティリティ（またはセキュリティウィザード）を実行して、すべての PG 上で同じ境界デバイスのリストを作成します。

# ネットワーク分離ユーティリティのコマンドラインシンタックス

ネットワーク分離ユーティリティは、コマンドラインまたは Unified Contact Center Security ウィザードから実行できます。

（注） 最初のポリシーの作成または変更には、セキュリティウィザードを使用します。コマンドラインを使用して、バッチ導入ができます。

コマンドラインからユーティリティを実行するには、ユーティリティがある C:\CiscoUtils\NetworkIsolation ディレクトリに移動し、そこから実行します。

C:\CiscoUtils\NetworkIsolation>

信頼済みデバイスでポリシーを有効にするためのコマンドラインシンタックスを次に示します。

```
cscript ICMNetworkIsolation.vbe <arguments>
```

（注） スクリプトを呼び出す場合は、**cscript** を使用する必要があります。

複数のフィルタを使用して、境界デバイスを追加できます。次の条件でフィルタリングできます。

- **IP アドレス**：個々の IP アドレス、またはデバイスのサブネット全体
- **動的に検出されたデバイス**：DNS、WINS、DHCP、デフォルトゲートウェイ

  Windows は、これらのデバイスの IP アドレスを動的に検出し、フィルタリストの更新を維持します。
- **トラフィックの方向**：インバウンドまたはアウトバウンド
- **プロトコル**：TCP、UDP、ICMP、または任意のプロトコル
- **ポート**（TCP または UDP が選択されている場合のみ）：特定のポートまたはすべてのポート

シンタックス内：

- 山カッコ <>= 必須
- 角カッコ [ ] = 任意
- パイプまたはバー | = バーの間のいずれかの項目

次の表に、コマンドのすべての使用に関するコマンドシンタックスを示します。

表 *1:* 各引数のネットワーク分離ユーティリティ コマンド シンタックス

| 引数名 | 構文と例 | 機能 |
|---|---|---|
| HELP | cscript ICMNetworkIsolation.vbe /? | コマンドのシンタックスを表示します。 |
| ENABLE POLICY | cscript ICMNetworkIsolation.vbe /enablePolicy <36+ characters PreSharedKey in double quotes> [/encrypt]<br>（注） PresharedKey で使用する唯一の非対応文字は二重引用符です。その文字はキーの始めと終わりをマークします。キー内の他の任意の文字を入力できます。<br>次に例を示します。<br>`cscript ICMNetworkIsolation.vbe /enablePolicy 「myspecialpresharedkey123456789mnbvcx」` | 新しいポリシーを作成するか、保存されているポリシー XML ファイルから既存のポリシーを有効にします。<br>必要に応じて、ネットワーク トラフィック データの暗号化を有効にします。<br>Windows IPSec ポリシーストアに新しいポリシーを作成し、XML ファイルにリストされているすべての境界デバイスを追加します。XML ファイルが存在しない場合、新しい XML ファイルが作成されます。/encrypt オプションは、XML ファイルで設定されている値を上書きします。 |
| （注） 追加、削除、および削除の引数では、XML ファイルのバックアップを作成し、その機能を実行する前に xml.lastconfig という名前を付します。 | | |

| 引数名 | 構文と例 | 機能 |
|---|---|---|
| ADD BOUNDARY | cscript ICMNetworkIsolation.vbe /addBoundary DNS\|WINS\|DHCP\|GATEWAY<br>次に例を示します。<br>`cscript ICMNetworkIsolation.vbe /addBoundary DNS`<br>この例では、DNS サーバを境界デバイスリストに追加します。 | 指定されたデバイスの種類を、境界デバイスリストに追加します。<br>このタイプは、DNS、WINS、DHCP、またはGATEWAYとして指定できます。<br>このユーティリティは、DNS、WINS、DHCP、および GATEWAY をそれぞれドメインネームシステム（DNS）デバイス、Windows インターネット ネーム サービス（WINS）デバイス、Dynamic Host Configuration Protocol（DHCP）デバイス、デフォルトゲートウェイ（GATEWAY）デバイスとして認識します。<br>Windows オペレーティングシステムは、上記のタイプの各デバイスの IP アドレスの変更を動的に検出し、それに応じて境界フィルタリストを動的に更新します。 |
| | cscript ICMNetworkIsolation.vbe /addAnyHostBoundary <Outbound\|Inbound> <TCP\|UDP> <PortNumber><br>次に例を示します。<br>`cscript ICMNetworkIsolation.vbe /addAnyHostBoundary Inbound TCP 5900`<br>この例では、すべてのマシンからの VNC アクセスを許可します。 | 次の基準に一致するデバイスのリストが、境界デバイスに追加されます。<br>• 指定されたトラフィックの方向の 1 つ（アウトバウンドまたはインバウンド）。<br>• 指定されたプロトコルの 1 つ、Transmission Control Protocol（TCP）または User Datagram Protocol（UDP）。<br>• 指定されたポート。 |

| 引数名 | 構文と例 | 機能 |
| --- | --- | --- |
| | cscript ICMNetworkIsolation.vbe /addIPAddrBoundary <IP address> <Outbound\|Inbound> <TCP\|UDP\|ICMP\|Any> [All\|PortNumber]<br>次に例を示します。<br>`cscript ICMNetworkIsolation.vbe /addIPAddrBoundary 10.86.121.160 Outbound Any`<br>この例では、指定されたIPアドレスを持つデバイスへのすべてのアウトバウンドトラフィックを許可します。 | 次の構成を持つデバイスのIPアドレスが、境界デバイスのリストに追加されます。<br>• （必須）指定された IP アドレス。<br>• （必須）指定されたトラフィックの方向の 1 つ（アウトバウンドまたはインバウンド）。<br>• （必須）指定されたプロトコル（必須）：Transmission Control Protocol（TCP）、User Datagram Protocol（UDP）、Internet Control Message Protocol（ICMP）、または任意のプロトコル。<br>• （任意）選択したプロトコルがTCPまたはUDPの場合、任意のポートまたは指定されたポート。 |
| | cscript ICMNetworkIsolation.vbe /addSubnetBoundary <StartingIP address> <Subnet Mask> <Outbound\|Inbound> <TCP\|UDP\|ICMP\|Any> [All\|PortNumber] | |

| 引数名 | 構文と例 | 機能 |
| --- | --- | --- |
| | | 次の構成を持つサブネットを、境界デバイスリストに追加します。<br>• （必須）次に指定した範囲の開始 IP アドレス。<br>• （必須）指定されたサブネットマスク（アドレス空間内の論理的なアドレスの範囲）。<br>• （必須）指定されたトラフィックの方向の 1 つ（アウトバウンドまたはインバウンド）。<br>• （必須）指定されたプロトコル、Transmission Control Protocol（TCP）、User Datagram Protocol（UDP）、Internet Control Message Protocol（ICMP）、または任意のプロトコル。<br>• （任意）プロトコルとして TCP または UDP が選択された場合、任意のポートまたは指定されたポート。 |

| 引数名 | 構文と例 | 機能 |
|---|---|---|
| REMOVE BOUNDARY | cscript ICMNetworkIsolation.vbe /removeBoundary DNS\|WINS\|DHCP\|GATEWAY<br>次に例を示します。<br>`cscript ICMNetworkIsolation.vbe /removeBoundary GATEWAY` | 指定されたデバイスを境界デバイスリストから削除します。<br>このタイプは、DNS、WINS、DHCP、またはGATEWAYとして指定できます。<br>このユーティリティは、DNS、WINS、DHCP、および GATEWAY をそれぞれドメインネームシステム（DNS）デバイス、Windows インターネット ネーム サービス（WINS）デバイス、Dynamic Host Configuration Protocol（DHCP）デバイス、デフォルトゲートウェイ（GATEWAY）デバイスとして認識します。<br>Windows は、上記のタイプの各デバイスの IP アドレスの変更を動的に検出し、それに応じて境界フィルタリストを動的に更新します。 |
| | cscript ICMNetworkIsolation.vbe /removeAnyHostBoundary <Outbound\|Inbound> <TCP\|UDP> <PortNumber><br>次に例を示します。<br>`cscript ICMNetworkIsolation.vbe /removeAnyHostBoundary Inbound TCP 5900` | 指定された IP アドレスにあるホストデバイスが、次の基準に一致すると、境界デバイスリストから削除されます。<br>• 指定されたトラフィックの方向の 1 つ（アウトバウンドまたはインバウンド）。<br>• 指定されたプロトコル（TCP または UDP）の 1 つ。<br>• インターネットトラフィック用に指定されたポート番号。 |
| | cscript ICMNetworkIsolation.vbe /removeIPAddrBoundary <IP address> <Outbound\|Inbound> <TCP\|UDP\|ICMP\|Any> [All\|PortNumber]<br>次に例を示します。<br>`cscript ICMNetworkIsolation.vbe /removeIPAddrBoundary 10.86.121.160 Outbound Any` | |

| 引数名 | 構文と例 | 機能 |
| --- | --- | --- |
| | | 指定されたIPアドレスにあるデバイスで、次の設定がされているものが境界デバイスリストから削除されます。<br>• （必須）指定された IP アドレス。<br>（必須）指定されたトラフィックの方向の 1 つ（アウトバウンドまたはインバウンド）。<br>• （必須）指定されたプロトコル（TCP、UDP、ICMP、または任意のプロトコル）の 1 つ。<br>• （任意）TCP または UDP が指定したプロトコルの場合、任意のポートまたは指定されたポート。 |
| | cscript ICMNetworkIsolation.vbe /removeSubnetBoundary <StartingIP address> <Subnet Mask> <Outbound\|Inbound> <TCP\|UDP\|ICMP\|Any> [All\|PortNumber]<br>次に例を示します。<br>`cscript ICMNetworkIsolation.vbe /removeSubnetBoundary 10.86.0.0.255.255.0.0 Inbound Any` | 指定されたIPアドレスにあるすべてのデバイスで、次の設定がされているものが境界デバイスリストから削除されます。<br>• （必須）次に指定した範囲の開始 IP アドレス。<br>• （必須）指定されたサブネットマスク。<br>• （必須）指定されたトラフィックの方向の 1 つ（アウトバウンドまたはインバウンド）。<br>• （必須）指定されたプロトコル（TCP、UDP、ICMP、または任意のプロトコル）の 1 つ。<br>• （任意）ポートまたは指定されたポート。 |

| 引数名 | 構文と例 | 機能 |
|---|---|---|
| DISABLE POLICY | `cscript ICMNetworkIsolation.vbe /disablePolicy` | コンピュータ上の Unified ICM ネットワーク分離 IPSec ポリシーを無効にします。ただし、ポリシーは削除されません。再有効化は可能です。<br>このオプションは、ネットワークの問題のトラブルシューティングに役立ちます。<br>ネットワーク接続に問題がある場合で、原因が分からない場合は、問題の原因を明確にするためにポリシーを無効にしてください。ポリシーが無効な状態でも問題が解決しない場合は、ポリシーが問題の原因ではありません。 |
| DELETE POLICY | `cscript ICMNetworkIsolation.vbe /deletePolicy` | Windows IPSec ポリシーストアから Unified ICM ネットワーク分離セキュリティポリシーを削除し、XML ファイルの名前を CiscoICMIPsecConfig.xml.lastconfig に変更します。 |

# ネットワーク分離 IPSec ポリシーのトラブルシューティング

ネットワーク分離 IPSec ポリシーのトラブルシューティングを行う場合は、次の手順を使用します。

### 手順

**ステップ 1** ポリシーを無効にして、発生したネットワークの問題がまだ存在するかどうかを確認します。ポリシーをシャットダウンすると、高度に分散されたシステムではオプションとして使用できない場合があります。そのため、Unified ICM アプリケーションの設定とテストの後にポリシーを導入することが重要です。

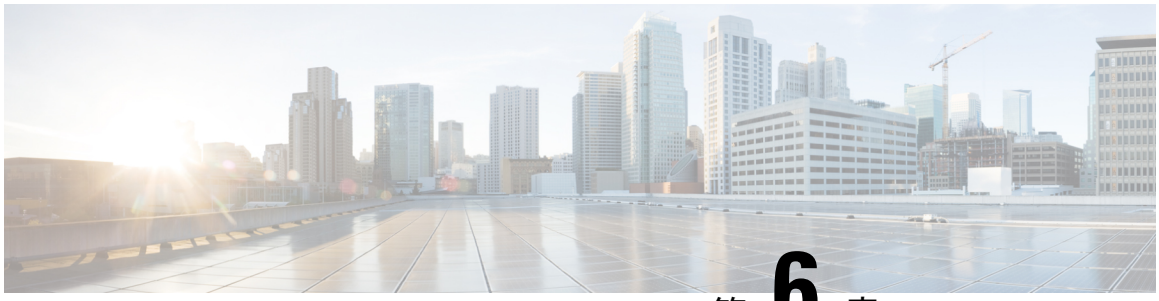
**ステップ 2** ポリシーの導入後に、境界デバイスの一覧で指定されている IP アドレスまたはポートが変更されたかどうかを確認します。

**ステップ 3** 通信パスが信頼済みおよび境界に設定されているかどうかを確認します。両方が重複すると、通信が失敗します。

**ステップ 4** <システムドライブ>:\CiscoUtils\NetworkIsolation\CiscoICMIPsecConfig.XML ファイルを参照して、必要な境界デバイスが境界デバイスとしてリストされているかどうかを確認します。セキュリティウィザードを使用して、境界デバイスを確認します。

**ステップ 5** Windows MMC コンソールから直接 IPSec ポリシーに加えた変更は、ユーティリティ（またはセキュリティウィザード）には反映されません。[ポリシーの有効化（Enable Policy）] オプションは、常に、XML ファイルに保存されている設定で IPSec ポリシーの保存内容を上書きします。

**ステップ 6** 記載されている警告を確認してください。



第 6 章

# ウィンドウ サーバのファイアウォールの設定



## Windows Server Firewall

Windows ファイアウォールはステートフル ホスト ファイアウォールで、すべての迷惑な着信トラフィックをドロップします。Windows ファイアウォールのこの動作は、迷惑な着信トラフィックを使用してコンピュータ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。

詳細については、https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/windows-firewall-with-advanced-security-design-guideを参照してください。

サーバ上で Windows ファイアウォールを有効にする場合は、CCE ソリューション コンポーネントに必要なすべてのポートを開きます。

シスコでは、Windows サーバ上の Unified CCE アプリケーションからのすべてのトラフィックを自動的に許可するユーティリティを提供しています。このユーティリティは、Contact Center Enterprise のソリューションで使用する一般的なサードパーティ製アプリケーションのポートを開くことができます。スクリプトは、ファイル `%SYSTEMDRIVE%\CiscoUtils\FirewallConfig\CiscoICMfwConfig_exc.xml`のポートのリストを読み取り、ディレクティブを使用してファイアウォールの設定を変更します。

このユーティリティは、アプリケーションからのすべてのトラフィックを許可し、関連するアプリケーションを除くプログラムとサービスのリストに追加します。除外アプリケーションが実行されると、Windows ファイアウォールはプログラムがリッスンするポートをモニタし、これらのポートを除外トラフィックのリストに自動的に追加します。

このスクリプトでは、アプリケーションポート番号を除外トラフィックのリストにアプリケーションポート番号を追加することで、サードパーティアプリケーションからのトラフィックを許可します。これらのポートを有効にするには、`CiscoICMfwConfig_exc.xml` ファイルを編集します。

デフォルトで有効になっているポートとサービス：

- 80/TCP および 443/TCP - HTTP および HTTPS（システムが IIS または TomCat [Web セットアップ用] をインストールする場合）
- Microsoft リモート デスクトップ
- ファイル共有および印刷共有の例外 - https://docs.microsoft.com/en-us/windows-server/storage/file-server/best-practices-analyzer/smb-open-file-sharing-ports を参照してください。

デフォルトで無効になっているファイアウォールのインバウンド：

- IPv6 用のコアネットワーキング
- コアネットワーキング - TCP の IPHTTPS
- コアネットワーキング - UDP 用の Teredo
- プライベートプロファイルのネットワーク検出
- Windows リモート管理 - ドメイン、プライベートプロファイル、およびパブリックプロファイルの HTTP

サービスはデフォルトでは無効：

- ファイルサーバのリモート管理

開くことができるオプションのポート：

- 5900/TCP - VNC
- 5800/TCP - Java ビューア
- 21800/TCP - Tridia VNC Pro（暗号化されたリモートコントロール）
- 5631/TCP および 5632/UDP - pcAnywhere

（注） XML ファイルを編集して、このリスト以外のポートベースの例外を追加できます。

ポートの使用法の完全なリストについては、https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html のページにある「*Cisco Unified Contact Center* ソリューションポート使用状況ガイド」を参照してください。

# Cisco ファイアウォール設定ユーティリティの前提条件

ファイアウォールの設定ユーティリティを使用する前に、次のソフトウェアをインストールします。

1. オペレーティングシステムの詳細については、https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html にある「互換性マトリクス」を参照してください。
2. Unified ICM/CCE コンポーネント

（注） Windows ファイアウォールの設定後にコンポーネントをインストールする場合は、Windows ファイアウォールを再設定します。このプロセスでは、前の設定を削除し、Windows ファイアウォールの設定ユーティリティを再び実行します。

# Cisco ファイアウォール設定ユーティリティの実行

Cisco ファイアウォール設定ユーティリティは、コマンドラインまたはユニファイド コンタクト センター セキュリティ ウィザードから実行できます。

警告 VNC などのリモートセッションからこのユーティリティを実行しようとすると、ファイアウォールの開始後に「ロックアウト」されることがあります。可能であれば、一部のリモートアプリケーションでネットワーク接続が切断される可能性があるから、コンピュータでファイアウォール関連の作業を実行します。

Unified ICM コンポーネントを実行している各サーバで、Cisco ファイアウォール設定ユーティリティを使用します。ユーティリティを使用するには、次の手順を実行します。

**手順**

**ステップ 1** すべてのアプリケーションサービスを停止します。

**ステップ 2** コマンドプロンプトから、`%SYSTEMDRIVE%\CiscoUtils\FirewallConfig\ConfigFirewall.bat` を実行します。

**ステップ 3** 初めてスクリプトを実行すると、スクリプトは `configfirewall.bat` を実行します。スクリプトは、同じコマンドを使用してアプリケーションを再設定する必要があります。指示がある場合は、スクリプトを再コマンドします。

**ステップ 4** [OK] をクリックします。

スクリプトは、Windows ファイアウォールサービスがインストールされていることを確認してから、実行されていない場合にこのサービスを開始します。

その後、スクリプトは `%SYSTEMDRIVE%\CiscoUtils\FirewallConfig\CiscoICMfwConfig_exc.xml` ファイルで指定されているポートとサービスでファイアウォールを更新します。

**ステップ 5** サーバをリブートします。

**関連トピック**

Windows ファイアウォールの構成 （37 ページ）

# 新しい Windows ファイアウォール設定の確認

次の手順に従って、Unified ICM のコンポーネントとポートが Windows ファイアウォール例外リストに追加されたことを確認できます。

**手順**

**ステップ 1** Windows サーバを 使用する場合は、**[開始（Start）] > [Windows 管理ツール（Windows Administrative Tools）]** を選択し、**[セキュリティが強化された Windows ファイアウォール（Windows Firewall with Advanced Security）]** を選択します。または、**[開始（Start）] > [コントロールパネル（Control Panel）] > [システムとセキュリティ（System and Security）] > [Windows ファイアウォール（Windows Firewall）]** を選択します。

[Windows ファイアウォール（Windows Firewall）] ダイアログボックスが表示されます。

**ステップ 2** **[例外（Exceptions）]** タブをクリックします。次に、Windows Server の [Windows ファイアウォール（Windows Firewall）] ダイアログボックスの **[インバウンドルールとアウトバウンドルール（Inbound and Outbound Rules）]** タブをクリックします。

**ステップ 3** 例外アプリケーションのリストをスクロールします。リストと、構成ファイルで定義されているポートまたはサービスに、いくつかの Unified ICM 実行ファイルが表示されます。

# Windows Server ファイアウォールと Active Directory の通信

ドメインコントローラ（DC）が LDAP や他のプロトコルとの通信に使用するポートを開いて、Active Directory がファイアウォール経由で通信可能か確認します。

ドメインと信頼関係のファイアウォールの設定に関する重要な情報については、Microsoft サポート技術情報の KB179442 の項目を参照してください。

DC と Unified ICM サービス間のセキュアな通信を確立するには、ファイアウォール上のアウトバウンドおよびインバウンドの例外に対して次のポートを定義します。

- すでに定義されているポート
- リモートプロシージャコール（RPC）で使用する変数ポート（高ポート）

# ドメイン コントローラ ポートの設定

外部 DC に対して複製可能な、緩衝地帯（DMZ）内のすべての DC に対して、以下のポート定義を定義します。ドメイン内のすべての DC 上のポートを定義します。

# 特定のスタティックポートへの FRS トラフィックの制限

特定の静的ポートへのファイル複製サービス（FRS）トラフィックの制限の詳細については、https://support.microsoft.com/en-in/help/832017/service-overview-and-network-port-requirements-for-windows を参照してください。

**手順**

**ステップ 1** **[レジストリ エディタ（Registry Editor）]**（regedit.exe）を起動します。

**ステップ 2** 位置を確認して、次のキーをレジストリにクリックします。
**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTFRS\Parameters**

**ステップ 3** 次のレジストリ値を追加します。

- 新規：**Reg_DWORD**
- 名前：**RPC TCP/IP ポートの割り当て**
- 値：**10000（10 進数）**

# 特定のポートへの Active Directory 複製トラフィックの制限

特定のポートへの Active Directory 複製トラフィックの制限の詳細については、https://support.microsoft.com/en-in/help/832017/service-overview-and-network-port-requirements-for-windows を参照してください。

**手順**

**ステップ 1** **[レジストリ エディタ（Registry Editor）]**（regedit.exe）を起動します。

**ステップ 2** 位置を確認して、次のキーをレジストリにクリックします。
**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters**

**ステップ 3** 次のレジストリ値を追加します。

- 新規：**Reg_DWORD**
- 名称：**RPC TCP/IP Port**
- 値：**10001**（**10 進数**）

# リモートプロシージャコール（RPC）ポートの割り当ての構成

RPC ポート割り当ての設定の詳細については、https://support.microsoft.com/en-in/help/832017/service-overview-and-network-port-requirements-for-windows を参照してください。

**手順**

**ステップ 1** **[レジストリ エディタ（Registry Editor）]**（regedit.exe）を起動します。

**ステップ 2** 特定して、次のキーをレジストリでクリックします：
**HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc**

**ステップ 3** **インターネット**キーを追加します。

**ステップ 4** 次のレジストリ値を追加します。

- Ports: **MULTI_SZ: 10002-10200**
- PortsInternetAvailable: **REG_SZ: Y**
- UseInternetPorts: **REG_SZ: Y**

# Windows ファイアウォールポート

ドメインと信頼のファイアウォールの設定に使用するポートの詳細については、Microsoft サポート技術情報の KB179442 の項目を参照してください。

***表 2 : Windows Server* ファイアウォールポート**

| サーバ ポート | [プロトコル（Protocol）] | プロトコル | サービス |
|---|---|---|---|
| 135 | [TCP] | RPC | RPC コネクタ ヘルパー（どの高いポートを使用するかを特定するために接続するマシン) |
| 137 | TCP | UDP | [NetBIOS 名（NetBIOS Name）] |
| 138 | | UDP | NetBIOS NetLogon とブラウズ |

| サーバ ポート | [プロトコル（**Protocol**）] | プロトコル | サービス |
|---|---|---|---|
| 139 | | | NetBIOS セッション |
| 123 | | UDP | NTP |
| 389 | TCP | | LDAP |
| 636 | TCP | UDP | LDAP SSL |
| 3268 | | | LDAP GC |
| 3269 | | | LDAP GC SSL |
| 54 | | | WINS 複製 |
| 53 | TCP | UDP | DNS |
| 88 | TCP | UDP | Kerberos |
| 445 | TCP | UDP | IP の SMB（Microsoft-DS） |
| 10000 | TCP | | RPC NTFRS |
| 10001 | [TCP] | | RPC NTDS |
| 10002 ～ 10200 | [TCP] | | RPC - 動的ハイオープンポート |
| 適用外 | ICMP | | TCP/IP スイート内のレイヤ 3 プロトコルスイート。これは、ping やトレースで使用されます。ポート 7 を閉じるとエコー応答をブロックできます。 |

# 接続のテスト

接続をテストし、Active Directory で FRS の設定を表示するには、Ntfrsult ツールを使用します。

**手順**

コマンドラインから、Windows ファイル複製ユーティリティを実行します：`Ntfrsutl version <server_name>`。

ドメインコントローラ間の通信が適切に設定されている場合、Ntfrtl 出力には Active Directory の FRS 設定が表示されます。

# 接続の検証

ドメインコントローラ間の接続を検証するには、Portqry ツールを使用します。

Portqry ユーティリティをダウンロードし、詳細について知りたい場合は、https://support.microsoft.com/en-in/help/310099/description-of-the-portqry-exe-command-line-utility を参照してください。

**手順**

**ステップ 1** **PortQryV2.exe** をダウンロードし、ツールを実行します。

**ステップ 2** 宛先 CD または PDC を選択します。

**ステップ 3** **[ドメインと信頼（Domains and Trusts）]**を選択します。

**ステップ 4** PortQry からの応答を使用して、ポートが開いているか確認します。

PortQry の機能の詳細については、Microsoft サポート技術情報の KB832919 の項目を参照してください。

# CiscoICMfwConfig_exc.xml File

CiscoICMfwConfig_exc.xml ファイルは、Cisco ファイアウォールスクリプトが Windows ファイアウォールの変更に使用するアプリケーション、サービス、およびポートのリストを含む標準 XML ファイルです。この変更により、ファイアウォールが Unified ICM/Unified CCE 環境で正常に機能します。

ファイルは、次の 3 つの主要な部分で構成されています。

- **サービス**：ファイアウォール経由でのアクセスが許可されているサービス。
- **ポート**：ファイアウォールが開くポート。

  この設定は、TCP/80 と TCP/443 の場合の IIS のインストールに応じた条件付きの設定です。
- **アプリケーション**：ファイアウォールを介したアクセスが許可されていないアプリケーション。

  スクリプトは、`CiscoICMfwConfig_exc.xml` ファイルにリストされているすべてのアプリケーションを自動的に除外します。

（注） [アプリケーション（Applications）] セクションの動作は、ファイル内の他の2つのセクションの動作とは逆です。[ポートとサービス（Ports and Services）] セクションでは、アクセスが許可されていますが、[アプリケーション（Application）] セクションではアクセスが拒否されています。

CiscoICMfwConfig_exc.xml ファイルにさらに多くのサービスまたはポートを手動で追加し、スクリプトを再実行して Windows ファイアウォールを再設定できます。たとえば、**Jaguar** サーバへのポート 9000（CORBA）からの接続を許可するには、[ポート（Ports）] セクションに回線を追加して、Windows ファイアウォール上のポート 9000 を開きます。

```
<Port Number="9000" Protocol="TCP" Name="CORBA" />.
```

（注） この変更は、リモート Jaguar 管理が求められている場合にのみ必要です。通常、この変更は不要です。

**[セキュリティが強化された Windows ファイアウォール（Windows Firewall with Advanced Security）]** を使用して、ポートまたはアプリケーションを追加または拒否できます。

このファイルには、一般に使用されるポートが XML コメントとしてリストされています。これらのポートの 1 つをすばやく有効にするには、ポートをコメントから **[ポート（Ports）]** タグの前の場所に移動します。

# Windows ファイアウォールのトラブルシューティング

Windows ファイアウォールで問題が発生した場合は、次のメモとタスクを参照してください。

## Windows ファイアウォール一般トラブルシューティング ノート

Windows ファイアウォールに関する一般的なトラブルシューティング ノート：

1. CiscoICMfwConfig アプリケーションを初めて実行する場合は、アプリケーションを 2 回実行すると、FirewallLib.dll の登録に成功します。場合によっては、特にシステムの速度が低下している場合、登録の完了に遅延が生じます。
2. 登録が失敗した場合は、.NET フレームワークが正しくインストールされていない可能性があります。次のパスとファイルが存在するかを確認します。

   ```
   %windir%\Microsoft.NET\Framework\v2.0.50727\regasm.exe

   %windir%\Microsoft.NET\Framework\v1.1.4322\gacutil.exe
   ```

3. 環境に合わせて、必要に応じて `%SYSTEMDRIVE%\CiscoUtils\FirewallConfig\Register.bat` を変更します。

# Windowsファイアウォールがルータのプライベートインターフェイス通信に干渉する

**問題** MDS は、Windows ファイアウォールが有効になっている場合のみ、サイド A ルータからプライベート インターフェイスの IP アドレス（分離）上のサイド B ルータへの接続に失敗します。

**考えられる原因** Windows ファイアウォールにより、アプリケーション（mdsproc.exe）がトラフィックをプライベートネットワーク上のリモートホストに送信するのを妨げている可能性があります。

**解決法** プライベートアドレス（ハイ およびハイ以外）用に、サイド A ルータおよびサイド B ルータの両方にスタティックルートを設定します。

# Windows ファイアウォールで Unified CCE 障害のないドロップされたパケットが表示される

**問題** Windows ファイアウォールログにドロップされたパケットが表示されますが、Unified ICM および Unified CCE アプリケーションではアプリケーション の障害が発生しません。

**考えられる原因** Windows ファイアウォールは、トラフィックが許可されていないか、許可されたアプリケーションがポートをリッスンしない場合に、ホストのトラフィックを記録します。

**解決法** pfirewall.log ファイルを詳しく確認して、送信元と宛先の IP アドレスとポートを確認します。`netstat` または `tcpview` を使用して、どのプロセスがリッスンし、どのポートで接続されるのか確認します。

# ファイアウォール設定の取り消し

ファイアウォール設定ユーティリティを使用すると、最後のファイアウォール設定の適用を元に戻すことができます。`CiscoICMfwConfig_undo.xml` ファイルが必要です。

（注） 元に戻すファイルは、設定が正常に完了した場合にのみ書き込まれます。このファイルが存在しない場合は、コントロールパネル経由の Windows ファイアウォールを使用して手動でクリーンアップする必要があります。

ファイアウォール設定を元に戻すには、次の操作を実行します。

**手順**

**ステップ 1** すべてのアプリケーションサービスを停止します。

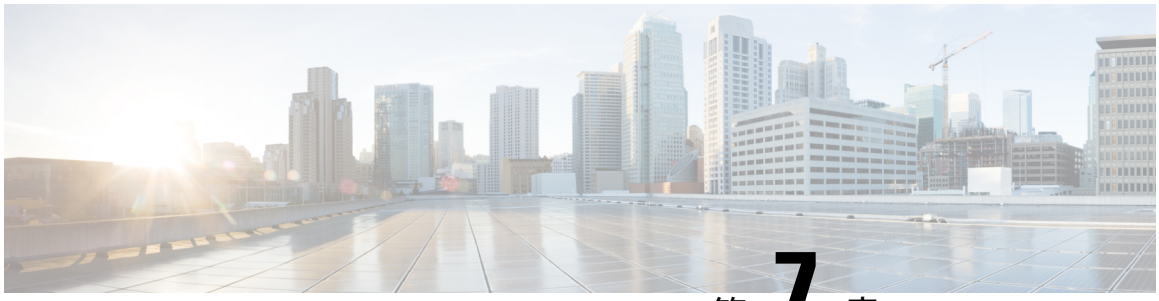
**ステップ 2** コマンドウィンドウを開きます。ダイアログウィンドウで **[開始（Start）]** > **[実行（Run）]** を選択し、`CMD` と入力します。

**ステップ 3** [OK] をクリックします。

**ステップ 4** 次のコマンドを入力します。`cd %SYSTEMDRIVE%\CiscoUtils\FirewallConfig`

**ステップ 5** Windows Server の `UndoConfigFirewall.bat` を入力します。

**ステップ 6** サーバをリブートします。



第 7 章

# SQL サーバの強化



# SQL サーバの強化に関する検討事項

## SQL の強化に関する検討事項の上位

SQL の強化に関する検討事項の上位：

1. Active Directory ドメインコントローラに SQL サーバをインストールしないでください。
2. Microsoft サイトから SQL サーバの最新の累積アップデートをインストールします：https://www.microsoft.com/en-us/download/details.aspx?id=56128。
3. ICM をインストールする前に、sa アカウントの強力なパスワードを設定します。
4. 最小権限のアカウントを使用して実行するには、常に SQL サーバサービスをインストールします。組み込みのローカルシステムアカウントを使用して、SQL サーバをインストールして実行してはなりません。代わりに、バーチャルアカウントを使用します。

   詳細については、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。
5. SQL サーバエージェントサービスを有効にして、Unified ICM でのデータベースメンテナンスのために [Automatic（自動）] に設定します。

（注） Microsoft から SQL サーバの最新の累積更新をインストールするには、SQL サーバエージェントサービスを無効にする必要がある場合があります。そのため、累積更新のインストールを実行する前に、このサービスを無効にリセットします。インストールが完了したら、サービスを停止して有効に戻します。

6. SQL ゲストアカウントを無効にします。
7. Unified ICM の管理者に sysadmin のメンバーを制限します。
8. 管理&データサーバがロガーと同じセキュリティゾーンにない限り、ネットワーク ファイアウォールで TCP ポート 1433 と UDP ポート 1434 をブロックします。
9. Microsoft SQL サーバサービスのリカバリアクションを変更し、失敗後に再起動します。
10. すべてのサンプルデータベースを削除します。
11. サインインの失敗に対する監査を有効にします。

次の表に、SQL 強化の設定と対応するデフォルト値とサポートされる値を示します。

| 設定名 | デフォルト値（Default Value） | サポートされる値 |
|---|---|---|
| 起動手順のスキャン | 無効 \|0\| | 0 または 1 がサポートされています。Unified CCE では、有効にする必要はありません。ただし、有効にすることで問題は発生しません。 |
| アドホック分散クエリ | 無効 \|0\| | 0 または 1 がサポートされています。0 の方が安全です。 |

**関連トピック**

SQL サーバのユーザと認証 （76 ページ）
バーチャル アカウント （79 ページ）

# SQL サーバのユーザと認証

SQL サーバアカウント用にユーザを作成する場合は、SQL サーバサービスを実行するための最も弱い権限を持つ Windows アカウントを作成します。SQL サーバのインストール中にアカウントを作成します。

インストール中は、SQL サーバデータベースエンジンが Windows 認証モードまたは SQL サーバと Windows 認証モードのいずれかのモードに設定されます。インストール中に Windows 認証モードを選択した場合、sa ログインは無効になります。後で認証モードを SQL サーバと Windows 認証モードに変更した場合、sa ログインは無効な状態のままです。sa ログインを有効にするには、ALTER LOGIN ステートメントを使用します。詳細については、https://msdn.microsoft.com/en-us/library/ms188670.aspx を参照してください。

SQL サーバサービスアカウント用に作成されたローカルユーザまたはドメインユーザアカウントは、それぞれ Windows またはドメインパスワードポリシーに従います。厳格なパスワードポリシーをこのアカウントに適用します。ただし、パスワードの有効期限は設定しないでください。パスワードの有効期限が切れると、SQL サーバサービスは機能しなくなり、管理 & データサーバが失敗します。

サイトの要件は、パスワードとアカウント設定を適用できます。次のような最小設定を検討してください。

**表 *3:* パスワードとアカウント設定**

| 設定 | 値 |
|---|---|
| パスワード履歴の強制 | 24 個のパスワードを記憶 |
| パスワードの最小文字数 | 12 文字 |
| パスワードの複雑度 | 有効 |
| 最短パスワード変更間隔 | 1 日 |
| アカウントロックアウト時間 | 15 分 |
| アカウントロックアウトしきい値 | 無効なログイン試行 3 回 |
| アカウントロックアウトカウンタのリセット | 15 分 |

混在モード認証は、SQL サーバの自動強化によって強制されます。

自動化された SQL サーバの強化中に、sa パスワードが空白だった場合は、sa アカウントを保護するために、ランダム生成の強力なパスワードが生成されます。

インストール後に sa アカウントのパスワードをリセットするには、Windows ローカル管理者アカウントを使用して SQL サーバにログインします。

# SQL サーバのセキュリティに関する検討事項

Microsoft SQL サーバは、設計、デフォルト、および導入により、以前のバージョンよりもはるかに安全です。これにより、はるかに詳細なアクセス制御と、攻撃対象領域を管理する新しいユーティリティが提供され、より低い権限で実行されます。セキュリティ機能を実装する際は、データベース管理者が次のセクションのガイドラインに従う必要があります。

## 自動 SQL サーバの強化

SQL サーバセキュリティの自動強化ユーティリティでは、次の作業を実行します。

- 混在モード認証を適用します。
- 名前付きパイプ（np）が SQL サーバクライアント ネットワーク プロトコル順序の TCP/IP（tcp）の前にリストされることを確認します。
- SQLWriter および SQLBrowser サービスを無効にします。
- 空白の場合、SQL サーバユーザの「sa」のパスワードを強制的に設定します。

# SQL サーバのセキュリティ強化ユーティリティ

SQL サーバのセキュリティ強化ユーティリティを使用すると、ロガーと管理サーバおよびデータサーバ/HDS コンポーネントの SQL サーバセキュリティの強化またはロールバックを可能にします。強化オプションにより、不要なサービスや機能が無効になります。最新バージョンのセキュリティ設定が既に適用されている場合は、[強化（Harden）] オプションは何も変更しません。[ロールバック（Rollback）] オプションでは、最後の強化を適用する前に存在していた SQL サービスと機能の状態に戻ります。

必要に応じて、Unified CCE のインストールとアップグレードの一部として、またはセキュリティ ウィザード ツールを使用して SQL サーバのセキュリティ強化を適用できます。このユーティリティは、Windows PowerShell スクリプト ICMSQLSecurity.ps1 を実行して内部で管理されます。PowerShell スクリプトを直接実行して、強化を適用することもできます。

（注） 管理者としてセキュリティ ウィザード ツールまたは Windows PowerShell スクリプトを実行します。

### ユーティリティの場所

このユーティリティは次の場所にあります。

```
%SYSTEMDRIVE%\CiscoUtils\SQLSecurity
```

### HARDEN コマンド

Windows PowerShell コマンドラインで、次の値を入力します。

```
Powershell .\ICMSQLSecurity.ps1 HARDEN
```

（注） 現在の SQL サーバの構成は、ユーティリティが SQL サーバの強化を適用する前に、`<ICMInstallDrive>:\CiscoUtils\SQLSecurity\icmsqlsecuritybkp.xml` にバックアップされています。

### ROLLBACK コマンド

前に強化が適用された場合、ROLLBACK コマンドは以前の SQL サーバ構成にロールバックします。

以前の SQL サーバ構成にロールバックするには、次のコマンドを入力します。

```
Powershell .\ICMSQLSecurity.ps1 ROLLBACK
```

（注） Unified CCE が正常に機能するには、次の設定が必要です。自動ロールバックを実行すると、元の状態には戻りません。

1. SQL サーバ クライアント ネットワーク プロトコル順序の TCP/IP（tcp）の前にリストされている名前付きパイプ（np）。
2. 混合モードの認証。

### コマンドのヘルプ

コマンドラインで引数を使用しない場合、ヘルプが表示されます。

### 出力ログ

すべての出力ログがファイルに保存されます。

```
%SYSTEMDRIVE%\CiscoUtils\SQLSecurity\Logs\ICMSQLSecurity.log
```

# 手動 SQL サーバの強化

デフォルトでは、SQL サーバ は VIA エンドポイントを無効にし、専用管理者接続（DAC）をローカルアクセスに制限します。また、デフォルトでは、すべてのログインが、共有メモリ、名前付きパイプ、TCP/IP、および VIA エンドポイントを使用して CONNECT に対する GRANT 権限を持っています。Unified ICM には、名前付きパイプエンドポイントと TCP/IP エンドポイントだけが必要です。

### 手順

- SQL サーバのセットアップ中に、名前付きパイプエンドポイントと TCP/IP エンドポイントの両方を有効にします。名前付きパイプエンドポイントの優先順位が TCP/IP よりも高くなるようにしてください。

（注） SQL サーバセキュリティ強化ユーティリティは、これらのエンドポイントの可用性と順序を確認します。

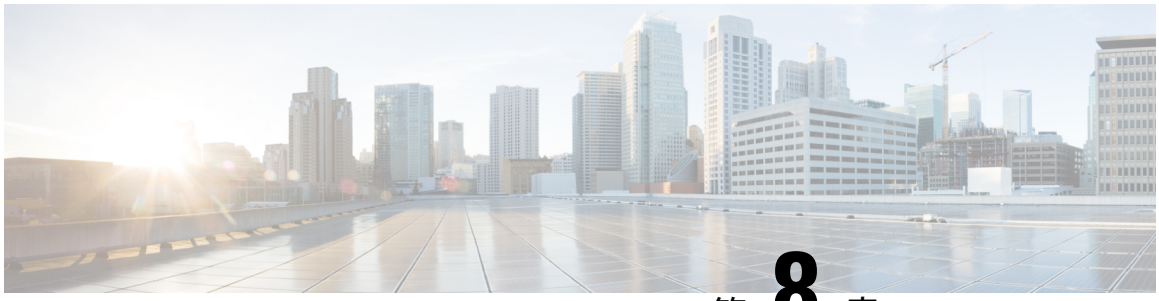
- すべての不要なエンドポイントへのアクセスを無効にします。たとえば、データベースにアクセスできるすべてのユーザ/グループに対して、VIA エンドポイントへの接続権限を拒否します。

# バーチャル アカウント

バーチャル アカウント、前者のセキュリティレベルが高いため、SQL サービスのネットワークまたはローカルサービスアカウントよりも優先されます。バーチャルアカウントは最小限の

権限で実行されます。CCE のインストーラは、ボリューム メンテナンス タスクの実行権限を SQLアカウントに追加します。この権限は、データベースの作成や拡張などのデータベース関連の操作を実行するために必要です。

社内ポリシーでこの権限の使用が許可されていない場合は、削除できます。ただし、データベースの作成や拡張などのデータベース関連の操作を実行すると、（データベースのサイズによっては）時間が長くなります。



第 8 章

# セキュアな接続用の証明書管理



## 証明書

証明書は、Web 上のクライアントとサーバを認証することにより、ブラウザの通信が安全であることを確保するために使用されます。ユーザは、認証局から証明書を購入でき（CA 署名付き証明書 - 推奨）、または自己署名証明書を使用できます。

### 自己署名証明書

自己署名証明書（名前が意味するとおり）は、認証局によって署名されるのではなく、そのアイデンティティを証明する同じエンティティによって署名されます。自己署名証明書は、CA 証明書ほど安全であるとはみなされませんが、多くのアプリケーションでデフォルトで使用されています。

## CCE 証明書管理ユーティリティ

シスコは、次の証明書管理ユーティリティを提供しています。

**シスコ SSL 暗号化ユーティリティ**：Web アプリケーションに使用される証明書管理ユーティリティ。

**CiscoCertUtil**：自己署名証明書および CA 署名付き証明書を作成およびインストールするために使用される証明書管理ユーティリティ。

（注） Unified CCE 証明書モニタリングサービスは、自己署名証明書および CA 署名付き証明書および証明書管理に使用されるキーをモニタします。サービスは、これらの証明書の有効性と有効期限についてシステム管理者に警告します。詳細については、以下にある *Cisco Unified ICM/Contact Center Enterprise* サービスアビリティ ベスト プラクティス ガイドを参照してください。http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html

# SSL 暗号化ユーティリティ

（注） 現在、このユーティリティには元の名前が付きますが、SSL 暗号化ユーティリティは、TLS で使用するために Web サーバを設定します。

Unified CCE Web サーバは、安全なアクセス（HTTPS）用に設定されています。シスコは、TLS で使用する Web サーバの設定に役立つ SSL 暗号化ユーティリティ（SSLUtil.exe）を提供しています。

（注） SSL 暗号化ユーティリティは、Windows Server 2016 を実行しているサーバでのみサポートされています。

IIS などのオペレーティング システムの機能は、SSL 暗号化ユーティリティで実行される操作を実行することもできます。ただし、シスコユーティリティを使用すると、プロセスが簡単になります。

SSLInstall.exe は、<ICMInstallDrive>\icm\bin フォルダにあります。SSL 暗号化ユーティリティは、セットアップの一部として、スタンドアロンモードで、または自動的に呼び出します。

SSL 暗号化ユーティリティは、実行する操作に関連したログメッセージを生成します。セットアップの一部として実行されると、ログメッセージがセットアップ ログ ファイルに書き込まれます。ユーティリティがスタンドアロンモードの場合、ログメッセージが SSL ユーティリティウィンドウおよび <SystemDrive>\temp\SSLUtil.log ファイルに表示されます。

SSL 暗号化ユーティリティは、次の主要な機能を実行します。

- SSL の設定（SSL Configuration）
- SSL 証明書の管理

SSLTLS は、Windows Server 2016 にインストールされている Unified CCE Web アプリケーションで使用できます。TLS 用のインターネット スクリプト エディタを設定できます。

## セットアップ中の TLS のインストール

デフォルトでは、セットアップにより、Unified CCE インターネット スクリプト エディタ アプリケーションで TLS が有効になります。

（注） ユーティリティが開いている間、IIS マネージャを使用して TLS 設定を変更する場合は、SSL 設定ユーティリティを再起動する必要があります。

SSL 設定ユーティリティを使用すると、自己署名証明書の作成と、作成された証明書の IIS へのインストールが容易になります。また、このツールを使用して IIS から証明書を削除することもできます。設定の一部として呼び出された場合、SSL 設定ユーティリティは IIS に TLS ポートを 443 に設定します（空白である場合）。

インターネット スクリプト エディタで TLS を使用するには、インストール中にデフォルト設定を受け入れ、サポートされているサーバが TLS を使用します。

セットアップ中に、ユーティリティは自己署名証明書を生成し、ローカルマシンストアにインポートし、Web サーバにインストールします。仮想ディレクトリが有効になり、256 ビット暗号化を使用する TLS の設定されます。

（注） セットアップ中に、証明書が存在する場合、または Web サーバに既存のサーバ証明書がインストールされている場合は、ログエントリが追加され、変更は適用されません。スタンドアロンモードでユーティリティを使用するか、IIS サービスマネージャを使用して証明書管理を変更します。

## スタンドアロンモードでの暗号化ユーティリティ

スタンドアロンモードでは、SSL 設定ユーティリティによって、ローカルマシンにインストールされている Unified ICM インスタンスのリストが表示されます。インスタンスを選択すると、ユーティリティにインストールされている Web アプリケーションとその SSL 設定が表示されます。その後、Web アプリケーションの SSL 設定を変更できます。

SSL 設定ユーティリティを使用すると、自己署名証明書の作成と、作成された証明書の IIS へのインストールが容易になります。また、このツールを使用して IIS から証明書を削除することもできます。設定の一部として呼び出された場合、SSL 設定ユーティリティは IIS に TLS ポートを 443 に設定します（空白である場合）。

# CiscoCertUtil ユーティリティ

CiscoCertUtil ユーティリティを使用すると、CCE マシン上の証明書を管理し、システムがコンポーネントをまたがって処理する PII を保護できます。

TLS が有効なコンポーネントは、このユーティリティを使用して証明書をセットアップします。CCEのセットアップでは、このユーティリティを使用して証明書を生成し、インストールします。

CiscoCertUtil ユーティリティ：

- 自己署名証明書を生成します。
- 証明書署名要求（CSR）を生成します。
- パーソナルフォルダの下にあるローカルマシンの証明書ストアにリモート証明書をインストールします。
- パーソナルフォルダの下にあるローカルマシンの証明書ストアから証明書を削除します。
- 自己署名証明書を PEM 形式（X509 内線）で生成します。
- ファイル名 *host.key* を使用して対応するキーを生成します。
- 証明書を検証しません。
- 実行する操作に関連するログファイルを作成しません。エラーが発生すると、エラーログがコンソールに表示されます。
- Windows Server を実行しているサーバでサポートされています。

（注） CiscoCertユーティリティを使用すると、自己署名証明書のみをインストールまたは削除できます。

### CiscoCert ユーティリティの使用

**CiscoCertUtil** *[/generateCert]|[/generateCSR]|[/generateCert /f]|[/remove <cert_name>]|[/install <cert_file>]| [/list]|[/help]|* コマンドを使用します。

ここで、

1. */list* は、信頼されたルートの下のローカルマシンストアに存在する証明書のリストを表示します。
2. */generateCert* は、ファイル名 *host.pem* とファイル名 *host.key* のキーを使用して自己署名証明書を生成します。自己署名証明書は`C:\icm\ssl\certs`に、キーは`C:\icm\ssl\keys`にコピーされます。キーが存在する場合は、同じキーを使用して自己署名証明書 *host.pem* を生成します。2048 ビットの RSA キー長が使用されます。

   */generateCert* コマンドは *host.key* と *host.pem* を上書きしません。既存の自己署名証明書を上書きするには、*/generateCert /f* コマンドを使用します。このコマンドは、すでにシステムで使用可能な場合、*host.key* と *host.pem* を上書きします。

（注） CCEのインストール中は、自己署名証明書がすでに生成されます。新しい証明書を生成する必要がある場合にのみ */generateCert* コマンドを使用する必要があります。たとえば、証明書のキーが侵害された場合や、自己署名証明書の有効期限が切れた場合に、証明書を生成する必要がある場合があります。

3. */generateCSR* は、ファイル名 *host.csr* と、ファイル名 *host.key*（秘密キー）を持つキーを使用してCSRを生成します。その後、*host.csr* は認証局に送信され、デジタルID証明書を取得します。キーが存在する場合、*host.csr* の生成に同じキーが使用されます。
4. */remove* <*certificate_name*> は、証明書 <*cert_name*> をパーソナルフォルダの下のローカルマシンの証明書ストアから削除します。コマンドの実行に失敗すると、エラーメッセージが表示されます。存在する証明書のリストを表示するには、*/list* コマンドを使用します。
5. */install* <*cert_file_path*> は、<*cert_file_path*> の下で説明されている証明書をパーソナルフォルダの下のローカルマシン証明書ストアにインストールします。コマンドの実行に失敗すると、エラーメッセージが表示されます。

   このコマンドの例を示します。

   ```
   CiscoCertUtil /install c:\icm\ssl\certs\host.pem.
   ```
6. */help* は、コマンドの使用方法を表示します。

（注） *remove* コマンドが失敗した場合は、*list* コマンドを使用して、削除しようとした証明書がローカルマシンの証明書ストアに存在するかどうかを確認します。

# 転送中の安全な PII

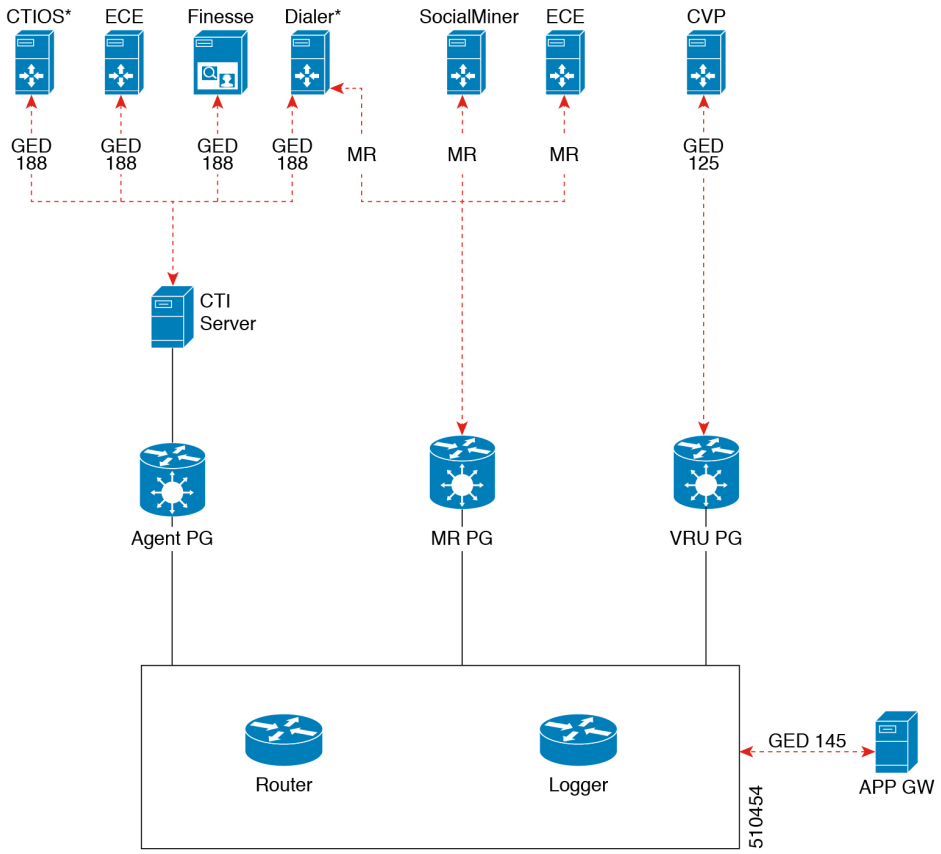
Contact Center Enterprise ソリューションは、クレジットカード情報、PIN、その他の機密情報を含む顧客の機密性の高い個人識別情報（PII）を処理します。このような機密情報はECC変数でシステム全体に送信され、利用される可能性があります。

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。したがって、PIIを移送するトランスポートチャネルを確保し、いかなる脅威からでも保護する必要があります。

PIIの確保は、規制のセキュリティ コンプライアンスにも準拠している必要があります。CCEソリューションは、TLSプロトコルを使用して、PIIをサポートするトランスポートチャネルのセキュリティを有効にします。

（注） 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。

図 *6:* セキュリティで保護された接続の例




次の表に、セキュアな接続、サーバからクライアントへの対応マトリクス、および使用されるプロトコルの導入例を示します。

| 使用例 | サーバ | サポート対象クライアント | [プロトコル（**Protocol**）] |
|---|---|---|---|
| **セキュアなセルフサービス通信**：セルフサービス通信を保護するために、CVP および VRU PG でのセキュアな接続を有効にします。 | CVP | VRU PG | GED 125 |

| 使用例 | サーバ | サポート対象クライアント | [プロトコル（Protocol）] |
|---|---|---|---|
| **セキュアなアウトバウンドコール**：アウトバウンドコールを保護するために、CTI サーバ、ダイヤラ、およびメディアルーティング PG でセキュアな接続を有効にします。 | CTI サーバ | ダイヤラ | GED 188 |
| | ダイヤラ | MR PG | メディアルーティングプロトコル |
| **セキュアなエージェントデスクトップ通信**：Cisco Finesse サーバおよび CTI OS との通信を保護するために、CTI サーバでの混在モード接続を有効にします。次に、必要に応じ、Cisco Finesse サーバまたは CTI OS でセキュアな接続を有効にします。 | CTI サーバ | Cisco Finesse | GED 188 |
| | | CTI OS | |
| **セキュアなサードパーティとの統合**：CCE とサードパーティの統合を保護するために、アプリケーションゲートウェイ サーバとクライアントでのセキュアな接続を有効にします。 | アプリケーションゲートウェイ サーバ | アプリケーションゲートウェイ クライアント | GED 145 |

| 使用例 | サーバ | サポート対象クライアント | [プロトコル（Protocol）] |
|---|---|---|---|
| **セキュアなマルチチャネル通信**：マルチチャネル通信を保護するために、以下の間のセキュアな接続を有効にします。<br>• ECE（サービスサーバ）と MR PG（クライアント）<br>• CTI サーバと ECE（クライアント） | ECE | MR PG | メディアルーティングプロトコル |
| | Customer Collaboration Platform | | |
| | CTI サーバ | ECE | GED 188 |

サーバとクライアント間のセキュアな接続を確立するには、次のいずれかのセキュリティ証明書を使用して相互認証を作成する必要があります。

- 自己署名証明書
- サードパーティー CA 署名付き証明書

たとえば、CTI サーバとダイヤラ間で自己署名証明書を交換してセキュアな接続を確立する場合は、次の手順を実行する必要があります。

1. CTI サーバで利用可能な自己署名証明書をコピーしてダイヤラにインストールします。有効な証明書をまだ利用できない場合は、新しい証明書を生成する必要があります。詳細については、自己署名証明書の管理 （90 ページ）を参照してください。
2. 同様に、ダイヤラで利用可能な自己署名証明書を CTI サーバにコピーしてインストールします。

（注） クライアントとサーバが同じマシン上にある場合は、マシンで利用可能なセキュリティ証明書を、サーバまたはクライアントによって信頼されているストアに 1 度置く必要があります。証明書を信頼されているストアに 2 度目に配置しようとすると失敗します。詳細については、CiscoCertUtil ユーティリティ （83 ページ）を参照してください。

3. 次に、それぞれのインターフェイスで **[セキュアな接続を有効にする（Enable Secured Connection）]** チェックボックスをオンにする必要があります。この場合は、**[アウトバウンドオプション ダイヤラのプロパティ（Outbound Option Dialer Properties）]** 画面の **[CTI サーバコンポーネントのプロパティ（CTI Server Component Properties）]** 画面で **[セキュアな接続を有効にする（Enable Secured Connection）]** チェックボックスをオンにする必要があります。

詳細については、次のガイドを参照してください。

- Cisco Unified Contact Center Enterprise インストールおよびアップグレード ガイド at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html
- Unified Contact Center Enterprise アウトバウンド オプション ガイド at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html

（注） 証明書を交換し、ソリューションのA側とB側の両方で個別にセキュアな接続を確立します。

（注） 証明書の追加、削除、更新など、証明書で新しいタスクを実行する場合は、必ずサービスを再起動して新しい接続を確立してください。

同様に、表「セキュア接続についてのサーバとクライアント間マトリクス」に記載された他のサーバとクライアント間でセキュアな接続を確立することもできます。

他のコンポーネント間のセキュアな接続については、次のガイドを参照してください。

- CVP と VRU PG 間のセキュアな接続については、http://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html にある 『*Configuration Guide for Cisco Unified Customer Voice Portal*』 を参照してください。
- ダイヤラとのセキュアな接続については、https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html にある *Unified Contact Center Enterprise* アウトバウンド オプション ガイド を参照してください。
- CTI サーバと Cisco Finesse 間のセキュアな接続については、https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-user-guide-list.html にある Finesse の証明書の管理 （91 ページ） と を参照してください。
- CTI サーバと CTI OS 間のセキュアな接続については、https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html にある Cisco Unified ICM CTI OS システム マネージャ ガイド を参照してください。
- アプリケーション ゲートウェイ サーバとクライアント間のセキュアな接続については、次にある Cisco Unified ICM/Contact Center Enterprise コンフィギュレーション ガイド を参照してください。https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html
- セキュアなマルチチャネル接続については、https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html にある Cisco Unified ICM/Contact Center Enterprise コンフィギュレーション ガイド を参照してください。

- セキュアな接続のポートの詳細については、https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html にある 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。

# 証明書とキーの場所

証明書、中間証明書、信頼できる証明書、およびキーをそれぞれのマシンの次のディレクトリに保存します。

| 証明書とキー | ディレクトリ |
|---|---|
| 証明書 | C:\icm\ssl\certs |
| 中間証明書と信頼できる証明書 | C:\icm\ssl\trust-certs<br>信頼できる証明書はこの場所に保存され、ここから Microsoft Windows ストアにインストールされます。 |
| オプション キー（Keys） | C:\icm\ssl\keys |

証明書を生成してインストールする手順については、このセクションで説明します。

## 自己署名証明書の管理

インターフェイス-サーバ-クライアント関係の範囲内でサーバとして定義されているマシン上の指定されたフォルダに、自己署名証明書を生成してコピーするには、次の手順を使用します。

**/generateCert /generateCert /f** および **generateCSR** のコマンドについては、CiscoCertUtil ユーティリティ （83 ページ） のコマンドの説明を参照してください。

### Windows オペレーティングシステム上で実行されているシステムの証明書の管理

Windows オペレーティングシステム上で実行されているシステムの証明書を管理するには、次の手順を参照してください。

クライアントマシンへのサーバ証明書のインストール

**手順**

**ステップ 1** サーバマシンで、以下のコマンドを使用して証明書を生成します：*<Install_Dir>:\icm\bin>CiscoCertUtil /generateCert*。このコマンドは、PEM 形式の証明書を生成し、このパス `C:\icm\ssl\certs` にコピーします。

有効な自己署名証明書がすでに利用可能な場合は、ステップ2に進みます。詳細については、CiscoCertUtil ユーティリティ （83 ページ） にある */generateCert* セクションを参照してください。

**ステップ 2** パス `c:\icm\ssl\certs` に移動します。

**ステップ 3** **host.pem** を クライアントマシンの一時的な場所にコピーします。

**ステップ 4** クライアントマシン上で、次のコマンドを使用して、信頼された証明書ストアにこの証明書ファイルをインストールします：*CiscoCertUtil /install c:\icm\ssl\certs\host.pem*。証明書ファイルがクライアントマシンの信頼された証明書ストアに既に存在している場合は、新しい証明書ファイルをインストールする前に、この既存の証明書ファイルを削除します。

**ステップ 5** 証明書ファイルが正常にインストールされたことを確認するには、*CiscoCertUtil /list* コマンドを実行します。次に、サーバホスト名が `LOCAL_MACHINE/ROOT` の下にリストされたかを確認します。

---

サーバへのクライアント証明書のインストール

### 手順

---

**ステップ 1** クライアントシステムで、以下のコマンドを使用して証明書を生成します：*<Install_Dir>:\icm\bin>CiscoCertUtil /generateCert*。このコマンドは、PEM 形式の証明書を生成し、このパス `C:\icm\ssl\certs` にコピーします。

有効な自己署名証明書がすでに利用可能な場合は、ステップ2に進みます。詳細については、CiscoCertUtil ユーティリティ （83 ページ） にある */generateCert* セクションを参照してください。

**ステップ 2** `c:\icm\ssl\certs` に移動します。

**ステップ 3** **host.pem** をサーバの一時的な場所にコピーします。

**ステップ 4** サーバ上で、次のコマンドを使用して、信頼された証明書ストアにこの証明書ファイルをインストールします：*CiscoCertUtil /install c:\icm\ssl\certs\host.pem*。証明書ファイルがサーバの信頼された証明書ストアに既に存在している場合は、新しい証明書ファイルをインストールする前に、この既存の証明書ファイルを削除します。

**ステップ 5** 証明書ファイルが正常にインストールされたことを確認するには、*CiscoCertUtil /list* コマンドを実行します。次に、クライアントホスト名が `LOCAL_MACHINE/ROOT` の下にリストされたかを確認します。

---

### 次のタスク

証明書のインストール後、対応するサービスを再起動します。

## Finesse の証明書の管理

Finesse サーバのセキュリティ証明書管理については、次の手順を参照してください。

## *Finesse* サーバからの証明書のエクスポート

セキュリティ証明書を Finesse サーバからエクスポートするには、次の手順を使用します。

### 手順

**ステップ 1** Finesse サーバの Cisco Unified Operating System の管理ページにログインします。

Finesse サーバ（`http://FQDN of Finesse server:8443/cmplatform`）の FQDN パスを使用してログインします。

**ステップ 2** **[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。

**ステップ 3** [検索（Find）] をクリックします。

**ステップ 4** Tomcat証明書のリストが表示されるかどうかに基づいて、次のいずれかの手順を実行します。

- Tomcat 証明書がリストされていない場合は、次の項目を実行します。
  - [新規作成（Generate New）] をクリックします。
  - 証明書の作成が完了したら、VOS サーバを再起動します。
  - この手順を再度行います。
- Tomcat 証明書がリストされている場合は、次の項目を実行します。
  - 証明書をクリックして選択します。[.pemファイルのダウンロード（Download .pem file）] をクリックして、ファイルをデスクトップに保存します。
  - 選択した証明書に、サーバのホスト名が含まれていることを確認します。

### 次のタスク

すべての Finesse サーバノードで、次の手順を実行します。

## *Finesse* サーバへの証明書のインポート

セキュリティ証明書を Finesse サーバにインポートするには、次の手順を使用します。

### 手順

**ステップ 1** Finesse サーバの Cisco Unified Operating System の管理ページにログインします。

Finesse サーバ（`http://FQDN of Finesse server:8443/cmplatform`）の FQDN パスを使用してログインします。

**ステップ 2** **[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。

**ステップ 3** [Upload Certificate] をクリックします。

**ステップ 4** **[証明書の名前（Certificate Name）] > [tomcat-trust]** を選択します。

**ステップ 5** **[参照（Browse）]**をクリックします。

.pem ファイル拡張子を使用して、CTI サーバ証明書の場所を参照します。

**ステップ 6** ファイルを選択し、[ファイルのアップロード（Upload File）] をクリックします。

### 次のタスク

残りのロードされていない証明書について、ステップ 3 ～ 6 を繰り返します。

すべての証明書をアップロードした後、Finesse Tomcat アプリケーションを再起動します。

## サードパーティ CA 署名付き証明書の生成とコピー

相互認証にサードパーティ認証局（CA）の署名付き証明書を使用している場合は、https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html にある『*Cisco Unified Contact Center Enterprise* インストレーションおよびアップグレードガイド』の「*CA* 証明書」の「CA 証明書」のセクションを参照してください。

# Customer Collaboration Platform

## Customer Collaboration Platformアプリケーションアクセスの制御

デフォルトでは、 Customer Collaboration Platform管理ユーザインターフェースへのアクセスは制限されています。管理者は、クライアントの IP アドレスを許可してアクセス権を提供し、許可リストからクライアントの IP を削除してアクセス権を取り消すことができます。許可リストを変更する場合は、Cisco Tomcat を再起動する必要があります。

（注） IP アドレス範囲とサブネットマスクはサポートされていません。

### utils whitelist admin_ui list

このコマンドは、許可されている IP アドレスをすべて表示します。このリストは、着信要求の送信元を承認するために使用されます。

#### 構文

**utils whitelist admin_ui list**

例

```
admin: utils whitelist admin_ui list Admin UI whitelist is: 10.232.20.31
10.232.20.32 10.232.20.33 10.232.20.34
```

### utils whitelist admin_ui add

このコマンドは, 指定された IP アドレスをアドレスの許可リストに追加します。

構文

**utils whitelist admin_ui add**

例

```
admin:utils whitelist admin_ui add 10.232.20.33 Successfully added IP:
10.232.20.33 to the whitelist Restart Cisco Tomcat for the changes to take
effect
```

### utils whitelist admin_ui delete

このコマンドは、指定された IP アドレスを許可リストから削除します。

構文

**utils whitelist admin_ui delete**

例

```
admin:utils whitelist admin_ui delete 10.232.20.34 Successfully deleted IP:
10.232.20.34 from the whitelist Restart Cisco Tomcat for the changes to take
effect
```

## CA 署名付き証明書の取得

サインインするごとに、ブラウザがサーバによって提示された証明書を検証します。証明書が信頼されたルート認証局（CA）によって署名されていない場合、ブラウザは通常、ユーザが明示的に許可するまで接続を許可しません。これを回避するには、CAによって署名されたルート証明書を取得し、Customer Collaboration Platform の上にインストールする必要があります。

Unified OS の管理の証明書管理ユーティリティを使用して、これを行います。

**[管理（Administration）] タブ > [プラットフォーム管理（Platform Administration）]** から Unified OS の管理を開きます。

### 証明書を取得する方法

1. **セキュリティ > 証明書管理 > CSRの生成**を選択します。
2. 生成が成功したら、**[CSR のダウンロード（Download CSR）]** をクリックします。
3. CSR を使用して、認証局（CA）から署名付きのアプリケーション証明書と CA ルート証明書を取得します。

### 証明書をアップロードする方法

1. 証明書を受け取った場合は、**[管理（Administration）]> [プラットフォーム管理（Platform Administration）]** から Unified OS 管理を開きます。
2. **[セキュリティ（Security）] > [証明書の管理（Certificate Management）] > [証明書のアップロード（Upload Certificate）]** を選択します。
3. [Certificate Name] リストから、証明書の名前を選択します。
4. ルート証明書をアップロードします。
    1. [アップロード（Upload）] ダイアログボックスで、ドロップダウンリストから **tomcat trust** を選択します。
    2. ファイルを参照し、**[開く（Open）]** をクリックします。
    3. [ファイルのアップロード（Upload File）] をクリックします。
5. アプリケーション証明書をアップロードします。
    1. [アップロード（Upload）] ダイアログボックスで、ドロップダウンリストから **tomcat** を選択します。
    2. [ルート証明書（Root Certificate）] テキストボックスに CA ルートの名前を入力します。
    3. ファイルを参照し、**[開く（Open）]** をクリックします。
    4. **[ファイルのアップロード（Upload File）]** をクリックします。

CA 署名付き証明書の詳細については、Unified OS の管理のオンラインヘルプのセキュリティに関するトピックを参照してください。

### 証明書のアップロード後

1. Customer Collaboration Platform からログアウトします。
2. XMPP サービスを再起動します。（SSH から Customer Collaboration Platform を選択して、コマンド *admin:utils service restart Customer Collaboration Platform XMPP Server*）をコマンドライン インターフェイスに入力します。

3. tomcat を再起動します。（SSH から Customer Collaboration Platform を選択して、コマンド *admin:utils service restart Cisco Tomcat)*をコマンド ライン インターフェイスに入力します。
4. Customer Collaboration Platform にログインします。

# 自己署名証明書の取得

ブラウザは、自己署名証明書をさまざまな方法で処理します。以下のセクションでは、Customer Collaboration Platform でサポートされているブラウザで自己署名証明書を処理する方法について説明します。

## Internet Explorer と自己署名証明書

Windows マシンで IE ブラウザを使用する場合は、DNS サーバが正しく設定されていることを確認して、完全修飾Customer Collaboration Platformホスト名をCustomer Collaboration Platformアドレスで解決 できます。信頼できる認証局（Verisign など）の署名付き証明書を使用します。

自己署名証明書（Customer Collaboration Platform でインストールされている場合）を使用する場合は、ログインのごとに証明書の警告が表示されるのを避けるために、次の手順に従います。

- [スタート（Start）] メニューで IE を右クリックし、[管理者として実行（Run as Administrator）] を選択します。
- アドレスバーに Customer Collaboration Platform サーバ の URL を入力します。
- セキュリティ警告が表示されたら、[**このサイトの閲覧を続行する（推奨されません）（Continue to this website (not recommended)**）] をクリックします。
- アドレスバーが赤色に変わると、アドレスバーの横に証明書エラーが表示されます。証明書エラーを選択します。
- ポップアップの下部にある **[証明書を表示（View certificates）]** を選択します。証明書ダイアログが開きます。
- [全般（General）] タブで、 **[証明書のインストール（Install Certificate）]** を選択します。に移動します。
- 証明書のエクスポートウィザードが起動します。[Next] をクリックします。
- 証明書の保存場所を確認するプロンプトが表示されたら、**[証明書をすべて次のストアに配置する（Place all certificates in the following store）]** を選択し、**[参照（Browse）]** をクリックして、**[信頼されたルート証明機関（Trusted Root Certification Authorities）]** を選択します。
- **[OK]** をクリックし、**[次へ（Next）]** をクリック して **[完了（Finish）]** をクリックして、証明書インポートウィザードを完了します。
- 証明書 の インポートを求めるプロンプトが表示されたら、**[はい（Yes）]** をクリックします。

• ブラウザを閉じて再起動して Customer Collaboration Platform にアクセスします。

## Firefox と自己署名証明書

Firefox のセキュリティモデルの変更により、Firefox 上の Customer Collaboration Platform Web アプリケーションを使用するために許可される必要がある、追加の自己署名証明書があります。

新しくインストールされた Firefox ブラウザ（任意のバージョン）を使用して Customer Collaboration Platform サーバにアクセスすると、Firefox は Customer Collaboration Platform が最初に使用するメインポート（ポート 443）への接続を試行します。接続できない場合は、自己署名証明書を許可するプロンプトがユーザに表示されます。

（注） ポップアップがブロックされている場合は、手動で証明書ページを起動する手順が示されます。また、証明書を許可する前に証明書ウィンドウを閉じると、ページが自動的に再起動します。

- 要求された場合は、**[リスクについて理解しました（I Understand the Risks）]** をクリックし、**[例外の追加（Add Exception）]** をクリックします。
- [セキュリティ例外の確認（Confirm Security Exception）] をクリックします。

次に、Firefox はポート 7443（セキュアな XMPP ポート）への接続を試行します。Firefox では、このポートを使用するために2番目の自己署名証明書を許可する必要があります。Customer Collaboration Platform の画面には、このプロセス中は「接続の確認中....」と表示されます。

「接続の確認中..」の画面が数秒間表示された場合、**[続行（Continue）]**をクリックして Firefox 証明書の許可画面に進みます（前述のとおり）。

**[リスクについて理解しました（I Understand the Risks）]** をクリックして、**[例外の追加（Add Exception）]**、**[セキュリティ例外の確認（Confirm Security Exception）]** を再度クリックします。

ユーザは、新しい Firefox ブラウザと自己署名証明書を初めて使用する場合にのみ、このプロセスを実行する必要があります。証明書が正しく設定されると、「接続の確認中...」の画面が表示されない場合があります（あるいは、少しの間表示され、Customer Collaboration Platform のログイン画面に進みます）。

## Google Chrome と自己署名証明書

Google Chrome ブラウザを使用して Customer Collaboration Platform のサーバにアクセスすると、ポート 7443 を使用してプライベートなセキュア接続の確立が試行されます。

- Chrome でサーバの IP アドレスを入力すると、ブラウザに**「接続はプライベートではありません」**という接続の警告メッセージが表示されます。セキュアな接続を続行するには、**[詳細設定（Advanced）]** をクリックします。

- **[<サーバ IP アドレス>に進む（Proceed to <Server IP Address>）]** をクリックします。次に、Chrome はポート 7443（セキュアな XMPP ポート）への接続を試行します。
- ブラウザに**「接続の確認中」**が表示されます。[続行（Continue）] をクリックして進みます。別の Chrome タブが開き、接続に関する別の警告メッセージが表示されます。
- **[詳細設定（Advanced）]** をクリックします。
- **[<サーバ IP アドレス> に進む（Proceed to <Server IP Address>）]** をクリックすると、Customer Collaboration Platform のログインページが表示されます。

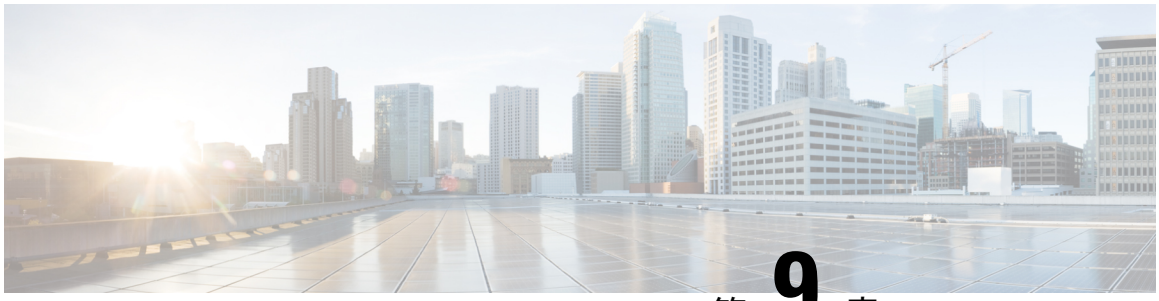
（注） ユーザは、新しい Chrome ブラウザと自己署名証明書を初めて使用する場合にのみ、このプロセスを実行する必要があります。

# Transport Layer Security（TLS）の要件

Contact Center Enterprise のソリューションは、Transport Layer Security（TLS）を使用します。TLS のサポートを設定する方法の詳細については、お使いのブラウザのマニュアルを参照してください。サポートされる TLS バージョンについては、https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html にある Contact Center Enterprise 互換性マトリクスを参照してください。

（注） 以前のバージョンのクライアントとの後方互換性を確保するために、Microsoft の手順に従って、Unified CCE Windows システムを以前のバージョンの TLS にダウングレードすることができます。

TLS のサポートを構成せずにセキュリティ強化を適用すると、お使いのブラウザが Web サーバに接続できません。ページが利用できない、または Web サイトに技術的な問題が発生しているというエラーメッセージが表示されます。



第 9 章

# 監査（Auditing）



## 監査（Auditing）

アカウントログインの試行などの重要なイベントを追跡するために、監査ポリシーを設定できます。常にローカルポリシーを設定します。

（注） ドメインの監査ポリシーは、常にローカルの監査ポリシーを上書きします。可能な場合には、2 つのポリシーセットを同一にしてください。

ローカルの監査ポリシーを設定するには、**[開始（Start）]**>**[プログラム（Programs）]**>**[管理ツール（Administrative Tools]）**>**[ローカル セキュリティ ポリシー（Local Security Policies）]** を選択します。

## 監査ポリシーの表示

手順

ステップ 1 **[開始（Start）]**>**[プログラム（Programs）]**>**[管理ツール（Administrative Tools）]**>**[ローカル セキュリティ ポリシー（Local Security Policies）]** を選択します。

[ローカルセキュリティ設定（Local Security Settings）] ウィンドウが開きます。

**ステップ 2** 左側のペインのツリーで、**[ローカルポリシー（Local Policies）]** を選択して展開します。

**ステップ 3** [ローカルポリシー（Local Policies）] の下のツリーで、**[監査ポリシー（Audit Policy）]** を選択します。

さまざまな監査ポリシーが左側のペインに表示されます。

**ステップ 4** ポリシー名をダブルクリックして、監査ポリシーを表示または変更します。

# セキュリティログの表示

監査ポリシーを設定した後、セキュリティログを 1 週間に 1 回確認します。ログオンの失敗や異常なアカウントを使用したログオンの成功などの異常なアクティビティを探します。

セキュリティログを表示するには、次のアクセスを実行します。

**手順**

**[開始（Start]）** > **[プログラム（Programs）]** > **[管理ツール（Administrative Tools）]** > **[イベント ビューア（Event Viewer）]** を選択します。

# リアルタイムアラート

Windows では、SNMP イベントトランスレータ機能が提供されています。この機能を使用すると、Windows イベントログのイベントをリアルタイムアラートに変換して、イベントを SNMP トラップに変換できます。evntwin.exe または evntcmd.exe を使用して SNMP トラップを設定します。

イベントをトラップに変換する設定の詳細については、**Evntcmd** に関する Microsoft TechNet の項目を参照してください。

SNMP トラップの宛先の設定については、『*Cisco Unified ICM/Contact Center Enterprise SNMP ガイド*』ガイドを参照してください。

# SQL サーバ監査ポリシー

一般的な SQL サーバの監査ポリシーについては、https://docs.microsoft.com/en-us/sql/relational-databases/security/auditing/sql-server-audit-database-engine?view=sql-server-2017 にある Microsoft のマニュアルを参照してください。

# SQL サーバ C2 セキュリティ監査

C2 セキュリティは、システムが分権的なリソース保護と監査機能によって認定される政府のセキュリティ評価です。

シスコでは、Unified ICM/Unified CCE 環境では、SQL サーバの C2 監査をサポートしません。

# Active Directory の監査ポリシー

Active Directory アカウントの管理とログインを定期的に監査します。異常なアクティビティについて、ログの監視も行います。

次の表に、強化されたデフォルトの DC 監査ポリシーを示します。

**表 *4 : Active Directory* の監査ポリシー設定**

| ポリシー | デフォルト設定 | 強化された設定 | 説明 |
|---|---|---|---|
| アカウントログインイベントの監査 | 監査なし | 成功と失敗 | アカウントログインイベントは、ドメインユーザアカウントがドメインコントローラで認証されると生成されます。 |
| アカウントの管理を監査する | 未定義 | 成功 | アカウント管理イベントは、セキュリティプリンシパル アカウントが作成、変更、または削除されると生成されます。 |
| ディレクトリ サービス アクセスを監査する | 監査なし | 成功 | ディレクトリ サービス アクセス イベントは、システムアクセス制御リスト（SLL）を含む Active Directory オブジェクトにアクセスすると生成されます。 |
| ログインイベントを監査する | 監査なし | 成功と失敗 | ログインイベントは、ドメインユーザがドメインコントローラにインタラクティブにログインするときに生成されます。ログインイベントは、ドメインコントローラへのネットワークログインを実行してログインスクリプトとポリシーを取得する際にも生成されます。 |
| オブジェクトのアクセスを監査する | 監査なし | （変更なし） | |
| ポリシー変更の監査 | 監査なし | 成功 | ポリシー変更イベントは、ユーザ権利割り当てポリシー、監査ポリシー、または信頼ポリシーへの変更に対して生成されます。 |

| ポリシー | デフォルト設定 | 強化された設定 | 説明 |
|---|---|---|---|
| 特権の使用を監査する | 監査なし | （変更なし） | |
| プロセストラッキングを監査する | 監査なし | （変更なし） | |
| システムイベントを監査する | 監査なし | 成功 | システムイベントは、ユーザがドメインコントローラを再起動またはシャットダウンするときに生成されます。システムイベントは、システムのセキュリティまたはセキュリティログに影響するイベントが発生した場合にも生成されます。 |

# 設定の監査

Unified CCE は、Config_Msg_Log テーブル内のすべてのシステム設定変更の履歴をキャプチャします。ただし、Config_Msg_Log テーブルにキャプチャされた情報は暗号化されています。テーブルをわかりやすい形式で表示するには、データベース管理ツールである dumpcfg ユーティリティを使用します。取得した情報は、監査の目的で使用できます。

ユーティリティを実行するには、コマンドプロンプトで次のコマンドを使用します。

**dumpcfg** *<database></@server>|[</bd begin date>]|[</bt begin time]>|[</ed enddate]>| [</ed endtime>]|[</nd number_of_days>]|[<low recovery key>]|[<high recovery key>]|*.

ここで、

1. データベース は、ロガーデータベースの大文字と小文字が区別される名前です。
2. *@server* は、AW またはロガーデータベースのホスト名です。
3. *<database></@server>|[</bd begin date>]|[</bt begin time]>|[</ed enddate]>| [</ed endtime>]|[</nd number_of_days>]|[<low recovery key>]|[<high recovery key>]|* は、情報が必要な時間範囲です。

   RecoveryKey は、ソフトウェアが仮想時間を追跡するために内部で使用する値です。

*dumpcfg* コマンドは 、次の出力の詳細を表示します。

- **LogOperation**：設定操作のタイプを示します。たとえば、追加および更新などです。
- **TableName**：設定操作が影響を受けたテーブルの名前を表します。
- **DateTime**：設定操作の日時を示します。

- **ConfigMessage**：設定操作のすべての設定メッセージが一覧表示されます。

たとえば、スキルグループを追加した場合、次のコマンドを実行します。

たとえば、スキルグループを追加した場合、次のコマンドを実行します：**dumpcfg ucce_sideA@uccergr100a /bd 09/27/2018**

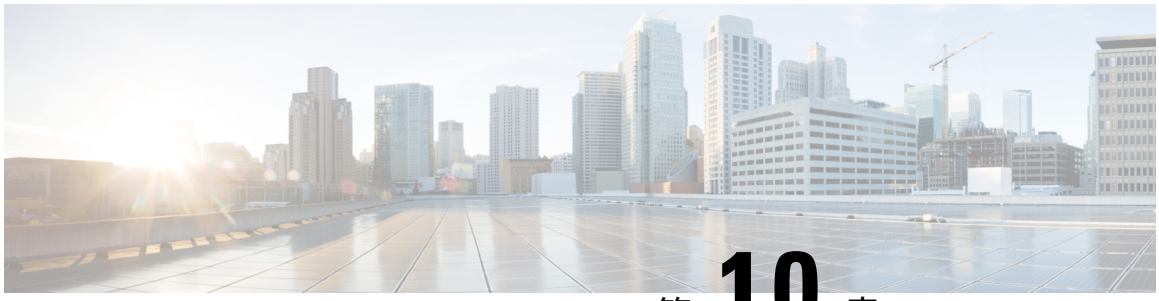
出力されたものとして表示される詳細は次のとおりです。

**LogOperation**：**追加**。

**TableNames**：**skill_target and t_skill_group**。

**DateTime**：スキルグループが追加された正確なタイムスタンプ。

**ConfigMessage**：**周辺機器名**、**企業名**などの、影響を受け取けたフィールド名。



第 10 章

# 一般的なウイルス対策ガイドライン



## ウイルス対策ガイドライン

ウイルス対策のアプリケーションには、データのスキャンとサーバ上でのデータ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、スキャンとサーバパフォーマンスのバランスを取る設定が必要です。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。詳細な設定情報については、特定のウイルス対策製品のマニュアルを参照してください。

この章のガイドラインに準拠しているサードパーティ製のウイルス対策ソフトウェア製品を使用することができます。シスコがテスト済みのウイルス対策ソフトウェア製品の一覧については、https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html にある *Contact Center Enterprise* 互換性マトリクス を参照してください。

サードパーティ製ソフトウェア製品に関するシスコガイドラインの詳細については、https://www.cisco.com/c/en/us/products/collateral/customer-collaboration/unified-ip-interactive-voice-response-ivr/prod_bulletin09186a0080207fb9.html にある「サードパーティ製のソフトウェアおよびセキュリティアップデートを使用する場合の *Cisco Customer Contact* 情報」を参照してください。

**警告** 多くの場合、デフォルトの AV 設定により、CPU の負荷とメモリとディスク使用量が増加し、ソフトウェアパフォーマンスに悪影響を及ぼします。シスコは特定の構成をテストして製品のパフォーマンスを最大化します。Unified ICM/Unified CCE で AV ソフトウェアを使用するには、次のガイドラインを使用する必要があります。

ウイルスは予測不可能で、シスコはミッションクリティカルなアプリケーションに対するウイルス攻撃の影響に対して責任を負うことはできません。Microsoft Internet Information Server（IIS）を使用するシステムには、特に注意してください。

次のリストでは、一般的なガイドラインについて説明します。

- 企業のウイルス対策戦略に、企業のファイアウォールの外部に配置されているサーバ、またはパブリックインターネットに頻繁に接続する対象となるサーバに関する特定の規定が含まれていることを確認します。
- Unified ICM/Unified CCE のリリースに対して適格で承認されているアプリケーションおよびバージョンについては、*Contact Center Enterprise* 互換性マトリクス を参照してください。
- 組織のポリシーに従って、AV ソフトウェアと定義ファイルを定期的に更新します。
- 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。可能な場合は、これらの各リモートマシンに、独自のウイルス対策ソフトウェアがインストールされていることを確認し、すべてのスキャンをローカルに保持します。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。
- AV ソフトウェアによるシステムの完全スキャンのスケジュールは、スケジュールされたメンテナンスウィンドウで**のみ**行い、AV スキャンによって他の Unified ICM メンテナンスアクティビティが中断できない場合にスケジュールを設定します。
- AV ソフトウェアが、自動またはバックグラウンドモードですべての着信データまたは変更ファイルをリアルタイムでスキャンしないように設定します。
- 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）。このアプローチは、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、この設定では、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のスキャンのオーバーヘッドがあります。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。
- 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時は、定期的なディスクスキャンをスケジュールします。
- サーバが電子メールを使用しない場合は、電子メールツールを無効にします。

- AV ソフトウェアでスパイウェアの検出と削除が行なわれる場合は、この機能を有効にします。感染したファイルをクリーンにするか、削除します（これらのファイルを削除できない場合）。
- AVアプリケーションでのロギングを有効にします。ログのサイズを2 MBに制限します。
- 圧縮ファイルをスキャンするために AV ソフトウェアを設定します。
- AV ソフトウェアが CPU の使用率をいつでも 20% を超えないように設定します。
- AV ソフトウェアが使用可能な場合は、バッファオーバーフロー保護を有効します。
- AV ソフトウェアを設定して、システムの起動時に起動します。

# Unified ICM/Unified CCE メンテナンスパラメータ

いくつかのパラメータは、特定の時間にアプリケーション アクティビティを制御します。Unified ICM/Unified CCE サーバで AV ソフトウェア アクティビティのスケジュールを設定する前に、重要な時期にウイルス対策ソフトウェアの設定で 「[毎日のスキャン（Daily Scans）]」「[自動 DAT 更新（Automatic DAT Updates）]」 および 「[自動製品アップグレード（Automatic Product Upgrades）]」 をスケジュールされないことを確認してください。

## ロガーに関する検討事項

AV ソフトウェアアクティビティを、次のロガーのレジストリキーで指定されている時間と一致するスケジュールに設定しないでください。

- HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\<inst>\Logger<A/B>\Recovery\CurrentVersion\Purge\Schedule\Schedule Value Name: Schedule
- HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\<inst>\Logger<A/B>\Recovery\CurrentVersion\UpdateStatistics\Schedule Value Name: Schedule

## ディストリビュータに関する検討事項

AV ソフトウェアアクティビティを、次のディストリビュータのレジストリキーで指定されている時間と一致するスケジュールに設定しないでください。

- HKLM\SOFTWARE\Cisco Systems, Inc. \ICM\<inst>\Distributor\RealTimeDistributor\CurrentVersion\Recovery\CurrentVersion\Purge\Schedule Value Name: Schedule
- HKLM\SOFTWARE\Cisco Systems, Inc. \ICM\<inst>\Distributor\RealTimeDistributor\CurrentVersion\Recovery\CurrentVersion\UpdateStatistics\Schedule Value Name: Schedule

# コールルータと PG に関する検討事項

CallRouter および周辺機器ゲートウェイ（PG）で、次のタイミングで AV プログラム タスクのスケジュールを設定しないでください。

- コール負荷がピークまたは重い時間帯。
- 30 分と 1 時間の時刻になるとき。Unified ICM プロセスはこれらの時間帯に増加します。

# その他のスケジュールされたタスクに関する検討事項

Windows 上で他のスケジュール された Unified ICM プロセスアクティビティは、[スケジュール済みタスク（Scheduled Tasks）] フォルダを調べることで確認できます。スケジュールされた AV プログラムアクティビティが、Unified ICM のスケジュール済みアクティビティと競合しないよう確認します。

# ファイルタイプの除外に関する検討事項

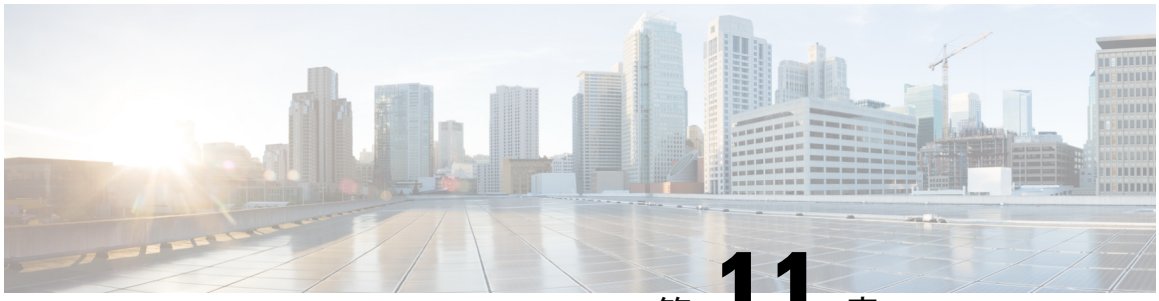
Unified ICM プロセスの操作中に書き込まれるいくつかのバイナリファイルには、ウイルス感染のリスクはほとんどありません。

AV プログラムのドライブおよびオンアクセススキャン設定から、次のファイル拡張子を含むファイルを省略します。

- *.hst は PG に適用されます。
- *.ems は ALL に適用されます。
- *.repl
- *.localrepl

（注） アウトバウンド高可用性の複製を使用している場合 、**repl** ディレクトリ（`/icm/<cust>/la` または `lb/repl` は、ウイルス対策のスキャンから除外する必要があります。

（注） すべてのウイルス対策スキャンから *c:\icm* フォルダを除外します。



第 11 章

# リモート管理



## Windows リモートデスクトップ

リモートデスクトップを使用すると、ユーザは、仮想的に任意のネットワーク接続を使用してさまざまなデバイスから Windows Server 上でアプリケーションをリモートで実行できます。リモートデスクトップは、アプリケーション サーバ モードとリモート管理モードのいずれかを使用して実行できます。Unified ICM/ Unified CCE は、リモート管理モードのみをサポートします。

（注）
- リモート管理アプリケーションを使用すると、負荷時に悪影響を引き起こす可能性があります。
- 暗号化を用いたリモート管理ツールを使用すると、サーバのパフォーマンスが影響を受ける可能性があります。パフォーマンスレベルの影響は、使用する暗号化のレベルに関連しています。暗号化を追加すると、サーバのパフォーマンスへの影響が大きくなります。

リモートデスクトップは、ICM-CCE-CCH サーバのリモート管理に使用できます。mstsc コマンドは、ローカル コンソール セッションに接続します。

リモート デスクトップ コンソール セッションを使用すると、次の操作を実行できます。

- 構成ツールの実行
- スクリプト エディタの実行

（注） リモートデスクトップは、ソフトウェアのインストールやアップグレードではサポートされていません。

（注） 管理者クライアントおよび管理ワークステーションは、リモート デスクトップ アクセスをサポートしています。ただし、一度に1つのクライアントまたはワークステーションにアクセスできるユーザは 1 人のみです。Unified CCE は、同じクライアントまたはワークステーション上の複数のユーザによる同時アクセスをサポートしていません。

# Remote Desktop Protocol

サーバとクライアント間の通信では、ネイティブの Remote Desktop Protocol（RDP）の暗号化を使用します。デフォルトでは、クライアントがサポートする最大キー強度に基づく暗号化により、すべてのデータが保護されます。

セキュリティとパフォーマンスへの影響が小さいので、リモート制御プロトコルとして推奨されるのが RDP です。

Windows Server 端末サービスを使用すると、コンソールセッションを無効にできます。端末サービスは、pcAnywhere または VNC の必要性を置き換える場合があります。Windows コマンドプロンプトから起動するには、次の値を入力します。

リモート デスクトップ接続：`mstsc /v:<server[:port]>`

# RDP-TCP 接続セキュリティ

RDP-TCP 接続に保護を提供するには、Microsoft のリモート デスクトップ サービス マネージャを使用して、接続のプロパティを適切に設定します。

- アクティブなクライアントセッションの数を 1 に制限します。
- 切断されたセッションを 5 分以内に終了します。
- セッションをアクティブにできる時間を 1 日または 2 日に制限します。
- セッションがアイドル状態のままである時間を 30 分に制限します。
- ユーザとグループに対して適切な権限を選択します。管理者とシステムにのみフルコントロールを与えます。一般ユーザにユーザアクセスを与えます。すべての制限付きユーザにゲストアクセスを与えます。
- 切断されたセッションの再接続を、ユーザがもともと接続していたクライアントコンピュータに制限することもできます。
- 通信の不正なモニタリングから保護するために、高い暗号化レベルを設定してください。

# ユーザごとの端末サービス設定

ユーザごとの端末サービス設定を各ユーザに対して設定するには、次の手順を実行します。

手順

**ステップ 1** Active Directory ユーザとコンピュータを使用してユーザを右クリックし、**[プロパティ（Properties）]** を選択します。

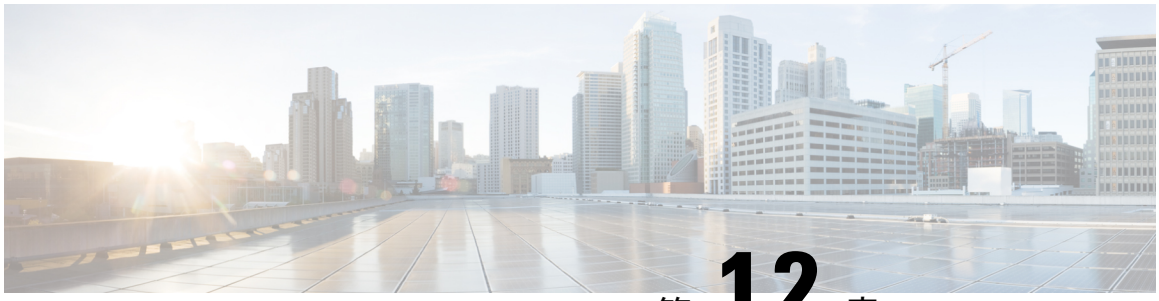
**ステップ 2** [端末サービスプロファイル（Terminal Services Profile）] タブで、**[端末サーバにログオンを許可する（Allow logon to terminal server）]** チェックボックスをオンにして、ユーザが端末サーバにログインする権利を設定します。必要に応じて、プロファイルを作成し、端末サービスのホームディレクトリへのパスを設定します。

**ステップ 3** [セッション（Sessions）] タブで、セッションをアクティブまたはアイドル状態のタイムアウトに設定します。

**ステップ 4** [リモート制御（Remote Control）] タブで、管理者がリモートセッションをリモートで表示および制御できるかどうか、およびユーザの権限が必要かどうかを設定します。

# VNC

SSH サーバを使用すると、暗号化されたトンネルで VNC を使用することにより、安全なリモート制御セッションを作成できます。ただし、シスコではこの設定をサポートしていません。SSH サーバを実行した場合のパフォーマンスへの影響は確認されていません。



第 12 章

# その他のセキュリティに関する検討事項



# その他のシスコ コール センター アプリケーション

次のセクションでは、他のシスコ コール センター アプリケーションのセキュリティに関する検討事項について説明します。

## Cisco Unified ICM ルータ

**dbagent.acl** ファイルは、内部のバックグラウンドファイルです。このファイルを編集しないでください。ただし、このファイルには読み取りアクセス許可が設定されている必要があります。このファイルを使用すると、ユーザがルータのリアルタイムフィードに接続できます。

# 周辺機器ゲートウェイ（PG）とエージェントログイン

誤ったパスワードを使用した Unified CCE エージェントログイン試行にはレート制限があります。デフォルトでは、エージェントアカウントは、15 分間で間違ったパスワード試行が 3 回行われると、15 分間無効になります。

このデフォルトは、レジストリキーを使用して変更できます。このレジストリキーは、次の下にあります。`HKLM\SOFTWARE\Cisco Systems, Inc.\\ICM\<inst>\PG(n)[A/B]\PG\CurrentVersion\PIMS\pim(n)\EAGENTData\Dynamic`

レジストリキーには、次のものが含まれます。

- **AccountLockoutDuration**： デフォルト

  ログイン試行が失敗してアカウントがロックアウトされた場合、この値はアカウントがあと何分間ロックアウトされたままかを表します。

- **AccountLockoutResetCountDuration**： デフォルトは 15 です。AccountLockoutThreshold 回数が 0 に戻るまでの時間（分）。これは、アカウントがロックアウトされずに、AccountLockoutThreshold で説明されている値よりも少ないログイン試行が失敗した場合に適用されます。

- **AccountLockoutThreshold**： デフォルトは 3 です。これは、アカウントがロックアウトされた後のログイン試行が失敗した回数です。

（注） これらの設定は、システム周辺機器ゲートウェイを備える CTI OS など、Cisco Finesse 以外のデスクトップソリューションにのみ適用されます。

エージェントまたはスーパーバイザがパスワードを誤って 5 回連続してデスクトップにログインしようとした場合、Finesse はユーザアカウントへのアクセスをブロックします。ロックアウトの時間は 5 分間です。これらの設定の詳細については、https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html にある『*Cisco Finesse* アドミニストレーション ガイド』を参照してください。

# エンドポイントセキュリティ

## エージェントのデスクトップ（Agent Desktops）

Cisco Finesse は、管理コンソールおよびエージェントおよびスーパーバイザクライアントで HTTPS（TLS 1.2 のみ）をサポートします。

## 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

## 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。

## 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。

# リバースプロキシ展開のセキュリティガイドライン

VPN を使用しないアクセスを許可するには、リバースプロキシホストにインターネットから直接アクセスできる必要があります。したがって、セキュリティはリバースプロキシ導入では非常に重要であり、ネットワークセキュリティを維持および管理するには、細心の注意が必要です。このセクションでは、リバースプロキシ導入を保護するための一連のガイドラインを提供します。

（注） 提供されるガイドラインと推奨事項は、管理者が導入を安全に行なうために必要な最小限のガイダンスとして使用することを目的としています。リバースプロキシとネットワークの導入、設定、およびセキュリティの責任は、コンタクトセンターにあります。

## リバースプロキシ

通常、リバースプロキシは、インターネットからコンタクト センター ネットワークに入るすべての要求で最初のアプリケーションレベルの着陸ポイントになります。リバースプロキシには、攻撃に耐え得る高いレベルのセキュリティが必要です。次に、リバースプロキシ導入を保護するためのガイドラインを示します。

- TLS 1.2 を設定し、他の TLS プロトコルをオフにします。
- セキュアな HTTP/2 ベースのアクセスのみを許可します。
- プロキシへの予定外のアクセスが提供されないよう、プロキシのデフォルトアクセスとデフォルトルールをオフにします。
- リバースプロキシとホストシステムがセキュリティパッチを使用して最新の情報を入手し、侵害の可能性を防ぐことを確認します。
- リバースプロキシがインターネットへの直接のアウトバウンド接続を確立できないことを確認します。
- インターネットにさらされた場合、プロキシホストの安全性を確保するために、セキュリティを強化します。ベストプラクティスについては、https://www.cisecurity.org/cis-benchmarks/ を参照してください。
- リバースプロキシホストで定期的にセキュリティテストを実施し、セキュリティが侵害されていないかを確認します。

- セキュリティ上の理由から、明示的に公開されている以外のAPIパスは、設定されたルールで使用できないことを確認します。Nginx リバースプロキシが導入されている場合は、**「Nginx Techzone」の項目**にあるNginxルールを参照して、各Finesse、IdS、およびCUICサーバに対して明示的に開いているパスを見つけることができます。
- セキュリティの観点からキャッシュが重要なのは、ほとんどの静的リソースは保護されていないためです。Finesseサーバ上でこれらのリソースをキャッシュすることで、簡易DoS攻撃を回避できます。ただし、リソースが最新の動作を行なえるよう、Finesse、IdS、およびCUIC サーバでリソースを定期的に検証する必要があります。
- HOSTヘッダーを検証して、目的のドメインだけがクライアントによってアクセスされるのを確認します。
- 必要な数のクライアントに対応するドメインごとに、Finesse、IdS、およびCUICサーバのWebsocket 接続を調整します。
- ベストプラクティスは、更新されたパッチと設定変更で、リバースプロキシのセキュリティが強化された金色のイメージを維持することです。これらの金色のイメージからインストールすると、すべてのリバース プロキシ インスタンスに一貫性があり、可能な限り安全になります。

（注） シスコは、Nginx のリバースプロキシに関するセキュアな設定ガイドラインを **「Nginx Techzone」の項目**で説明しています。

## 非武装地帯のセキュリティ

ネットワークとホストのセキュリティを更新するための継続的なプロセスと関連する取り組みがない場合は、リバースプロキシの導入では、セキュリティの強化を維持できません。DMZがセキュアな環境を確保するための重要な点は次のとおりです。

- （複数のインターフェイスを備える単一のファイアウォールではなく）デュアルファイアウォールを使用して、DMZ と内部ネットワークを分離することを検討してください。
- 内部ファイアウォールでルールを設定し、DMZ から発生した要求が、リバースプロキシで設定されているホスト以外のホストに到達しないことを確認します。
- DMZ が、ルーティングとセキュリティポリシーが分離された内部ネットワークから分離されている必要があります。
- リバースプロキシ導入のセキュリティは、構成とソフトウェアを更新し続けるプロセスによって異なります。

## レート制限

Finesse、IdS、およびCUIC は、DoS 攻撃から保護するためにホストレベルのファイアウォールルールに依存します。これらのコンポーネントでリバースプロキシホストが設定されている場合、設定されたリバースプロキシホストは、すべてのホストレベルのレート制限ルールから

免除されます。これは、プロキシに接続された複数のクライアントにサービスを提供するプロキシの必須のスループットをサポートするためにあります。したがって、逆プロキシを介してホストにルーティングされるトラフィックが個々の IP ごとに規制対象になじむよう、パケットレートの制限とレート制限要求（使用可能な場合）を適用する必要があります。これにより、リバースプロキシとホストの可用性が向上します。

（注） ネットワークを DMZ に接続する ISP ルータでは、一般的なネットワークパケットレートの制限を課すことを検討してください。周囲のルータにレート制限を実装すると、ISP リンクを飽和状態にすることを目的とした DoS 攻撃には効果的ではありません。

レートの制限の計算の詳細については、『*Cisco Unified Contact Center Enterprise Features Guide*』の「プロキシの規模とハードウェアの検討」セクション、およびNginx固有の情報については**「Nginx Techzone」の項目**を参照してください。

## ネットワーク セキュリティ デバイス

DMZ に入るトラフィックに対してセキュリティを強化するために、この侵入防御システム（IPS）機能を組み込むネットワーク セキュリティ デバイスを導入する必要があります。これらは、プロキシまたはファイアウォールが効果的に検出または防止する機能を備えていないクラス全体の攻撃を防ぐためのデバイスです。IPS デバイスの導入中は、分散型サービス妨害（DDoS）署名を検出できるデバイスを導入し、DDoS 攻撃から保護します。

### Web アプリケーションのファイアウォール

リバースプロキシ展開に対してより高いセキュリティ層を提供する Web Application Firewall（WAF）を導入すると良いでしょう。WAF デバイスは、セキュリティチェックをアプリケーション層に拡張します。これは、Web アプリケーション トラフィックでスクリプト、ヘッダー、Cookie、HTTP メソッドなどについて検査し、既知の脆弱性や、不正なトラフィックをブロックするループホールを見つけた場合に実現します。これにより、Webアプリケーションに固有の脆弱性を利用する複雑なサイバー攻撃が回避されます。IPS と WAF の機能を統合するデバイスや、上述のすべての機能を提供するクラウドサービスを使用するデバイスを用意することができます。

## 推奨される DDoS 保護

複数のクライアントを使用してDoS攻撃を開始することでレート制限を超える複雑な攻撃は、DDoS 攻撃と呼ばれます。個々のシステムが、DDoS 攻撃を検出したり、適切に反応したりできない場合が多く発生します。このような攻撃を回避するには、適切なレート制限を適用することによってトラフィックが規制されていることを確認します。

DDoS 攻撃を処理する最も効果的な方法の 1 つは、コンテンツ配信ネットワーク（CDN）を利用することによって、ほとんどの攻撃に対して高いレベルの保護を提供し、これらの総当たり攻撃の衝撃を吸収することです。DDoS 署名を検出できる IPS デバイス、ルータ、またはファイアウォールを組み込むことも、このような攻撃を防ぐのに役立ちます。

# Java のアップグレード

Unified CCE は、インストールおよびアップグレード中に、基本として必要な Java バージョンをインストールします。

次のように、コンタクトセンターに Java の更新を適用できます。

- 最新の 32 ビット Java 8 マイナーバージョンの Java アップデートを適用します。

  最新の Java サポート情報については、https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html にある「Contact Center Enterprise 互換性マトリクス」を参照してください。

  OpenJDK の Java の更新は OpenLogic Web サイトからダウンロードおよびインストールできます。

- Windows CCE_JAVA_HOME環境変数を変更し、変更された場合は、新しい OpenJDKJava ランタイム環境（JRE）の場所をポイントします。

# Tomcat ユーティリティのアップグレード

オプションの Cisco アップグレード Tomcat ユーティリティを使用して、次のことを実行します。

- Tomcat をバージョン 9.0 ビルドリリースにアップグレードします（つまり、バージョン 9.0 ビルドリリースのみがこのツールで動作します）。最新のセキュリティ修正に対応するために、Tomcat リリース 9.0 の新しいビルドへのアップグレードを選択することができます。

  Tomcat では、メジャー.マイナー.ビルドというリリース番号のスキームが使用されます。たとえば、9.0.21 から 9.0.22 にアップグレードできます。このツールは、メジャーバージョンまたはマイナーバージョンのアップグレードには使用できません。

- 最近インストールした Tomcat が問題の原因である場合は、このユーティリティを使用して以前のバージョンをインストールします。

ツールを使用する前に:

- Tomcat インストーラー（apache-tomcat-version.exe）を Tomcat Web サイトからダウンロードします： http://archive.apache.org/dist/tomcat/tomcat-9/。インストーラーを Unified CCE コンポーネント VM にコピーします。C:\UpgradeTomcatTool など。

- ユーティリティ zip ファイルをダウンロードし、解凍し、バッチファイルを実行して Tomcat をアップグレードします。

  ダウンロード リンク: https://software.cisco.com/download/home/284360381/type/284416107/release/12.6(1)

- これらのディレクトリ内のサイズの大きいログファイルを削除またはバックアップして、アップグレード時間を短縮します：

  c:\icm\tomcat\logs
  c:\icm\debug.txt

# Tomcat のインストール

各ステップの結果の詳細については、以下を参照してください。/UpgradeTomcatResults/UpgradeTomcat.log ファイル。

（注） Tomcat ユーティリティを使用する前に、VM 上の Unified CCE サービスを停止します。

**手順**

**ステップ 1** コマンドラインから、アップグレードした Tomcat ユーティリティをコピーしたディレクトリに移動します。

**ステップ 2** ツールを実行するには、次のコマンドを入力します：**tomcatutility.bat**。

**ステップ 3** プロンプトが表示されたら、使用する Tomcat のインストーラバージョンの完全なパス名を入力します。

次に例を示します。

```
c:\tomcatInstaller\apache-tomcat-9.0.21.exe
```

**ステップ 4** プロンプトが表示されたら、**[はい（yes）]** を入力してインストールを続行します。

**ステップ 5** すべての Unified CCE コンポーネント VM に対して、これらの手順を繰り返します。

# Microsoft セキュリティの更新

サードパーティベンダーからセキュリティおよびソフトウェアの更新パッチを自動的に適用すると、いくつかのリスクがあります。機能の微妙な変化やコードの層が追加されている場合、Cisco Contact Center 製品の全体的なパフォーマンスが変化する可能性があります。

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。Microsoft Windows アップデートを自動的に有効にしないでください。更新スケジュールが、他の Unified ICM/Unified CCE アクティビティと競合する可能性があります。Microsoft Software Update Service または同様のパッチ管理製品を使用して、重大かつ重要なセキュリティパッチを選択して適用検討してください。これらの更新を適用する時期と方法については、Microsoft のガイドラインに従ってください。

（注） Microsoft for Windows、IIS、および SQL によってリリースされた重大なセキュリティパッチまたは累積アップデートのセキュリティリスクを評価します。サイトに必要と思われる重大なセキュリティパッチまたは累積アップデートを適用します。

詳細については、https://www.cisco.com/en/US/products/sw/custcosw/ps1844/prod_bulletins_list.html にある『サードパーティ製のソフトウェアおよびセキュリティ アップデートを使用する場合の *Cisco Customer Contact* ソフトウェア ポリシー』を参照してください。

# Microsoft Internet Information Server（IIS）

インターネット スクリプト エディタには、Internet Information Server（IIS）が必要です。ディストリビュータを除く他のノードでサービスを無効にします。ソリューションのマルチメディア設定にはいくつかの例外があります。その場合は、製品のマニュアルとシステム要件に従ってください。

# 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。

（注） 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。

（注） 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。

**関連トピック**

Windows Server の強化 （131 ページ）

# ネットワークアクセス保護

ネットワークアクセス保護（NAP）は、Windows Server に導入されたプラットフォームとソリューションです。NAPは、クライアントコンピュータのシステム正常性ポリシーへの準拠に基づいてネットワークリソースへのアクセスを制御することで、ネットワークの全体的な整合性を維持するのに役立ちます。

NAP サーバは、システムの正常性ポリシーを使用してクライアントの正常性を検証します。

NAP クライアントのプラットフォーム要件の詳細については、https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html にある「互換性マトリクス」を参照してください。

## ネットワークポリシーサーバ

Unified CCE で承認されたソフトウェア以外の目的で Unified CCE サーバを使用しないでください。Unified CCE VM 上では、ネットワークポリシーサーバを実行しないでください。

## Unified CCE サーバと NAP

NAP は、いくつかの異なる方法で使用できます。ユーザが Unified CCE で使用を検討できる導入オプションの一部を以下に示します。

- 限定されたアクセス環境を使用する Unified CCE サーバ：**サポートされません**

  **警告** このモデルでは、Unified CCE サーバが準拠しなくなると、アクセスできなくなります。このアクセス不能により、マシンが再度準拠するまで、コールセンター全体がダウンします。

- Unified CCE サーバは、モニタリング専用環境を使用します。このモードは、Unified CCE サーバの正常性ステータスを追跡するために便利なものです。
- 正常性の検証から免除される Unified CCE サーバ：このモードでは、Unified CCE サーバは NAP 環境で動作しますが、ネットワークからアクセスできなくなります。Unified CCE サーバの正常性の状態は、他の Unified CCE サーバとの間の通信には影響しません。

# WMI サービスの強化

Windows Management Instrumentation（WMI）は、Windows システムの管理に使用されます。WMI セキュリティは、Windows オペレーティングシステムに組み込まれたセキュリティサブシステムの拡張です。WMI セキュリティには、WMI 名前空間レベルのセキュリティ、Distributed COM（DCOM）セキュリティ、標準 Windows OS セキュリティが含まれます。

# WMI ネームスペースレベルのセキュリティ

名前空間レベルのセキュリティを構成するには、次の手順を実行します。

**手順**

**ステップ 1** `%SYSTEMROOT%\System32\Wmimgmt.msc MMC` コントロールを起動します。

**ステップ 2** **[WMI 制御（WMI Control）]** アイコンを右クリックし、**[プロパティ（Properties）]** を選択します。

**ステップ 3** **[セキュリティ（Security）]** プロパティのページを選択します。

**ステップ 4** ルートフォルダを選択し、**[セキュリティ（Security）]** ボタンをクリックします。

**ステップ 5** 選択リストから全員を削除し、**[OK]** ボタンをクリックします。

<machine>\Administrators にのみすべての権限を与えます。

# その他の詳細なセキュリティに関する検討事項

WMI サービスは、デフォルトで**[手動（Manual）]**のスタートアップに設定されています。サードパーティ管理エージェントは、これらのサービスを使用してシステムデータをキャプチャします。必要ではない場合、WMI サービスは無効にしないでください。

スクリプト環境と一致する方法で DCOM セキュリティの設定を実行します。DCOM セキュリティの使用の詳細については、この WMI セキュリティマニュアルを参照してください。リモートの WMI 接続のセキュリティ保護の詳細については、Microsoft Developer Network の「http://msdn.microsoft.com/en-us/library/aa393266%28v=vs.85%29.aspx」の項目を参照してください。

# SNMP の強化

インストール、地域の名前、ユーザ名、および宛先の設定の詳細については、 *Cisco Unified ICM/Contact Center Enterprise SNMP* ガイド を参照してください。

SNMP 管理機能には Microsoft の管理およびモニタリングツールのサブコンポーネントが必要ですが、Web セットアップツールでは、Microsoft ネイティブ SNMP サービスが無効になります。より安全なエージェント インフラストラクチャが、ネイティブの Microsoft ネイティブ SNMP サービスに置き換わります。Microsoft SNMP サービスを再び有効にしないでください。シスコがインストールした SNMP エージェントと競合する可能性があります。

Microsoft SNMP トラップ サービスを明示的に無効にします。コンタクトセンターサーバ上の SNMP トラップを収集するために管理ソフトウェアを実行しないでください。この制限により、Microsoft SNMP トラップサービスは不要になります。

SNMP プロトコルのバージョン 1 と 2c は、バージョン 3 よりも安全ではありません。SNMP バージョン3は、セキュリティの大幅なステップフォワードを特長とします。企業のファイアウォールの背後にある内部ネットワーク上にあるコンタクトセンターホストの場合は、次の設定を適用して SNMP の管理性を強化します。

1. 大文字と小文字を組み合わせて、SNMP v1/v2c コミュニティストリングまたは SNMP v3 ユーザ名を作成します。共通の「パブリック」および「プライベート」なコミュニティストリングを使用しないでください。推測が難しい名前を作成します。
2. SNMP v3 の使用を強く推奨します。各 SNMP v3 ユーザ名の認証は常に有効にします。プライバシープロトコルの使用も推奨されます。
3. SNMP 管理可能なデバイスへの接続を許可されるホストの数を制限します。
4. SNMP 管理アプリケーションを実行しているホストからの SNMP 要求のみを受け入れる管理可能デバイスで、コミュニティストリングとユーザ名を設定します。（この設定は、コミュニティストリングとユーザ名を定義する際に、SNMP エージェント設定ツールで行います）
5. 認証失敗に対する SNMP トラップの送信を有効にします。これらのトラップは、攻撃者が、コミュニティストリングやユーザ名を「推測」しようとしていることをアラートします。

SNMPの管理可能性はコンタクトセンターサーバにインストールされ、デフォルトで実行されています。ただし、セキュリティ上の理由により、前の設定手順が完了するまでSNMPアクセスは拒否されます。

セキュリティを強化するには、SNMP 管理ステーションと SNMP エージェント間の SNMP トラフィックに IPSec フィルタと IPSec ポリシーを設定します。フィルタとポリシーの設定方法に関する Microsoft の指示に従います。SNMP トラフィックの IPSec ポリシーの詳細については、Microsoft TechNet の項目を参照してください。

# 電話ハッカーの侵入阻止

通信業界では、料金の不正利用が深刻な問題です。電気通信技術の不正使用は企業にコストがかかる可能性があるため、電気通信管理者は、不正な使用を防ぐために必要な予防措置を取る必要があります。Unified CCE 環境では、Unified CM システムをロックダウンする方法と、料金の不正利用を軽減する方法について Cisco.com のリソースで説明しています。

Unified ICM では、Unified ICM スクリプトのラベルノードでダイナミックラベルを使用する場合が主な懸念事項です。ダイナミックラベルを、発信者が入力した情報（外部スクリプトの実行など）から作成した場合、次の形式のラベルを作成できます。

- 9.....
- 9011....
- さらに同様のパターン

これらのラベルは、コールを外部回線にも、国際番号にも送信できます。ルーティングクライアントで設定された一部のダイヤルプランでは、このような番号を通過できます。顧客がこのようなラベルを使用しない場合は、Unified ICM スクリプトで有効なラベルを使用する前にチェックする必要があります。

簡単な例は、「相手の内線が分かっている場合は、入力してください」と発信者に促す ICM スクリプトです。スクリプトは、ダイナミックラベルノードにブラインドで入力された数字を使用します。このスクリプトは、どこからでもコールを転送する場合があります。この動作が不要な場合は、Unified ICM ルーティングスクリプトまたはルーティングクライアントのダイヤルプランのどちらかをチェックして、無効な番号を禁止する必要があります。

Unified ICM スクリプトチェックの例は、次のような式を使用する 「If」 ノードです。

```
substr (Call.CallerEnteredDigits, 1, 1) = "9"
```

このノードの True ブランチはブランチバックして、発信者にもう一度尋ねます。False ブランチを使用すると、コールを続行できます。このケースは一例です。各顧客は、それぞれの環境に基づいて、何を許可し、許可しないのかを決定する必要があります。

Unified ICM は通常、コールを任意の電話番号に転送しません。番号は、法律上の宛先として明示的に設定されている必要があります。また、Unified ICM ルーティングスクリプトのロジックで、スクリプト変数からコールを電話番号に転送できます。スクリプトを作成して、発信者が一連の数字を入力し、スクリプトが宛先の電話番号として扱い、ルーティングクライアントに対してその番号にコールを転送する必要があります。要求した宛先の電話番号が適正か確認するために、このようなスクリプトにロジックを追加します。

# サポートされているコンテンツ セキュリティ ポリシー ディレクティブ

### コンテンツ-セキュリティ ポリシー ディレクティブ

コンテンツ セキュリティ ポリシー（CSP）のディレクティブを使用すると、Web アプリケーションがリソースがロードされている場所を定義することで、XSS 攻撃のリスクを軽減できます。

ブラウザが CSP ディレクティブで指定された場所以外の場所からデータを読み込むのを防ぐため、ヘッダーには CSP ディレクティブが使用されます。

**Websetup** および **Diagnostic Portico** でサポートされるコンテンツ セキュリティ ポリシー ディレクティブ

| CSP directive-name | 説明 | directive-value |
|---|---|---|
| base-uri | このディレクティブは、以下で使用できるURLを制限します。 <base> 追加します。<br>この値が存在しない場合、任意のURLが許可されます。<br>このディレクティブが指定しない場合、ユーザエージェントは次の値を使用します。 <base> 追加します。 | 'self' |
| frame-ancestors | このディレクティブは、<frame> <iframe> <object> <embed><applet> を使用してリソースを埋め込む有効なソースを定義します。 | 'self' |
| default-src | default-src は、JavaScript、画像、CSS、フォント、AJAXリクエスト、フレーム、HTML5メディアなどのコンテンツのロード時に使用されるデフォルトポリシーです。 | **Diagnostic Portico** の場合：'self'、'unsafe-inline' および 'unsafe-eval'<br>**Websetup** の場合：'self' |

Websetup および Diagnostic Portico のコンテンツ ポリシー ヘッダーをサポートするブラウザの詳細については、http://3.%20https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP#Browser_compatibility を参照してください。

# サードパーティのセキュリティプロバイダー

シスコでは 、NTLM、Kerberos V、および IPSec セキュリティプロトコルのオペレーティングシステム実装により、Unified ICM ソフトウェアを適格にしています。

シスコでは、他のサードパーティ製セキュリティプロバイダーの実装をサポートしていません。

# サードパーティ管理エージェント

サーバ オペレーティング システムのインストールでは、便利なサーバ管理とモニタリングを行うエージェントがベンダーに含まれます。

このようなエージェントは有用ですが、パフォーマンスにも影響を及ぼす可能性があります。シスコは、ミッションクリティカルな Unified ICM/CCE サーバでの使用をサポートしません。

警告 このドキュメントで説明するセキュリティポリシーに従ってエージェントを設定します。ピーク時には、ポーリングまたは業務に支障を与えるスキャンを実行するのではなく、メンテナンスウィンドウ用にこれらのアクティビティのスケジュールを設定します。

（注） これらのサードパーティ管理アプリケーションの指示に従ってSNMPサービスをインストールし、サーバに提供される管理機能を活用します。SNMP を指定しない場合、企業管理アプリケーションはハードウェア事前設定アラートを受信します。Unified CCE サーバは、32 ビットの内線エージェントのみをサポートします。

**関連トピック**

一般的なウイルス対策ガイドライン

# 自己暗号化ドライブ

Unified CCE を使用すると、リアルタイムで着信データを暗号化し、発信データを復号する特別なハードウェアを備えた自己暗号化ドライブ（SED）を導入できます。データを暗号化および復号化しても、システム全体のパフォーマンスには影響を及ぼしません。

ディスク上のメディア暗号化キーは、データの暗号化と復号化を制御します。メディア暗号キーの暗号化には、セキュリティキー（キー暗号キーまたは認証パスフレーズとも呼ばれます）が使用されます。セキュリティキーは、ユーザがローカルに提供するか、KMIP サーバを使用してリモートに提供できます。ドライブをロックしている場合は、データを取得する際にセキュリティキーは必要ありません。

SED の詳細については、『***Cisco UCS C* シリーズサーバ統合管理コントローラ *CLI* 設定ガイド**』https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c-series-integrated-management-controller/products-installation-and-configuration-guides-list.html を参照してください。

導入するドライブは、仮想化 Wiki で説明されているハードドライブの仕様と一致する必要があります。詳細については、https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-unified-contact-center-enterprise.htmlを参照してください。

# 内部クラウド接続 API エンドポイント

APIはシステム内部で使用され、完全に認証され、セキュリティコンプライアンスの目的で文書化されています。ただし、お客様の使用やサードパーティとの統合の目的ではサポートされません。

API の一覧を次に示します。

- https://cloudconnecthost:port/<service-name>/status?details=true

- https://cloudconnecthost:port/inventory/<end_point>
- https://cloudconnecthost:port/Get inventory list - /inventory/managedhosts
- https://cloudconnecthost:port/Update Inventory Hosts - /inventory/managedhosts/<productType>/<clusterID>
- https://cloudconnecthost:port/Delete Inventory Hosts - /inventory/managedhosts/<productType>/<clusterID>
- https://cloudconnecthost:port/Get Nodes status - /inventory/status
- https://cloudconnecthost:port/Get Node Public Key - /inventory/controlnode/key
- https://cloudconnecthost:port/Ping API : /contm/ping
- https://cloudconnecthost:port/dataconn/ccxstreamerconfig
- https://cloudconnecthost:port/dataconn/ccestreamerconfig
- https://cloudconnecthost:port/Container List API : /contm/containers
- https://cloudconnecthost:port/Get container API : /contm/containers/{id}
- https://cloudconnecthost:port/Container start API : /contm/containers/{id}/start
- https://cloudconnecthost:port/Container Stop API : /contm/containers/{id}/stop
- https://cloudconnecthost:port/cherrypoint/config
- https://cloudconnecthost:port/cherrypoint/surveyendpoint
- https://cloudconnecthost:port/cherrypoint/dispatchtemplates
- https://cloudconnecthost:port/cherrypoint/dispatchtemplates/{dispatchTemplateId}
- https://cloudconnecthost:port/cherrypoint/surveydispatch/
- https://cloudconnecthost:port/cherrypoint/authtoken
- https://cloudconnecthost:port/cherrypoint/questionnaires
- https://cloudconnecthost:port/cherrypoint/questionnaires/v2
- https://cloudconnecthost:port/cherrypoint/questionnaires/v2/{QuestionnaireName}
- https://cloudconnecthost:port/cloudconnectmgmt/config
- https://cloudconnecthost:port/cloudconnectmgmt/config?details=true
- https://cloudconnecthost:port/cloudconnectmgmt/status
- https://cloudconnecthost:port/cloudconnectmgmt/notify
- https://cloudconnecthost:port/cloudconnectmgmt/token?scopes=scope1,scope2
- https://cloudconnecthost:port/cloudconnectmgmt/token
- https://cloudconnecthost:port/dataconn/status
- https://cloudconnecthost:port/dataconn/maintenance
- https://cloudconnecthost:port/dataconn/ccxstreamerconfig

- https://cloudconnecthost:port/dataconn/ccestreamerconfig

# 内部 CCE API エンドポイント

コンタクトセンター展開用の Unified CCE、Packaged CCE、HCS に適用可能な内部 API を次に示します。これらの API は、顧客の使用またはサードパーティとの統合の目的でサポートされていません。

- `/unifiedconfig/config/activedirectorydomain/`

  システムで使用可能な Active Directory ドメインを取得するには、`GET` メソッドのみをサポートします。

- `/unifiedconfig/config/deployment`

  アプリケーションの現在の導入タイプを取得するには、`GET` メソッドのみをサポートします。

- `/unifiedconfig/config/redirect/`

  要求を他のソリューション コンポーネントにリダイレクトするプロキシ API として使用され、`GET` メソッドと `POST` メソッドの両方をサポートします（この API は PCCE 導入にのみ適用されます）。

- `/unifiedconfig/config/downloadablefiles/`

  プライマリ AW から path param で指定されている IVR アプリケーションファイルをダウンロードするには、`GET` メソッドのみをサポートします。

- `/unifiedconfig/config/smartlicense/sync/`

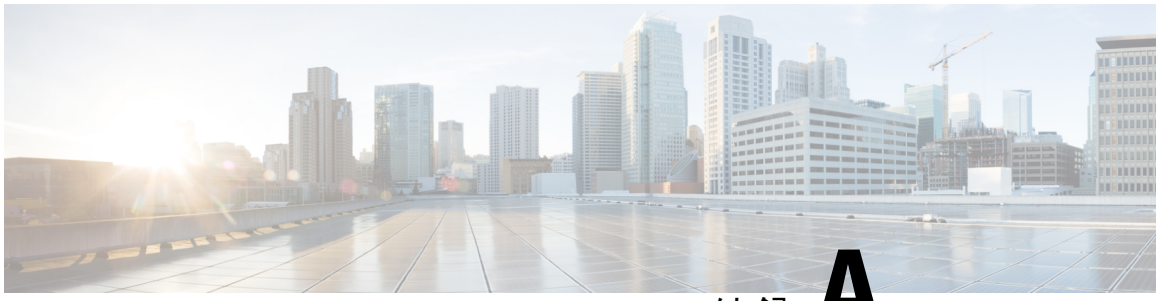
  スマートライセンス情報、ライセンス付与、およびサーバビーンをデータベース内のエントリと比較するには、`GET` メソッドのみサポートします。

- `/unifiedconfig/config/smartlicense/status`

  スマート ライセンス サーバのステータスを取得するには、`GET` メソッドのみをサポートします。

- `/unifiedconfig/config/useridentity/authorization/migration`

  ユーザが Unified CCE to Packaged CCE 移行ツールを実行できるアクセシビリティを確認するには、`GET` メソッドのみをサポートします。



付録 A

# Windows セキュリティの強化



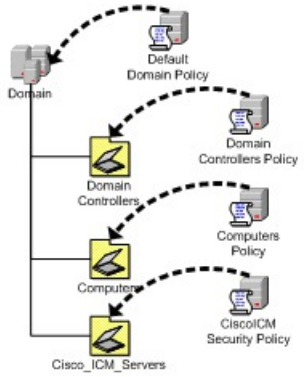
## Windows Server の強化

Unified CCE インストーラには、グループポリシーオブジェクト（GPO）バックアップという形式でセキュリティポリシーがカスタマイズされています。このポリシーは、Unified CCE サーバを含む別の組織ユニット（OU）に適用できます。このポリシーにより、Unified CCE アプリケーションが適切に機能し、セキュリティが向上します。OU を Cisco_ICM_Servers（または同様の明確に識別可能な名前）として明確に識別し、社内ポリシーに従ってその OU が文書化されていることを確認します。

この OU は、**コンピュータ**コンテナと同じレベルで、または Cisco ICM ルート OU で作成します。Active Directory に不慣れな場合は、ドメイン管理者に問い合わせて、グループポリシーの導入を支援してもらいます。

（注） Unified CCE GPO のバックアップは、Windows Server Domain Controller の下に作成されたメンバーサーバ OU にのみ適用できます。

図 7: グループポリシーの展開




OU レベルでセキュリティポリシーを適用した後は、異なるポリシーが Unified ICM/Unified CCE サーバ OU で継承されるのをブロックする必要があります。高い階層レベルで[強制（Enforced）/上書きなし（No Override）] オプションを選択した場合、OU オブジェクトレベルの設定オプションである、ブロックの継承を上書きすることができます。グループポリシーの適用は、最も一般的な分母で始まる考え抜かれた設計に従う必要があります。これらのポリシーは、階層内の適切なレベルでのみ制限する必要があります。

# Windows Server の Unified CCE のセキュリティ強化

このトピックには、Unified CCE を実行している Windows サーバの強化に関するセキュリティ基準について説明します。

を編集したものです。

次の表に示す GPO 設定に加えて、次の設定を無効にします。

- NetBIOS
- SMBv1

（注） これらの設定の詳細については、Microsoft Windows Server のマニュアルを参照してください。

この基準には、重大度が「重大」および「重要」と評価される設定だけが含まれます。[オプション（Optional）]および[なし（None）]の条件を含む設定は、この基準には含まれません。

| 設定名 | デフォルト値（Default Value） | コンプライアンス |
|---|---|---|
| ネットワーク セキュリティ：LAN Manager 認証レベル | NTLMv2 応答のみを送信 | NTLMv2応答のみを送信。LM & NTLM は拒否 |

| 設定名 | デフォルト値（Default Value） | コンプライアンス |
|---|---|---|
| ネットワークセキュリティ：NTLM の制限：このドメインで NTLM の認証を監査 | 未定義 | 未定義 |
| ネットワーク セキュリティ：NTLM の制限：着信 NTLM トラフィック | 未定義 | 未定義 |
| インタラクティブ ログオン：スマートカードが必要 | 未定義 | 未定義 |
| ネットワークセキュリティ：NTLM の制限：NTLM 認証用のリモートサーバ例外を追加 | 未定義 | 未定義 |
| ネットワークセキュリティ：LocalSystem NULL セッションフォールバックを許可する | 未定義 | 無効 |
| Microsoft ネットワーククライアント：暗号化されていないパスワードをサードパーティの WEB サーバに送信 | 無効 | 無効 |
| ネットワークセキュリティ：ローカルシステムが NTLM でコンピュータ ID を使用することを許可 | 無効 | 有効 |
| ネットワークセキュリティ：次のパスワード変更で LAN Manager ハッシュ値を保存しない | 有効 | 有効 |
| ネットワークセキュリティ：このコンピュータに対する PKU2U 認証要求を許可して、オンラインのアイデンティティを使用 | 未定義 | 未定義 |

Windows セキュリティの強化

| 設定名 | デフォルト値（Default Value） | コンプライアンス |
|---|---|---|
| ネットワークセキュリティ：NTLM SSP ベースサーバ（セキュアな RPC を含む）のための最小限のセッションセキュリティ | 128 ビット暗号化が必要 | NTLMv2 セッションセキュリティが必要、128 ビット暗号化が必要 |
| Microsoft ネットワークサーバ：サーバ SPN ターゲット名の検証レベル | 未定義 | 未定義 |
| インタラクティブログオン：スマートカードの削除操作 | アクションなし | ワークステーションのロック |
| ネットワークセキュリティ：NTLM SSP ベースクライアント（セキュアな RPC を含む）のための最小限のセッションセキュリティ | 128 ビット暗号化が必要 | NTLMv2 セッションセキュリティが必要、128 ビット暗号化が必要 |
| インタラクティブログオン：キャッシュに対する前回のログオン回数（ドメインコントローラが利用できない場合） | ログオン 10 回 | ログオン 4 回 |
| ネットワークセキュリティ：NTLM の制限：このドメインの NTLM の認証 | 未定義 | 未定義 |
| ネットワークセキュリティ：NTLM の制限：リモートサーバへの発信 NTLM トラフィック | 未定義 | 未定義 |
| ネットワークアクセス：匿名ユーザに対してすべてのユーザの権限を適用 | 無効 | 無効 |

| 設定名 | デフォルト値（Default Value） | コンプライアンス |
|---|---|---|
| ネットワークセキュリティ：NTLM の制限：このドメインにサーバ例外を追加 | 未定義 | 未定義 |
| ネットワークセキュリティ：NTLM の制限：着信 NTLM トラフィックの監査 | 未定義 | 未定義 |
| ネットワークアクセス：SAM のアカウントと共有の匿名列挙を許可しない | 無効 | 有効 |
| ネットワークアクセス：SAM のアカウントの匿名列挙を許可しない | 有効 | 有効 |
| シャットダウン：仮想メモリのページファイルの消去 | 無効 | 無効 |
| ネットワークアクセス：リモートでアクセスできるレジストリパス | System\CurrentControlSet\Control\ ProductOptionsSystem\ CurrentControlSet\Control\ Server Applications Software\Microsoft\ WindowsNT\CurrentVersion | System\CurrentControlSet\Control\ ProductOptionsSystem\ CurrentControlSet\Control\ Server Applications Software\Microsoft\ WindowsNT\CurrentVersion |
| ネットワークアクセス：匿名でアクセスできる共有 | 未定義 | 未定義 |
| ファイルとフォルダの「Web に公開」タスクをオフにする | 未設定 | 未設定 |
| シャットダウン：ログオンすることなくシステムのシャットダウンを許可する | 無効 | 無効 |
| システムオブジェクト：Windows 以外のサブシステムに大文字と小文字を区別しない | 有効 | 有効 |

Windows セキュリティの強化

| 設定名 | デフォルト値（Default Value） | コンプライアンス |
|---|---|---|
| ネットワークアクセス：ローカルアカウントの共有とセキュリティモデル | クラシック - ローカルユーザは、自身で認証 | クラシック - ローカルユーザは、自身で認証 |
| インタラクティブログオン：CTRL+ALT+DEL を要求しない | 有効 | 無効 |
| デバイス：取り外し可能なメディアのフォーマットと取り出しを許可 | 管理者 | 管理者 |
| Windows Messenger のカスタマーエクスペリエンス向上プログラムの電源を切る | 未設定 | 未設定 |
| システム設定：ソフトウェア制限ポリシーに Windows の実行ファイルで証明書ルールを使用する | 無効 | 無効 |
| 検索コンパニオン コンテンツ ファイルの更新をオフにする | 未設定 | 未設定 |
| ネットワークアクセス：匿名の SID/名前変換を許可 | 無効 | 無効 |

Windows セキュリティの強化

| 設定名 | デフォルト値（Default Value） | コンプライアンス |
|---|---|---|
| ネットワークアクセス：リモートでアクセスできる登録パスとサブパス | System\CurrentControlSet\Control\Print\ PrintersSystem\CurrentControlSet\Services\ Eventlog, Software\Microsoft\OLAP ServerSoftware\ Microsoft\Windows NT\CurrentVersion\Print Software\ Microsoft\WindowsNT\CurrentVersion\ Windows System\CurrentControlSet\Control\ ContentIndexSystem\CurrentControlSet\ Control\Terminal ServerSystem\ CurrentControlSet\Control\Terminal Server\ UserConfigSystem\CurrentControlSet\ Control\Terminal Server\ DefaultUserConfigurationSoftware\ Microsoft\Windows NT\CurrentVersion\PerflibSystem\ CurrentControlSet\Services\SysmonLog | System\CurrentControlSet\Control\Print\ PrintersSystem\CurrentControlSet\Services\ Eventlog, Software\Microsoft\OLAP ServerSoftware\ Microsoft\Windows NT\CurrentVersion\Print Software\ Microsoft\WindowsNT\CurrentVersion\ Windows System\CurrentControlSet\Control\ ContentIndexSystem\CurrentControlSet\ Control\Terminal ServerSystem\ CurrentControlSet\Control\Terminal Server\ UserConfigSystem\CurrentControlSet\ Control\Terminal Server\ DefaultUserConfigurationSoftware\ Microsoft\Windows NT\CurrentVersion\PerflibSystem\ CurrentControlSet\Services\SysmonLog |
| 回復コンソール：自動管理ログオンを許可する | 無効 | 無効 |
| 自動再生をオフにする | 無効 | 有効 |
| Windows Update デバイスドライバの検索をオフにする | 未設定 | 未設定 |
| ネットワークアクセス：名前付きパイプおよび共有への匿名アクセスを制限する | 有効 | 有効 |
| 回復コンソール：フロッピーコピーを許可し、すべてのドライブとすべてのフォルダへのアクセスを許可する | 無効 | 無効 |
| ネットワークアクセス：匿名でアクセスできる名前の付いたパイプ | 未定義 | 未定義 |
| ポリシーの監査：システム：IPSec ドライバ | 監査なし | 成功と失敗 |

Windows セキュリティの強化

| 設定名 | デフォルト値（Default Value） | コンプライアンス |
|---|---|---|
| 監査ポリシー：システム：セキュリティシステムの拡張 | 監査なし | 成功と失敗 |
| 監査ポリシー：アカウント管理：セキュリティグループ管理 | 成功 | 成功と失敗 |
| 監査：監査ポリシーサブカテゴリ設定を強制（Windows Vista 以降）して、監査ポリシーカテゴリの設定を上書きする | なし | 有効 |
| 監査ポリシー：アカウント管理：その他のアカウント管理イベント | 監査なし | 成功と失敗 |
| 監査ポリシー：システム：セキュリティ状態の変更 | 成功 | 成功と失敗 |
| 監査ポリシー：詳細なトラッキング：プロセスの作成 | 監査なし | 成功 |
| 監査ポリシー：システム：その他のシステムイベント | 成功と失敗 | 成功と失敗 |
| 監査ポリシー：ログインとログアウト：アカウントのロックアウト | 成功 | 成功 |
| 監査ポリシー：ポリシーの変更：監査ポリシーの変更 | 成功 | 成功と失敗 |
| 監査：グローバル システム オブジェクトへのアクセスを監査する | 未定義 | 未定義 |
| 監査ポリシー：ログイン-ログアウト：特別なログイン | 成功 | 成功 |

| 設定名 | デフォルト値（Default Value） | コンプライアンス |
|---|---|---|
| 監査ポリシー：アカウント管理：ユーザアカウント管理 | 成功 | 成功と失敗 |
| 監査ポリシー：アカウントログイン：資格情報の検証 | 成功 | 成功と失敗 |
| 監査ポリシー：ログイン-ログアウト：ログイン | 成功 | 成功と失敗 |
| 監査ポリシー：アカウント管理：コンピュータアカウント管理 | 成功 | 成功 |
| 監査ポリシー：特権の使用：機密性の高い特権の使用 | 成功 | 成功と失敗 |
| 監査ポリシー：ログイン-ログアウト：ログアウト | 成功 | 成功 |
| 監査ポリシー：ポリシーの変更：監査ポリシーの認証 | 成功 | 成功 |
| 監査：バックアップと復元の権限の使用を監査する | 未定義 | 未定義 |
| 監査ポリシー：システム：システムの整合性 | 成功と失敗 | 成功と失敗 |
| ロック画面で Toast 通知をオフにする | 無効 | 有効 |
| Microsoft ネットワークサーバ：セッションを一時停止する前に必要なアイドル時間 | 15 分 | 15 分 |
| インタラクティブログオン：ログオンしようとしているユーザへのメッセージテキスト | 未定義 | 未定義 |

Windows セキュリティの強化

| 設定名 | デフォルト値（Default Value） | コンプライアンス |
|---|---|---|
| インタラクティブログイン：マシンの非アクティブ状態の制限 | 0 秒 | 900 秒 |
| Microsoft ネットワークサーバ：ログオン時間の期限が切れたときにクライアントを切断する | 有効 | 有効 |
| インタラクティブログオン：ログオンしようとしているユーザへのメッセージタイトル | 未定義 | 未定義 |
| ネットワークセキュリティ：ログイン時間の期限が切れるとき、強制的にログオフする | 有効 | 有効 |
| システムが開始した再起動後、最後のインタラクティブユーザに自動的にサインイン | 有効 | 無効 |
| インタラクティブログイン：セッションがロックされているときにユーザ情報を表示する | 未定義 | 未定義 |
| インタラクティブログイン：最後のユーザ名を表示しない | 無効 | 有効 |
| インタラクティブログイン：マシンアカウントのロックアウトのしきい値 | 未定義 | 無効なログイン試行 10 回 |
| リモートシェルアクセスを許可する | 未設定 | 未設定 |
| デバイス：ユーザによるプリンタドライバのインストールを防ぐ | 有効 | 有効 |

| 設定名 | デフォルト値（Default Value） | コンプライアンス |
|---|---|---|
| グローバルオブジェクトの作成 | 管理者、サービス、ローカルサービス、ネットワークサービス | 管理者、サービス、ローカルサービス、ネットワークサービス |
| ネットワークからこのコンピュータにアクセスする | 全員、管理者、ユーザ、バックアップオペレータ | 管理者、認証済みユーザ |
| ドメインコントローラ：サーバオペレータによるタスクのスケジュールの設定を許可する | 未定義 | 未定義 |
| オブジェクトラベルの変更 | なし | なし |
| セキュリティの監査を生成する | ローカルサービス、ネットワークサービス | ローカルサービス、ネットワークサービス |
| スケジュール設定の優先順位を上げる | 管理者 | 管理者 |
| リモートシステムからのシャットダウンを強制する | 管理者 | 管理者 |
| リモート デスクトップ サービスによるログインを許可する | 管理者、リモートデスクトップユーザ | 管理者 |
| システム時刻を変更する | ローカルサービス、管理者 | ローカルサービス、管理者 |
| ドメインにワークステーションを追加する | 未定義（ドメインコントローラの認証済みユーザ） | 未定義 |
| ページファイルを作成する | 管理者 | 管理者 |
| 単一プロセス プロファイル | 管理者 | 管理者 |
| バッチ処理としてのログインを拒否する | なし | ゲスト |
| オペレーティングシステムの役割を果たす | なし | なし |

Windows セキュリティの強化

| 設定名 | デフォルト値（Default Value） | コンプライアンス |
|---|---|---|
| タイムゾーンの変更 | ローカルサービス、管理者 | ローカルサービス、管理者 |
| ディレクトリサービスデータを同期する | 未定義 | 未定義 |
| メモリ内のページをロックする | なし | なし |
| 信頼できる発信者として資格情報マネージャーにアクセスする | なし | なし |
| トークンオブジェクトを作成する | なし | なし |
| プログラムのデバッグ | 管理者 | 管理者 |
| サービスとしてのログインを拒否する | なし | ゲスト |
| ネットワークからのこのコンピュータへのアクセスを拒否する | ゲスト | ゲスト、NT AUTHORITY\Local アカウント、および管理者グループのメンバー |
| ファイルとディレクトリのバックアップ | 管理者、バックアップオペレータ | 管理者 |
| システムをシャットダウンする | 管理者、バックアップオペレータ、ユーザ | 管理者 |
| ローカルでのログインを拒否する | ゲスト | ゲスト |
| プロセスレベルトークンを置き換える | ローカルサービス、ネットワークサービス | ローカルサービス、ネットワークサービス |
| ファームウェア環境の値を変更する | 管理者 | 管理者 |
| ローカルからのログオンを許可 | ゲスト、管理者、パワーユーザ、ユーザ、バックアップオペレータ | 管理者、ユーザ |
| ファイルとディレクトリの復元 | 管理者、バックアップオペレータ | 管理者 |
| システム パフォーマンス プロファイル | 管理者、NT Service\WdiServiceHost | 管理者、NT Service\WdiServiceHost |

| 設定名 | デフォルト値（Default Value） | コンプライアンス |
|---|---|---|
| バッチ処理としてログインする | 未定義 | 未定義 |
| ボリューム メンテナンス タスクを実行する | 管理者 | 管理者 |
| 監査ログとセキュリティログを管理する | 管理者 | 管理者 |
| コンピュータアカウントとユーザアカウントの信頼を高めて委任できるようにする | なし | なし |
| 認証後にクライアントになりすます | 管理者、サービス、ローカルサービス、ネットワークサービス | 管理者、サービス、ローカルサービス、ネットワークサービス |
| デバイスドライバをロードし、ロードを解除する | 管理者 | 管理者 |
| ファイルやその他のオブジェクトの所有権取得 | 管理者 | 管理者 |
| プロセスのメモリ容量を調整する | ローカルサービス、ネットワークサービス、管理者 | 管理者、ローカルサービス、ネットワークサービス |
| サービスとしてログイン | 未定義 | 未定義 |
| シンボリックリンクを作成する | 管理者 | 管理者 |
| 永続共有オブジェクトを作成する | なし | なし |
| システム暗号化：コンピュータに保存されているユーザキーに対して強力なキー保護を強制する | 未定義 | 未定義 |
| ドメインメンバー：強力な（Windows 2000 以降）セッションキーを要求する | 有効 | 有効 |

Windows セキュリティの強化

| 設定名 | デフォルト値（Default Value） | コンプライアンス |
|---|---|---|
| Windows ファイアウォール：ドメイン：ユニキャスト応答を許可する | はい | いいえ |
| Windows ファイアウォール：ドメイン：ローカル ファイアウォール ルールを適用する | はい | [はい（Yes）]（デフォルト） |
| Windows ファイアウォール：ドメイン：インバウンド接続 | Block | 有効 |
| Windows ファイアウォール：プライベート ファイアウォールの状態 | オン | オン |
| Windows ファイアウォール：プライベート：ローカル接続のセキュリティ ルールを適用する | はい | [はい（Yes）]（デフォルト） |
| Windows ファイアウォール：プライベート：ユニキャスト応答を許可する | はい | いいえ |
| Windows ファイアウォール：パブリック：ローカル ファイアウォール ルールを適用する | はい | [はい（Yes）]（デフォルト） |
| Windows ファイアウォール：パブリック：ローカル接続のセキュリティ ルールを適用する | はい | はい |
| Windows ファイアウォール：パブリック：ファイアウォールの状態 | オン | オン |
| Windows ファイアウォール：プライベート：アウトバウンド接続 | 許可 | 許可する（デフォルト） |

| 設定名 | デフォルト値（Default Value） | コンプライアンス |
|---|---|---|
| Windows ファイアウォール：ドメイン：アウトバウンド接続 | 許可 | 許可する（デフォルト） |
| Windows ファイアウォール：ドメイン：ファイアウォールの状態 | オン | オン |
| Windows ファイアウォール：パブリック：ユニキャスト応答を許可する | × | × |
| Windows ファイアウォール：パブリック：インバウンド接続 | Block | 有効 |
| Windows ファイアウォール：ドメイン：ローカル接続のセキュリティルールを適用する | はい | [はい（Yes）]（デフォルト） |
| Windows ファイアウォール：プライベート：通知を表示する | はい | [はい（Yes）]（デフォルト） |
| Windows ファイアウォール：ドメイン：通知を表示する | はい | [はい（Yes）]（デフォルト） |
| Windows ファイアウォール：パブリック：通知を表示する | はい | はい |
| Windows ファイアウォール：パブリック：アウトバウンド接続 | 許可 | 許可する（デフォルト） |
| Windows ファイアウォール：プライベート：インバウンド接続 | Block | 有効 |
| Windows ファイアウォール：プライベート：ローカル ファイアウォール ルールを適用する | はい | [はい（Yes）]（デフォルト） |

Windows セキュリティの強化

| 設定名 | デフォルト値（Default Value） | コンプライアンス |
|---|---|---|
| Internet Explorer のデフォルトの保護 | 有効 | 有効 |
| スクリーンセーバーのパスワード保護 | 未設定 | 有効 |
| ローカルポリシー<br>ユーザアカウント制御：組み込み管理者アカウントの管理者承認モード | 無効 | 無効 |
| ソフトウェアのデフォルト保護 | なし | 有効 |
| ユーザアカウント制御：安全な場所にインストールされているUIアクセスアプリケーションのみを利用できます。 | 有効 | 有効 |
| ネットワークログオンでローカルアカウントにUACの制限を適用する | なし | 有効 |
| ユーザアカウント制御：管理者承認モードでの管理者に対する特権プロンプトの動作 | Windows 以外のバイナリに対する同意を求めるプロンプト | セキュアなデスクトップに対する同意のプロンプト |
| ユーザアカウント制御：安全なデスクトップを使用せずにUIアクセスのアプリケーションの昇格プロンプトを許可する | 無効 | 無効 |
| ローカルポリシー<br>ユーザアカウント制御：ユーザごとの場所に対するファイルおよびレジストリの書き込み失敗を仮想化する | なし | 無効 |

| 設定名 | デフォルト値（Default Value） | コンプライアンス |
|---|---|---|
| ユーザアカウント制御：昇格プロンプトの際にセキュアなデスクトップに切り替える | 有効 | 有効 |
| ユーザアカウント制御：管理者承認モードですべての管理者を実行する | 有効 | 有効 |
| ダイジェスト認証 | 無効 | 無効 |
| ユーザアカウント制御：標準ユーザに対する昇格プロンプトの動作 | クレデンシャル用のプロンプト | 昇格要求を自動的に拒否する |
| System ASLR | なし | 有効 |
| System DEP | 有効 | 有効 |
| システムオブジェクト：内部システムオブジェクトのデフォルト許可を強化（例：シンボリックリンク） | 有効 | 有効 |
| スクリーンセーバーを有効にする | スクリーンセーバーの有効化または無効化は、ユーザがローカルで管理します。 | 有効 |
| 特定のスクリーンセーバーを強制する | 無効 | 有効 |
| プロセス作業セットを増加する | 未定義 | 未定義 |
| ユーザアカウント制御：アプリケーションのインストールを検出し、昇格をプロンプトする | 無効 | 有効 |
| システム SEHOP | 有効：アプリケーションのオプトアウト | 有効 |
| ネットワークセキュリティ：Kerberos に許可される暗号化タイプを設定する | 未定義 | 未定義 |

Windows セキュリティの強化

| 設定名 | デフォルト値（Default Value） | コンプライアンス |
|---|---|---|
| クライアント接続の暗号化レベルを設定する | 未設定 | 未設定 |
| Microsoft ネットワーククライアント：デジタル署名通信（サーバが同意する場合） | 有効 | 有効 |
| ドメインコントローラ：LDAP サーバ署名の要件 | 未定義 | 未定義 |
| ネットワークセキュリティ：LDAP クライアント署名の要件 | 署名のネゴシエート | 署名のネゴシエート |
| Microsoft ネットワーククライアント：デジタル署名通信（常時） | 無効 | 有効 |
| Microsoft ネットワークサーバ：デジタル署名通信（常時） | 無効 | 有効 |
| ドメインメンバー：セキュアなチャネルデータにデジタルで署名する（可能な場合） | 有効 | 有効 |
| ドメインメンバー：安全なチャネルデータをデジタルで暗号化または署名する（常時） | 有効 | 有効 |
| Microsoft ネットワークサーバ：デジタル署名通信（クライアントが同意する場合） | 無効 | 有効 |
| ドメインメンバー：セキュアなチャネルデータにデジタルで暗号化する（可能な場合） | 有効 | 有効 |
| 最大ログファイルのサイズ（KB）を指定する | 20480 KB | 有効 |

| 設定名 | デフォルト値（Default Value） | コンプライアンス |
|---|---|---|
| 最大ログファイルのサイズ（KB）を指定する | 20480 KB | 有効 |
| 最大ログファイルのサイズ（KB）を指定する | 20480 KB | 有効 |
| 監査：セキュリティ監査が記録できない場合、システムを即時にシャットダウンする | 無効 | 無効 |
| アカウント：ローカルアカウントでの空白のパスワードの使用をコンソールログオンにのみ制限する | 有効 | 有効 |
| ドメインコントローラ：マシンアカウントのパスワード変更を拒否する | 未定義 | 未定義 |
| ドメインメンバー：マシンアカウントのパスワード変更を無効にする | 無効 | 無効 |
| ドメインメンバー：マシンアカウントのパスワードの最大使用時間 | 30 日 | 30 日 |
| ネットワークアクセス：ネットワーク認証用のパスワードと資格情報の保管を許可しない | 未定義 | 未定義 |
| インタラクティブログオン：ユーザにプロンプトして、有効期限が切れる前にパスワードを変更する | 5 日 | 14 日 |
| 暗号化されたファイルのインデックス作成を許可する | 無効 | 無効 |
| アカウント：管理者アカウントの名前を変更する | 未定義 | 未定義 |

Windows セキュリティの強化

| 設定名 | デフォルト値（Default Value） | コンプライアンス |
|---|---|---|
| ネットワーク選択UIを表示しない | 無効 | 有効 |
| Microsoft のアカウントをオプションにするのを許可する | 無効 | 有効 |
| アカウント：管理者アカウントのステータス | 無効 | 未定義 |
| アカウント：ゲストアカウントステータス | 無効 | 無効 |
| アカウント：ゲストアカウントの名前を変更する | ゲスト | 未定義 |
| ロック画面のスライドショーの有効化を防止する | 無効 | 有効 |
| ロック画面カメラの有効化を防止する | 無効 | 有効 |
| IRC ポート | 無効 | 無効 |
| 発信電子メールポート 25 | 無効 | 無効 |
| 詳細な監査ポリシー設定 -アカウントログイン：資格情報の検証を監査する | 成功 | 成功と失敗 |
| 管理用テンプレート（コンピュータ）：<br>昇格特権を付与された状態で常にインストールする | 無効 | 無効 |
| 詳細な監査ポリシー設定 -オブジェクトアクセス：<br>その他のオブジェクト アクセス イベントを監査する | 監査なし | 成功と失敗 |

| 設定名 | デフォルト値（Default Value） | コンプライアンス |
|---|---|---|
| 管理用テンプレート（ユーザ）- クラウドコンテンツ：<br>Windows のスポットライトにサードパーティ製コンテンツを推奨しない | 無効 | 有効 |
| 管理用テンプレート（ユーザ）クラウドコンテンツ：カスタマイズされたエクスペリエンスに診断データを使用しない | 無効 | 有効 |
| 管理用テンプレート（ユーザ）クラウドコンテンツ：すべての Windows スポットライト機能をオフにする | 無効 | 有効 |
| 管理用テンプレート（コンピュータ）：入力のパーソナル化を許可する | 有効 | 無効 |
| 管理用テンプレート（コンピュータ）；オンラインヒントを許可する | 有効 | 無効 |
| 管理テンプレート（コンピュータ）：構造例外処理上書き保護（SEHOP）を有効にする | 32 ビットプロセスで無効化 | 有効 |
| 管理用テンプレート（コンピュータ）：マルチキャスト名解像度をオフにする | 無効 | 有効 |

Windows セキュリティの強化

| 設定名 | デフォルト値（Default Value） | コンプライアンス |
|---|---|---|
| 管理用テンプレート（コンピュータ）；フォントプロバイダーを有効にする | 有効<br>（注） Windows に含まれるがローカルに保存されていないフォントを、オンデマンドでオンラインのフォントプロバイダーからダウンロードできます。 | 無効 |
| 管理テンプレート（コンピュータ）：セキュアでないゲストログインを有効にする | 有効<br>（注） SMB クライアントは、セキュアでないゲストログインを許可します。 | 無効 |
| 管理用テンプレート（コンピュータ）：DNS ドメインネットワークでのインターネット接続共有の使用を禁止する | 無効<br>（注） すべてのユーザがモバイルホットスポットにアクセスできます。 | 有効 |
| 管理用テンプレート（コンピュータ）：リモートホストはエクスポートできない資格情報の委任を許可する | 無効 | 有効 |
| 管理用テンプレート（コンピュータ）：このデバイスでエクスペリエンスを継続する | デフォルトの動作は、Windows Edition によって異なります。 | 無効 |
| 管理用テンプレート（コンピュータ）：サインインの時にユーザーに対するアカウント詳細の表示をブロックする | 無効<br>（注） サインイン画面にアカウントの詳細を表示するかを選択できます。 | 有効 |
| 管理用テンプレート（コンピュータ）：ピクチャパスワードのサインインをオフにする | 無効<br>（注） 画像パスワードを設定して使用することができます。 | 有効 |

| 設定名 | デフォルト値（Default Value） | コンプライアンス |
|---|---|---|
| 管理用テンプレート（コンピュータ）：信頼されないフォントブロッキング | オフ<br>（注） ブロックされたフォントはありません。 | 有効<br>（注） 信頼されていないフォントとログイベントはブロックされます。 |
| 管理用テンプレート（コンピュータ）：接続したスタンバイ（プラグイン）中のネットワーク接続を許可する | 有効<br>（注） 接続すると、ネットワーク接続がスタンバイモードになります。 | 無効 |
| 管理用テンプレート（コンピュータ）：アドバタイジング ID をオフにする | 無効<br>（注） アプリケーションが、すべてのアプリケーションにわたるエクスペリエンスにアドバタイジングIDを使用できるかどうかを選択できます。 | 有効 |
| 管理用テンプレート（コンピュータ）：Windows アプリでアプリケーションデータをユーザ間で共有するのを許可する | 無効 | 無効 |
| 管理用テンプレート（コンピュータ）：強化されたスプーフィング対策を設定する | サポートされているデバイスで拡張スプーフィングを有効または無効にできます。 | 有効 |
| 管理用テンプレート（コンピュータ）：カメラの使用を許可する | 有効<br>（注） カメラデバイスが有効化されています。 | 無効 |
| 管理用テンプレート（コンピュータ）：Microsoft のコンシューマ エクスペリエンスをオフにする | 無効<br>（注） Microsoftからの提案と、Microsoftアカウントに関する通知が表示されます。 | 有効 |

Windows セキュリティの強化

| 設定名 | デフォルト値（Default Value） | コンプライアンス |
|---|---|---|
| 管理用テンプレート（コンピュータ）：<br>ペアリングにピンが必要 | 無効<br>（注） ワイヤレスディスプレイデバイスとペアリングする場合は、個人識別番号（PIN）は不要です。 | 有効 |
| 管理用テンプレート（コンピュータ）：<br>テレメトリを許可する | 無効<br>（注） テレメトリレベルは設定で構成できます。 | 有効：0-セキュリティ [企業のみ] |
| 管理用テンプレート（コンピュータ）：<br>接続されたユーザエクスペリエンスとテレメトリサービス用に認証済みのプロキシ使用量を設定する | 無効<br>（注） 接続されたユーザエクスペリエンスとテレメトリサービスは、認証済みのプロキシを使用してデータを自動的に Microsoft に返送します。 | 有効<br>（注） 認証済みプロキシが無効になっています。 |
| 管理用テンプレート（コンピュータ）：<br>プレリリースの機能または設定を無効にする | [設定（Settings）]で、**このビルドで Microsoft が機能を試行できるようにする**オプションを構成できます。 | 無効 |
| 管理用テンプレート（コンピュータ）：<br>フィードバック通知を表示しない | 無効<br>（注） Windows フィードバックアプリケーションには、フィードバックの通知が表示されます。フィードバックの質問を受信する時間を設定できます。 | 有効 |
| 管理用テンプレート（コンピュータ）：<br>インサイダービルドのユーザ制御を切り替える | 有効<br>（注） デバイスに Windows プレビューソフトウェアをダウンロードしてインストールできます。 | 無効 |

| 設定名 | デフォルト値（Default Value） | コンプライアンス |
|---|---|---|
| 管理用テンプレート（コンピュータ）：<br>システム：最大ログファイルのサイズ（KB）を指定する | 無効<br>（注） デフォルトのログサイズは 20,480 KB です。ローカル管理者は **[ログのプロパティ（Log Properties）]** ダイアログを使用して、この値を変更できます。 | 有効 - 32,768 以上 |
| 管理用テンプレート（コンピュータ）：<br>メッセージ サービス クラウド同期を許可する | 有効 | 無効 |
| 管理用テンプレート（コンピュータ）：<br>すべてのコンシューマ Microsoft アカウントのユーザ認証をブロックする | 無効 | 有効 |
| 管理用テンプレート（コンピュータ）：<br>ファイル保管用の OneDrive の使用を防止する | 無効 | 有効 |
| 管理用テンプレート（コンピュータ）：<br>クラウド検索を許可する | 有効<br>（注） クラウド検索が有効になっている - これは、検索と Cortana が OneDrive や SharePoint のようなクラウドソースを検索することができます。 | 有効<br>（注） クラウド検索が無効になっています。 |
| 管理用テンプレート（コンピュータ）：<br>Watson イベントを設定する | 有効<br>（注） プログラムまたはサービスがクラッシュまたは失敗すると、Watson のイベントが自動的に Microsoft に送信されます。 | 無効 |

Windows セキュリティの強化

| 設定名 | デフォルト値（Default Value） | コンプライアンス |
|---|---|---|
| 管理用テンプレート（コンピュータ）：<br>削除可能なドライブをスキャンする | 無効<br>（注） 削除可能なドライブは、フルスキャン中はスキャンされませんが、クイックまたはカスタムスキャンの間はスキャンできます。 | 有効 |
| 管理用テンプレート（コンピュータ）：<br>電子メールスキャンをオンにする | 無効<br>（注） Windows Defender ウイルス対策による電子メールスキャンは無効になっています。 | 有効 |
| 管理用テンプレート（コンピュータ）：<br>攻撃対象領域の削減ルールを設定する | 無効<br>（注） ASR ルールが設定されていません。 | 有効 |
| 管理用テンプレート（コンピュータ）：<br>攻撃対象領域の削減ルールを設定する：各 ASR ルールの状態を設定する | 無効<br>（注） ASR ルールが設定されていません。 | ブロック |
| 管理用テンプレート（コンピュータ）<br>ユーザとアプリが危険な Web サイトにアクセスするのを防ぐ | 無効<br>重要 ユーザとアプリケーションは、危険なドメインへの接続をブロックされていません。 | 有効：ブロック |
| 管理用テンプレート（コンピュータ）：<br>Windows Ink Workspace での推奨アプリケーションを許可する | 有効<br>（注） Windows Ink Workspace での推奨されるアプリケーションが許可されます。 | 無効 |

| 設定名 | デフォルト値（Default Value） | コンプライアンス |
|---|---|---|
| 管理用テンプレート（コンピュータ）：<br>Windows Ink Workspace を許可する | 有効<br>（注） Windows Ink Workspace は、ロック画面の上で使用できます。 | 有効<br>（注） 上記のロックへのアクセスは無効になっています。 |
| 管理用テンプレート（コンピュータ）：<br>WinRM によるリモートサーバ管理を許可する | 無効<br>（注） WinRM サービスは、WinRM の質問者設定に関係なく、リモートコンピュータからの要求に応答します。 | 無効 |
| 管理用テンプレート（コンピュータ）：<br>プレビュービルドを管理する | 無効<br>（注） **[設定（Settings）] > [更新とセキュリティ（Update and Security)]** で設定するまで、プレビュービルドはデバイスにインストールされません。 | 有効<br>（注） プレビュービルドは無効になっています。 |
| 管理用テンプレート（コンピュータ）：<br>プレビュービルドと機能の更新が受信したときに選択する | 無効<br>（注） Microsoft からリリースされた場合、機能の更新は遅延しません。 | 有効化 - 半期チャネル（180 日以上）<br>： |
| 詳細な監査ポリシー設定<br>ディレクトリ サービスアクセスを監査する | 成功 | 成功と失敗 |
| 管理テンプレート（ユーザ）<br>ヘルプエクスペリエンス改善プログラムをオフにする | 無効 | 有効 |

Windows セキュリティの強化

| 設定名 | デフォルト値（Default Value） | コンプライアンス |
|---|---|---|
| 管理テンプレート（ユーザ）<br>ユーザによるプロファイル内のファイル共有を防止する | 無効 | 有効 |
| ローカルポリシー - アカウント：<br>Microsoft アカウントのブロック | Windows で Microsoft のアカウントを使用できます。 | Microsoft アカウントを使用して追加またはログインすることはできません。 |
| ローカルポリシー<br>ネットワークアクセス：ネットワーク認証用のパスワードと資格情報の保管を許可しない | 無効 | 有効 |
| ローカルポリシー<br>ネットワークアクセス：匿名でアクセスできる共有 | なし | ブランク |
| ローカルポリシー<br>ネットワークセキュリティ：Kerberos に許可される暗号化タイプを設定する | • RC4_HMAC_MD5<br>• AES128_HMAC_SHA1<br>• AES256_HMAC_SHA1<br>• 今後の暗号化タイプ<br>参考資料：1 | • AES128_HMAC_SHA1<br>• AES256_HMAC_SHA1<br>• 今後の暗号化タイプ |
| ローカルポリシー<br>ユーザアカウント制御：組み込み管理者アカウントの管理者承認モード | 無効 | 有効 |

| 設定名 | デフォルト値（Default Value） | コンプライアンス |
|---|---|---|
| ローカルポリシー<br>ユーザアカウント制御：標準ユーザに対する昇格プロンプトの動作 | クレデンシャル用のプロンプト。<br>（注） 機能により高いレベルの特権への昇格が必要な場合は、管理者の資格情報の入力を求めるプロンプトが表示されます。資格情報が有効な場合、より高いレベルの権限が許可されます。 | システムは、より高いレベルの特権への昇格を自動的に拒否します。 |
| ローカルポリシー<br>ユーザアカウント制御：アプリケーションのインストールを検出し、昇格をプロンプトする | 無効 | 有効 |
| ローカルポリシー<br>ユーザアカウント制御：安全な場所にインストールされている UI アクセスアプリケーションのみを利用できます。 | 有効 | 有効 |
| ローカルポリシー<br>ユーザアカウント制御：ユーザごとの場所に対するファイルおよびレジストリの書き込み失敗を仮想化する | イネーブル<br>（注） システムは、ファイルシステムとレジストリの両方について、実行時にアプリケーションの書き込み失敗を定義されたユーザの場所にリダイレクトします。 | 有効 |

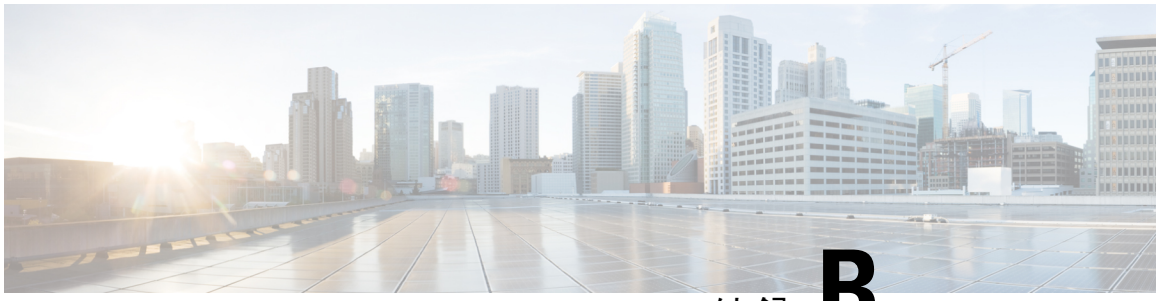
### Windows の強化に関するその他の検討事項

次の表に、対応するデフォルト値と使用可能な値を含む IIS 設定を示します。

Windows セキュリティの強化

| 設定名 | デフォルト値（**Default Value**） | サポートされる値 |
|---|---|---|
| ASP.NET アプリケーション カスタム エラー | リモートのみ | • **オン**：リモートシステムとローカルホストの両方にカスタムエラーが表示されます。<br>• **Off**：リモートシステムとローカルホストの両方に ASP.NET エラーが表示されます。<br>• **リモートのみ**：リモートシステムにカスタムエラーが表示され、ローカルホストに ASP.NET エラーが表示されます。<br>（注） これらのオプションは、システムの機能に影響を与えずに使用できます。 |
| HTTPOnlyCookie | 消灯 | 消灯 |
| AllowUnlisted | 正しい | 正しい |
| requestFiltering<br>許可される属性の値として *false* を使用してブロックされたファイル拡張子。 | .asax, .ascx, .master, .skin, .browser, .sitemap, .config, .cs, .csproj, .vb, .vbproj, .webinfo, .licx, .resx, .resources, .mdb, .vjsproj, .java, .jsl, .ldb, .dsdgm, .ssdgm, .lsad, .ssmap, .cd, .dsprototype, .lsaprototype, .sdm, .sdmDocument, .mdf, .ldf, .ad, .dd, .ldd, .sd, .adprototype, .lddprototype, .exclude, .refresh, .compiled, .msgx, .vsdisco, .rules | .asax, .ascx, .master, .skin, .browser, .sitemap, .config, .cs, .csproj, .vb, .vbproj, .webinfo, .licx, .resx, .resources, .mdb, .vjsproj, .java, .jsl, .ldb, .dsdgm, .ssdgm, .lsad, .ssmap, .cd, .dsprototype, .lsaprototype, .sdm, .sdmDocument, .mdf, .ldf, .ad, .dd, .ldd, .sd, .adprototype, .lddprototype, .exclude, .refresh, .compiled, .msgx, .vsdisco, .rules<br>.com, .doc, .docx, .docm, .jar, .hta, .vbs, .pdf, .sfx, .bat, .dll, .tmp, .py, .msi, .msp, .gadget, .cmd, .vbe, .jse, .ps1, .ps1xml, .ps2, .ps2xml, .psc1, .psc2, .lnk, .inf, .scf, .ws, .wsf, .scr, .pif |

（注） .exe、.htm および .dll などの特定の内線は、IIS でフィルタリングできません。



付録 B

# CCE Orchestration Windows OpenSSH の強化



## CCE Orchestration Windows OpenSSH の強化

Cloud Connect サーバが、オーケストレーション用の Windows ノード（ICM および CVP）へのパスワードレス セキュア シェル（SSH）接続を確立します。このセクションでは、CCE オーケストレーションの OpenSSH 強化について説明します。

Windows ノードの*%programdata%\ssh\sshd_config* にある OpenSSH サービス のデーモン設定ファイルで次の設定を変更し、OpenSSH サービスを再起動する必要があります。OpenSSH サービスの詳細については、『CCE のインストールとアップグレードガイド』の「オーケストレーション」のセクションを参照してください。

| 設定 | コンプライアンス設定 | 説明 |
|---|---|---|
| SSH 接続の制限 | `AllowUsers localuser@CloudConnectIP` | sshd_config の AllowUsers は、クラウド接続サーバホストだけが SSH 経由で Windows ユーザに接続できるようにします。<br>（注） 設定 `localuser@CloudConnectIP` とは、Cloud Connect IP で指定されているリモートクラウド接続ノードが、SSH 経由でローカルの Windows アカウントユーザに接続を許可することを意味します。クラウド接続のパブリッシャとサブスクライバの両方に、この設定のエントリが必要です。 |

| 設定 | コンプライアンス設定 | 説明 |
|---|---|---|
| DNS ホスト名チェックの有効化 | `UseDNS はい` | このフラグを [はい（Yes）] に設定すると、サーバは DNS サーバに対して接続されているクライアント（クラウド接続サーバ）のホスト名または IP アドレスの組み合わせを検証します。 |
| 認証試行の最大回数を設定する | `MaxAuthTries 3` | 推奨される MaxAuthTries は 3 です。 |
| 暗号化方式 | `HostKey _PROGRAMDATA __/ssh/ssh_host_rsa_key #HostKey __PROGRAMDATA __/ssh/ssh_host_dsa_key #HostKey __PROGRAMDATA __/ssh/ssh_host_ecdsa_key #HostKey __PROGRAMDATA __/ssh/ssh_host_ed25519_key #HostKey` | デフォルトでは、RSA がデフォルトの暗号として使用され、クラウド接続サーバと Windows ノード間で SSH 接続が確立されます。<br>顧客は ECDSA などの暗号を選択できます。ECDSA のコメントを解除し、RSA をコメントアウトします。<br>（注） 暗号タイプを変更した後、ユーザは、この特定の Windows ノードに対して、パブリッシャとサブスクライバの両方から、Cloud Connect CLI でコマンド `utils deployment test-connection` を実行し、新しい暗号がセキュリティハンドシェイクに使用されるのを確認する必要があります。CLI の詳細については、『CCE のインストールとアップグレードガイド』を参照してください。 |

# OpenSSH sshd_config へのアクセスの制限

当初、Windows ノードの Orchestration 用の Cloud Connect へのオンボードに使用される CVP または ICM の必須 ES のインストールを通じて、OpenSSH のインストール中に `sshd_config` に対して適切なユーザベースの権限が設定されています。

プラットフォームのオーケストレーション管理者ユーザが管理者によって変更された場合は、その権限を設定して、新しいユーザの `OpenSSH sshd_config` へのアクセス権を制限する必要があります。`OpenSSH sshd_config` へのアクセス権を制限するには、次の手順を実行します。

### 手順

**ステップ 1** 新しいプラットフォームのオーケストレーション管理者ユーザを使用して Windows ノード（CVP または ICM）にログインします。

**ステップ 2** 管理者モードで PowerShell を起動します。

**ステップ 3** OpenSSH のデフォルトのインストールディレクトリに移動します（ICM の場合は `C:\icm\install\OpenSSH-Win64` など）。

**ステップ 4** コマンド `Repair-SshdConfigPermission -FilePath C:\ProgramData\ssh\sshd_config` を実行します。

**ステップ 5** **Enter** キーを押して、継承およびアクセス制限に関するクエリのデフォルトオプション「Y」を選択します。
上記のコマンドが正常に実行されると、*%programdata%\ssh\sshd_config* が制限付きアクセスで設定されます。

**ステップ 6** OpenSSH サービスを再起動します。OpenSSH サービスの詳細については、『CCE のインストールとアップグレードガイド』の「オーケストレーション」のセクションを参照してください。

**ステップ 7** この特定の Windows ノードに対して、パブリッシャとサブスクライバの両方から、Cloud Connect CLI でコマンド **utils deployment test-connection** を実行します。これは、Cloud Connect サーバが、オーケストレーションの Windows ノード（ICM および CVP）に対してパスワードレスのセキュアシェル（SSH）接続を確立できる状態を確保できるようにするために行ないます。

CCE Orchestration Windows OpenSSH の強化