IPCC のセキュリティ管理

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

セキュリティの概要

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

シスコは、企業のお客様による効率性、安全性、信頼性、および拡張可能性を持つネットワークの構築を支援するために、シスコのさまざまなネットワーキング ソリューションに関する詳細な設計および実装ガイダンスを取り上げた、一連のドキュメントを開発しました。http://www.cisco.com/go/srnd から入手できるこれらの『*Solution Reference Network Design（SRND）*』では、Cisco Architecture for Voice, Video, and Integrated Data（AVVID）に基づいたネットワーク インフラストラクチャを構築するための、検証済みのベスト プラクティスを提供します。これらのガイドには、IPCC ネットワークの展開を成功させるために使用する必要がある、セキュリティおよび IP テレフォニーに関する次の関連ドキュメントが含まれます。更新および追加は随時行われますので、サイトへは定期的にアクセスして最新版を確認してください。

- 『*IP Telephony SRND for Cisco CallManager 3.3*』
- 『*IP Telephony SRND for Cisco CallManager 4.0*』
- 『*Data Center Networking: Securing Server Farms SRND*』
- 『*Data Center Networking: Integrating Security, Load Balancing, and SSL Services*』

セキュリティで適切に保護された IPCC 設定には、対象となる攻撃およびウイルスの伝搬からシステムを保護するために、多層にわたる対策が必要です。第一の対策は、シスコのコンタクト センター アプリケーションをホスティングしているサーバのセキュリティが物理的に保護されていることの確認です。これらのサーバは、承認された担当者だけがアクセスを許可されたデータ センター内に配置される必要があります。次のレベルの保護は、最新のウイルス定義ファイルが使用されたウイルス対策アプリケーションをサーバが実行し、Microsoft および他のサードパーティのセキュリティ パッチを使用して、サーバが常に最新の状態に保たれていることを確認することです。お客様のアプリケーションのリリースに適用可能な、セキュリティのベスト プラクティス ガイド内に提供されたガイドラインに従って、サーバを強化できます。

別のレベルのセキュリティとしては、サーバのネットワークのセグメント化が挙げられます。IPCC サーバは、システムのインターネットへの公開や攻撃に対して堅固に防御されたホストの展開を前提とした設計はなされていません（唯一の例外は Web コラボレーション オプションです）。CTI OS、Cisco Agent Desktop、または Cisco Supervisor Desktop などのデスクトップベース アプリケーションが、オープンな企業 Virtual LAN（VLAN; 仮想 LAN）内で展開される傾向にありますが、IPCC ソリューションを構成しているサーバはセキュリティで保護されたネットワークの背後にあるデータ センター内に配置する必要があります。サーバが地理的に分散されている場合、セキュリティによってネットワーク リンクを確実に保護するための適切な配慮が必要です。

セキュリティのベスト プラクティス

デフォルト（標準）の Windows 2000 Server オペレーティング システムのインストール

IPCC ソリューションは、管理手順の異なる多数のサーバ アプリケーションによって構成されています。次のサーバのためのセキュリティのベスト プラクティスは、IPCC ソリューション内のその他のアプリケーションとわずかに異なります。

- ICM Router
- ICM Logger
- ICM ペリフェラル ゲートウェイ
- ICM アドミン ワークステーション（Historical Data Server および WebView）
- CTI ベース サーバ（CTI、CTI OS、および Cisco Agent Desktop サーバ）

これらのサーバのためのセキュリティのベスト プラクティスは、Microsoft Windows 2000 Server 環境のためのセキュリティ強化設定ガイドラインが説明されたドキュメント内に統合されています。このドキュメント（『*Security Best Practices for Cisco Intelligent Contact Management Software*』）は、次の URL から入手できます。

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

『*Security Best Practices*』ガイド内に含まれた推奨事項は、他のサードパーティ ベンダーによる強化のための推奨事項だけではなく、『*Windows 2000 Security Hardening Guide*』内の推奨事項など、Microsoft によって発行された強化ガイドラインに部分的に基づいています。『*Security Best Practices*』の目的は、特にコンタクト センター サーバ製品に適用される際にこれらのガイドラインをより詳細に解釈し、カスタマイズすることです。例外または特定の推奨事項が発生する場合、『*Security Best Practices*』では、その違いをできる限り原理的に説明するように努めています。

『*Security Best Practices*』では、その対象読者を Windows 2000 Server のセキュリティによる保護に精通している、経験豊富なネットワーク管理者であると想定しています。さらに、ICM および IPCC ソリューションを構成するアプリケーションだけではなく、これらのシステムのインストールおよび管理にもその対象読者が完全に精通していると想定しています。これらのベスト プラクティスの別の目的は、Cisco IP Contact Center アプリケーションが依存しているさまざまなサードパーティ アプリケーションとオペレーティング システムに対して、セキュリティという視点から統合された解釈を与える点にあります。

シスコが提供する Windows 2000 Server のインストール（CIPT OS）

IP IVR、Internet Service Node（ISN）、および Cisco CallManager サーバではすべて、Cisco IP Telephony Operating System と呼ばれる、強化されたオペレーティング システムがサポートされています。このオペレーティング システムの強化のための仕様は、『*Cisco IP Telephony Solution Reference Network Design (SRND)*』内で参照できます。このガイドは次のリンクから入手できます。

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

パッチ管理

デフォルト（標準）の Windows 2000 Server オペレーティング システムのインストール

セキュリティ パッチ

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

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

Microsoft から重大または重要なセキュリティ アップデートがリリースされると、シスコは ICM ベース アプリケーションに対する影響を判断し、通常は 24 時間以内にこの判断を含む Field Notice をリリースします。影響があると区分されたセキュリティ アップデートに対しては、シスコは自社の製品に対するテストを続け、最初の Field Notice 後に潜在的な競合が発生するかどうかをより詳細に判断します。Field Notice のアップデートは、これらのテストの完了時にリリースされます。

お客様は次のリンクにアクセスして、セキュリティ アップデートを通知する Field Notice のアラートを受信するプロファイルを設定できます。

http://www.cisco.com/cgi-bin/Support/FieldNoticeTool/field-notice

これらのアップデートをいつどのように適用するのかについては、お客様は Microsoft のガイドラインに従う必要があります。

Microsoft からリリースされたすべてのセキュリティ パッチをコンタクト センターのお客様が個別に判断し、お客様の環境に適切であると判断されたパッチをインストールすることが推奨されます。より深刻な重大度を持つセキュリティ パッチを個別に判断するサービス、また必要に応じて、これらのセキュリティ パッチを検証するサービスの提供をシスコは継続します。コンタクト センターのソフトウェア製品には、より深刻な重大度を持つセキュリティ パッチが適切な場合があります。

自動パッチ管理

ICM ベース サーバでは、Microsoft の Software Update Services（SUS）との統合がサポートされます。これにより、お客様はこれらのサーバにどのパッチをいつ展開できるのかをコントロールします。Windows Update の自動更新をサーバに設定できますが、ローカルの Software Update Services（SUS）または Windows Update Services（WUS）サーバを参照することが推奨されます。

シスコが提供する Windows 2000 Server のインストール（CIPT OS）

セキュリティ パッチ

『*Cisco CallManager Security Patch Process*』は、次のリンクから入手できます。

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

シスコがサポートするオペレーティング システム ファイル、SQL Server、およびセキュリティ ファイルの追跡情報を提供するドキュメントは、次のリンクから入手できます。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/osbios.htm

このドキュメントでは、ソフトウェア アップデート（Cisco CallManager、IP IVR、および ISN に限定）の適用に関するシスコの推奨事項も提供します。

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

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

http://www.cisco.com/warp/public/779/largeent/software_patch.html

自動パッチ管理

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

ウイルス対策

サポートされるアプリケーション

IPCC システムでは、多くのサードパーティのウイルス対策アプリケーションがサポートされます。特定の IPCC ソフトウェア リリース上でサポートされるアプリケーションおよびバージョンの一覧については、『*Cisco Intelligent Contact Management (ICM) Bill of Materials*』および Cisco CallManager 製品のマニュアル（http://www.cisco.com にて入手可）内に掲載されている、ICM プラットフォーム ハードウェア仕様および関連するソフトウェア互換性データを参照してください。

（注）　お客様の環境でサポートするアプリケーションだけを展開します。特に、IPCC システムに Cisco Security Agent などのアプリケーションがインストールされている場合、サポートしないアプリケーションを展開すると、ソフトウェアの競合が発生する場合があります。（「Cisco Security Agent」（P.9-8）を参照してください）。

設定ガイドライン

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

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

次のリストでは、一般的なベスト プラクティスの一部を取り上げます。

- サードパーティ ウイルス対策アプリケーションの最新サポート バージョンへアップグレードします。以前のバージョンと比較して、より新しいバージョンではスキャン速度が改善され、サーバでのオーバーヘッドはより小さくなります。
- リモート ドライブ（ネットワーク マッピングまたは UNC 接続など）からアクセスされているファイルに対するスキャンを回避します。可能な場合、これらの各リモート マシンにはそれぞれ独自のウイルス対策ソフトウェアをインストールして常にローカルでスキャンを実行するようにします。多層なウイルス対策戦略において、ネットワーク全体でのスキャンおよびネットワーク ロードへの追加は必須ではありません。
- 従来のウイルス対策スキャンと比較してヒューリスティックス　スキャンではより大きなスキャン オーバーヘッドが発生するため、信頼性の保証のないネットワーク（電子メールおよびインターネット ゲートウェイなど）からのデータ入力における重要な状況でだけ、この先進のスキャン オプションを使用します。
- リアルタイムまたはアクセス時のスキャンを有効にすることは可能ですが、その対象を着信ファイルだけにします（ディスクへの書き込み時）。これは、ほとんどのウイルス対策アプリケーションにとってのデフォルト設定です。ファイルの読み出しへのアクセス時のスキャンの実装は、高パフォーマンス アプリケーション環境において、システム リソースに対して必要以上に大きな影響を与えます。

- すべてのファイルに対する手動およびリアルタイム スキャンでは、最適な保護が提供される一方、この設定では、悪意あるコード（たとえば、ASCII テキスト ファイル）のサポートが不可能なファイルに対するスキャンによるオーバーヘッドが発生します。すべてのスキャン モードにおいて、システムを危険にさらすことがないと認識されているファイルまたはファイルのディレクトリを除外することが推奨されます。次のリンクから入手できる『*Security Best Practices for Cisco Intelligent Contact Management Software*』内で説明するように、ICM または IPCC 実装において特定の ICM ファイルを除外するための推奨事項にも従います。

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

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

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

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

Cisco Security Agent

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

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

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

スタンドアロン エージェントおよび管理エージェントのサポート

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

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

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

- Cisco ICM、IPCC Enterprise、および ISN（Customer Voice Portal（CVP）としても知られる）のエージェントは、次のリンクから入手できます。

  http://www.cisco.com/kobayashi/sw-center/contact_center/csa/
- 他のエージェントは、次のリンクから入手できます。

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

サードパーティ アプリケーションの依存関係

Cisco Security Agent は、『*Cisco Intelligent Contact Management (ICM) Bill of Materials*』またはインストールしている Cisco Security Agent のインストール ガイド内に掲載されている、サポートされているアプリケーションと同じサーバ上にだけ配置できます。

Cisco ICM エージェントのインストールの詳細については、次のリンクから入手できる『*Installing Cisco Security Agent for Cisco Intelligent Contact Management Software*』を参照してください。

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

ファイアウォールと IPSec

ファイアウォール

ファイアウォールが配置されている環境でのアプリケーションの展開では、ネットワーク管理者がどの TCP/UDP IP ポートが使用されているのかを認識する必要があります。最も広範に展開されているシスコ製品のバージョンのための、一連のコンタクト センター アプリケーション全体で使用されているすべてのポートのインベントリについては、次のリンクから入手できる『*Cisco Contact Center Product Port Utilization Guides*』を参照してください。

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

（注）　アウトバウンド オプション ダイヤラおよび Cisco CallManager サーバには、PIX ファイアウォールを介したセグメント化を実行しません。詳細は、http://www.cisco.com/en/US/products/sw/secursw/ps2120/prod_release_notes_list.html で入手できる『*Release Notes for the Cisco Secure PIX Firewall*』を参照してください。

IPSec および NAT

トンネル モードでの IP セキュリティ（IPSec）のサポート

データおよび音声を問わず、ネットワークの展開において増大するセキュリティ上の懸念を理由に、現在の ICM および IPCC Enterprise の展開では、コール制御サーバおよびエージェント デスクトップ間だけではなく、セントラル コントローラ サイトおよびリモート Peripheral Gateway（PG; ペリフェラル ゲートウェイ）サイト間での IPSec サポートが追加されます。このセキュリティで保護されたネットワーク実装は、IPSec トンネルを介してセキュリティが保護された WAN 接続を含む分散モデルを意味します。このリリースにおいて実施されたテストは、トンネル モードでの Cisco IOS IPSec の設定に限定されています。つまり、2 つのサイト間の Cisco IP Router（IPSec ピア）だけが、セキュリティで保護されたチャネルの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 リンク全体で暗号化されていますが、ローカル エリア ネットワークでは暗号化されていません。トンネル モードでは、IPSec ピア間においてトラフィック フローの機密保持が保証されます。この場合、IPSec ピアはセントラル サイトをリモート サイトに接続する IOS Router です。

IPSec 設定のための認定された仕様は次のとおりです。

- HMAC-SHA1 認証（ESP-SHA-HMAC）
- 3DES 暗号化（ESP-3DES）

IP ルータの CPU オーバーヘッドおよびスループットによる影響の深刻な増大を回避するためには、ハードウェアの暗号化を使用することが推奨されます。遅延に対する影響も発生します。したがって、ネットワーク インフラストラクチャ（ネットワーク ハードウェアおよび物理リンク）の大きさを適切に調節することが重要です。QoS ネットワークに対して考慮する必要がある検討事項もあります。一般的な推奨事項は、トラフィックがトンネル カプセル化および暗号化（またはどちらか一方）される前に、パケット ヘッダー情報を基に QoS 機能を分類し、適用することです。

Cisco IOS IPSec の機能についての詳細は、次のリンクから入手できます。

http://www.cisco.com/en/US/tech/tk583/tk372/tech_protocol_family_home.html

Network Address Translation（NAT）のサポート

IPCC Release 6.0(0) では、エージェント デスクトップおよび IP 電話（IPCC）の NAT 全体への展開に対するサポートを正式に追加しています。シスコは、セントラル コントローラ サーバ（Router および Logger）から NAT ネットワーク リモート上へのリモート PG サーバの配置もテストしました。エージェント デスクトップおよび PG サーバのための NAT サポート機能の適用は、NAT 機能を持つ Cisco IP ルータを実装しているネットワーク インフラストラクチャに限定されています。

Cisco IOS NAT は、大規模なネットワークにおいて登録済み IP アドレスを保護し、IP アドレスの管理タスクを簡素化するするためのメカニズムです。その名称が示すとおり、Cisco IOS NAT では、プライベートな「内部」ネットワーク内の IP アドレスを、公共な「外部」ネットワーク（インターネットなど）を介した転送のために、「法的な」IP アドレスに変換します。着信トラフィックは、内部ネットワーク内での送信のために変換し直されます。

NAT の設定方法についての詳細なリソースは、次のリンクから入手できます。

http://cisco.com/en/US/partner/tech/tk648/tk361/tk438/tech_protocol_home.html

IPCC 展開のための NAT 全体における IP 電話の展開方法についての詳細は、次のリンクから入手できます。

http://cisco.com/en/US/partner/products/sw/iosswrel/ps1834/products_feature_guide09186a008008052e.html

（注）　IPSec NAT トランスペアレンシ機能では、NAT および IPSec 間の既知の非互換性の処理により、ネットワーク内の NAT または Port Address Translation（PAT）ポイントを介した IPSec トラフィックの移動のためのサポートが導入されます。NAT トラバーサル機能は、VPN デバイスによって自動検出される機能です。Cisco IOS Software Release 12.2(13)T 以降を実行しているルータでは、設定する手順はありません。両方の VPN デバイスが NAT-T 対応の場合、NAT トラバーサル機能は自動検出され、オートネゴシエーションされます。

Cisco CallManager Release 4.0 におけるセキュリティ機能

デバイス認証

Cisco CallManager Release 4.0 を基にして IPCC ソリューションを設計する場合、IPCC では Cisco 7940 IP Phone および Cisco 7960 IP Phone のためのデバイス認証がサポートされないことへの注意が重要です。Cisco CallManager におけるパフォーマンス上の影響により、対象となる環境での徹底的なパフォーマンス テストを実施しない限り、現在はこの機能を有効にしないことが推奨されます。

メディア暗号化

現在、メディア暗号化は Cisco 7970 IP Phone においてだけサポートされています。この Cisco 7970 IP Phone は、IPCC 環境ではサポートされていません。シスコのアクセス権を持つ IPCC ソリューションの一部として Cisco 7970 IP Phone が展開されている場合、このモデルの IP 電話を備えたエージェントは、サイレント モニタ機能や録音機能などの機能を使用できません。

電話の設定

Cisco CallManager における Cisco IP Phone デバイスの設定では、音声 VLAN への PC のアクセス制限だけではなく、電話の PC ポートを無効にする機能が提供されます。PC アクセスを無効にするこれらのデフォルト設定の変更は、IPCC ソリューションのモニタ機能も無効にします。設定は次のように定義されます。

- PC ポート
  - 電話上の PC ポートが有効なのか無効なのかを示します。電話の背面にある「10/100 PC」とラベルが付けられたポートによって、PC またはワークステーションが電話に接続され、単一のネットワーク接続の共有が可能になります。
  - これは必須のフィールドです。
  - デフォルトは有効です。
- PC 音声 VLAN アクセス
  - PC ポートに接続されたデバイスによる音声 VLAN へのアクセスを許可するかどうかを示します。音声 VLAN アクセスを無効にすると、接続された PC による音声 VLAN 上でのデータの送受信が回避されます。また、電話によって送受信されるデータの PC による受信も回避されます。電話のトラフィックに対するモニタリングが必要な PC 上でアプリケーションが実行されている場合、この設定を有効にします。これには、分析を目的としたモニタリングと録音アプリケーションおよびネットワーク モニタリング ソフトウェアが含まれます。
  - これは必須のフィールドです。
  - デフォルトは有効です。