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

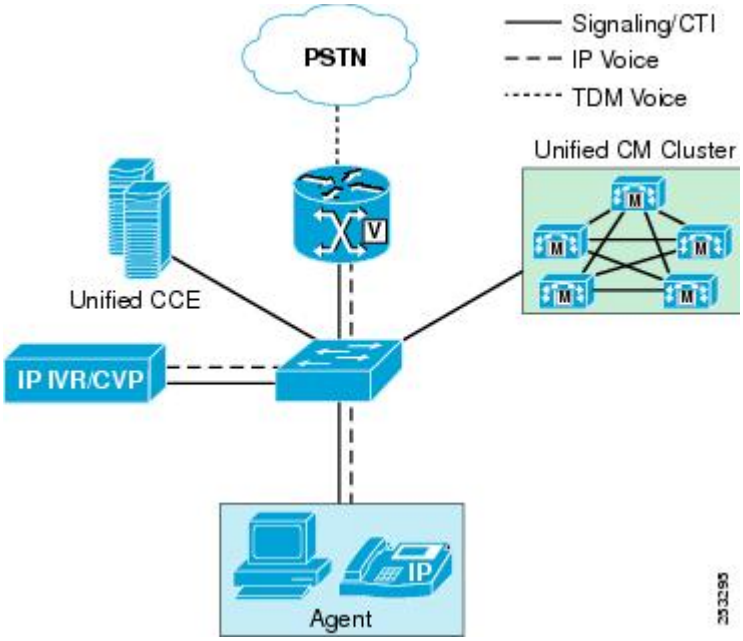
モニタリングは、製品アーキテクチャのすべての重要なコンポーネントをカバーする必要がある業務を効果的に管理する上で重要な役割を果たします。モニタリングは、セキュリティ上の問題を検出し、その重大度に基づいて分析と緩和を可能な限り早く行うのに役立ちます。

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。

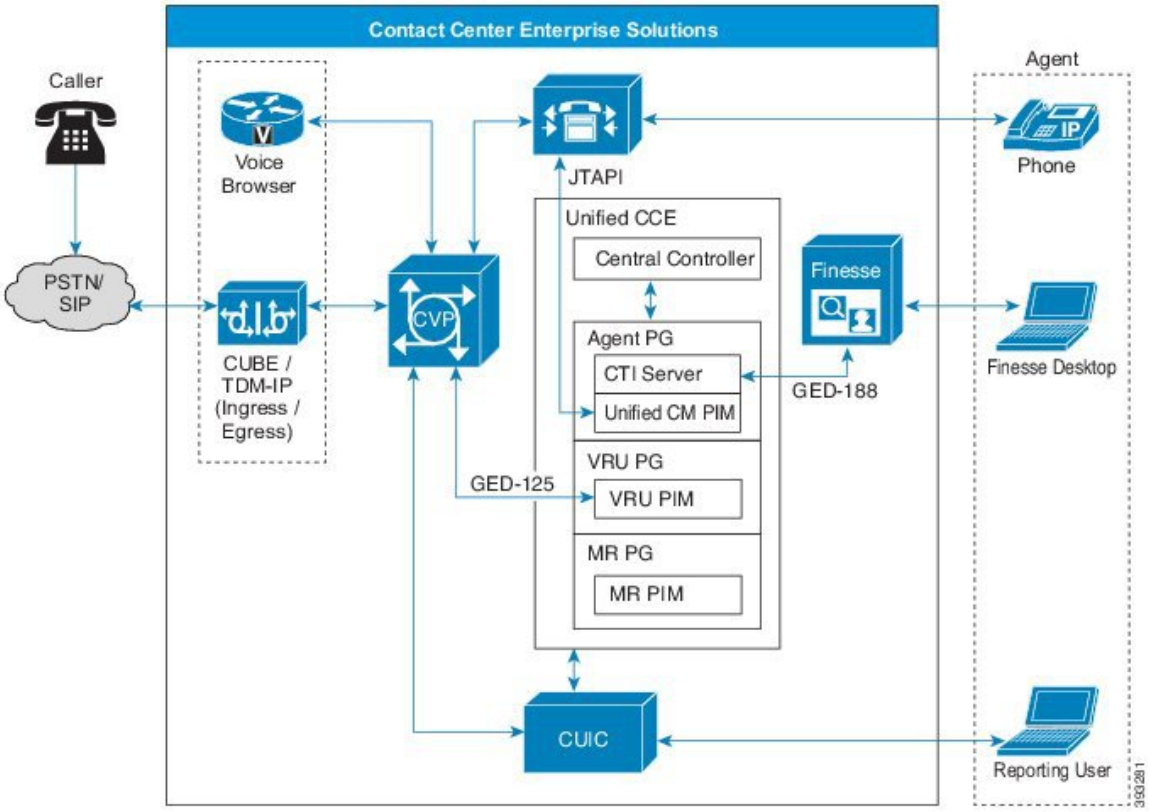
Cisco Prime Assurance

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

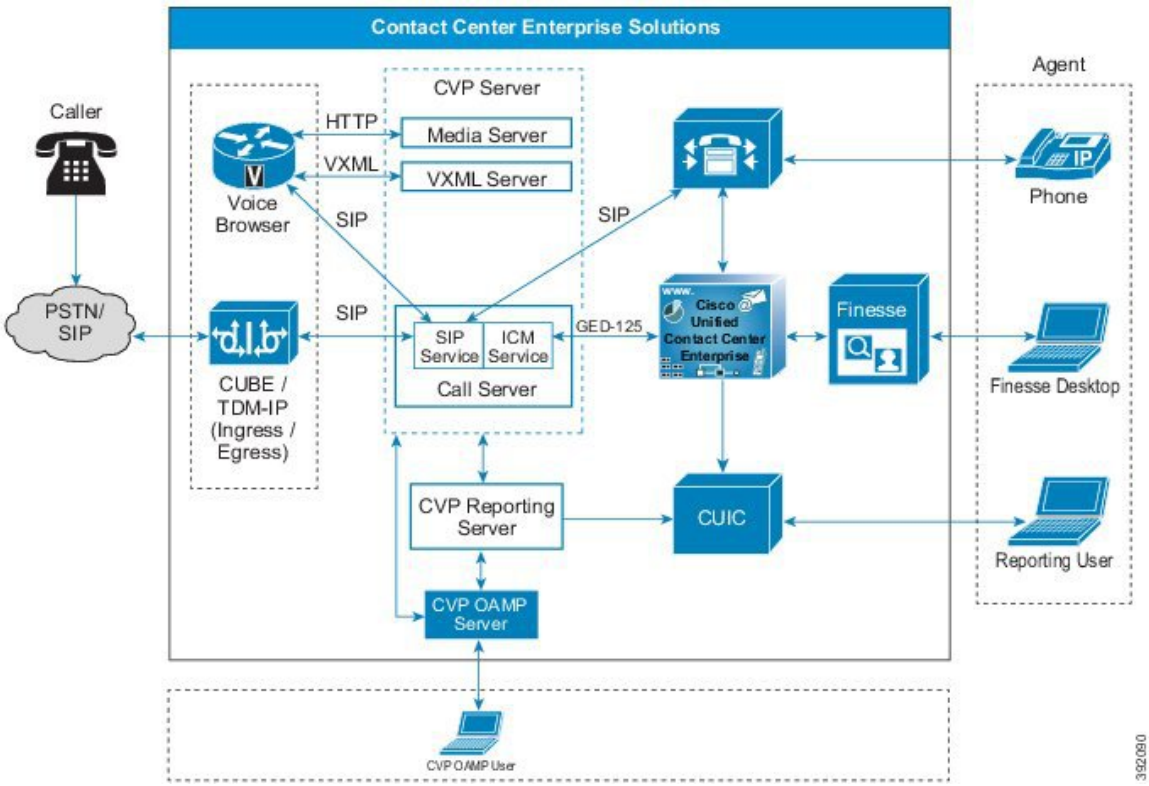
TDoS 攻撃は一般に、データネットワークのサービス妨害（DoS）と同じモデルに従います。不正なユーザがシステムにフラッディングしすぎてアクセス要求が多くなると、権限を持つユーザがシステムにアクセスできなくなります。Unified CCE には、輻輳制御機能が搭載されています。輻輳制御を使用すると、着信コールのコール/秒（CPS）パターンをモニタし、コンタクトセンターにアラートしてTDoS 攻撃から保護できます。

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）