Cisco Desk Phone 9800 シリーズのセキュリティ

セキュリティ技術文書

2024 年 6 月

webex by CISCO

コンテンツ

PhoneOS を実行している Cisco Desk Phone 9800 シリーズは、最新のセキュリティ機能を提供します。 このテクニカル ペーパーでは、デスク フォン 9800 シリーズの重要なセキュリティ機能について説明します。

この技術文書ドキュメントでは、Cisco がデスクフォン 9800 シリーズに加えたセキュリティの改善について説明します。 デスク フォン 9800 シリーズおよび Cisco Video Phone 8875 は PhoneOS を実行します。 このオペレーティング システムは、工場出荷時設定にリセットするだけで、Unified Communications Manager (Unified CM) または Webex Calling などの指定されたクラウド通話プラットフォームのいずれかに登録できます。 エンタープライズ ファームウェアを実行している 7800 および 8800 シリーズとは異なり、PhoneOS では環境間を移動するときにファームウェアを移行する必要がなくなりました。 さらに、ハードウェア セキュリティの強化である Trusted Platform Module (TPM) がデスク フォン 9800 シリーズに追加され、9800 シリーズは、TPM 2.0 ハードウェア モジュールを含む業界初のデスク フォンとなりました。

1. 最高のエンドツー エンド セキュリティ

Cisco Desk Phone 9800 シリーズのセキュリティ フレームワークは、最新のセキュリティ機能を提供します。
図 1 に示すように、次のセキュリティの柱は PhoneOS ファームウェアとデスクフォン 9800 シリーズハードウェアの重要なセキュリティ機能を含みます。

- ハードウェアにより有効化されるセキュリティ
  - Trusted Platform Module (TPM)
  - ハードウェアによる強制音声パスコントロール（ハードウェアによるミュート）
  - ハードウェアの信頼性チェック
  - チップ保護（チップガード）
  - イメージ署名

    - セキュア ブート
- 実行時保護
    - ランタイム防御
    - セキュリティ強化 Linux
- アプリケーションのセキュリティ
    - セキュアなインフラストラクチャ: PKI 証明書管理。
    - TLS 1.3
    - 休止中および使用中のユーザーデータを保護する
    - ユーザデータのエンドツーエンド暗号化
    - 安全なオンボーディング
    - セキュア コール
    - エンドユーザを保護するスパム対策サポート
    - Webex Calling における個人を特定できる情報（PII）のプライバシー
- 業界のコンプライアンス
    - セキュリティ コンプライアンス: FedRAMP* および FIPS。
- Cisco CSDL、PSIRT、製品セキュリティベースライン。

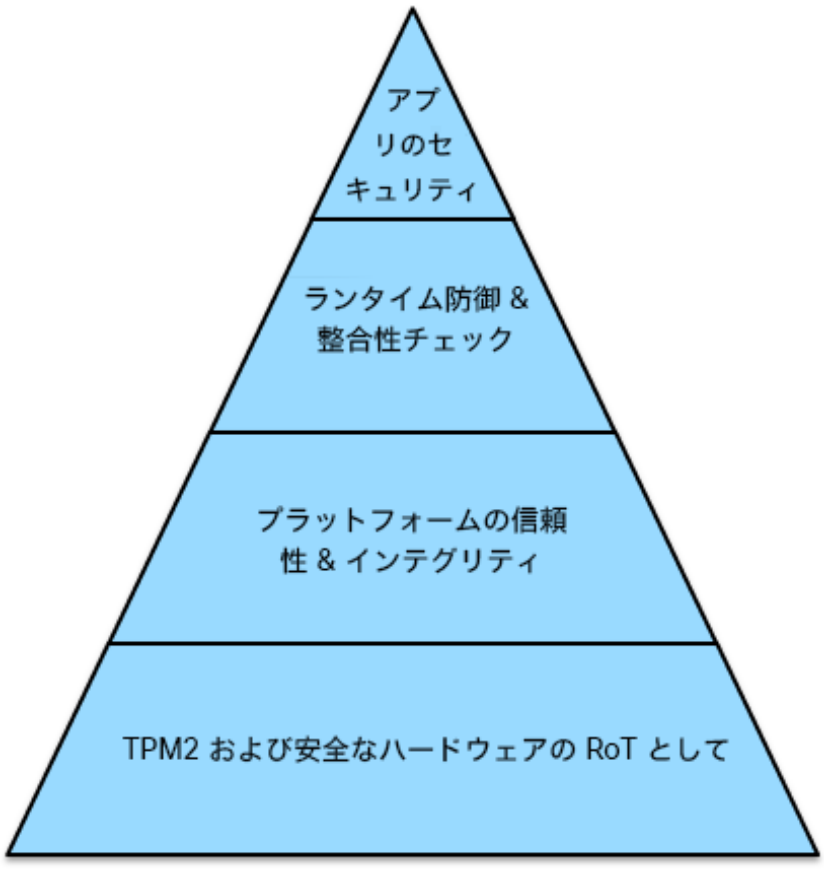

図 1. デスクフォン 9800 シリーズとの PhoneOS セキュリティアーキテクチャ

2. ハードウェア対応のセキュリティ

図 1 上記を見るとわかるように、Cisco は階層型のセキュリティアプローチを設計しています。 これらの各レイヤーは、ハードウェアとソフトウェアの両方で連携して機能し、システムの整合性を維持します。

TPM2 および セキュア SoC はハードウェアの信頼のルートを提供し、デスクフォン 9800 シリーズで PhoneOS の強固なセキュリティ基盤を構築し、デバイスのライフサイクル全体でセキュリティ脅威を回避します。

3. Trusted Platform Module 2.0

- 9800 ハードウェアに含まれる TPM 2.0 モジュールは、暗号などのセキュリティ関連機能を提供するために設計されたディスクリートハードウェアモジュールです。 このモジュールは業界標準 (TCG-TPM2.0) に準拠しています。
- TPM は以下のような脅威を軽減します。
    - ハードウェアの改ざん。 ハードウェアチップを交換し、PhoneOS のセキュアブートをバイパスする行為。
    - ハードウェアのなりすまし (ハードウェアの複製) 企業ネットワークまたはクラウド通話サービスにアクセスするために、電話の識別情報をスプーフィングする行為。
    - 偽造ハードウェア。 データ盗難のためのバックドアを作成するために、偽造ハードウェアを作成する行為。
    - データを危険にさらす。 機密性の高いユーザ データまたは資格情報の盗難。
    - セキュアでない通信。 弱い暗号を悪用してトラフィックを解読することによるデータの危険。
- ハードウェアの真正性チェック
    - TPM にインストールされた X.509 Secure Unique Device Identifier (SUDI) 証明書を使用して、Cisco ハードウェアが信頼できるものであることを確認するプロセス。 ハードウェアの真正性チェックは、セキュアブートプロセスが完了し、ソフトウェアが信頼できることが確認された後にのみ実行されます。
    - PhoneOS は、TPM から SUDI 証明書を取得し、証明書がプラットフォームに属するという暗号証明を提供します。
- チップ保護（チップガード）
    - マルウェアまたは同様のタイプの攻撃を含む CPU 交換のサプライチェーンの脅威を軽減します。 チップガードは、TPM 2.0 ハードウェアモジュールを使用してこの脅威を軽減します。
- 安全な通信
    - PhoneOS は、TPM ハードウェアによって保護される TLS 1.3*、SUDI 証明書、ユーザーがインストールした証明書（LSC）、および SIP OAuth をサポートします。

メモ: 8875 は PhoneOS を実行し、TPM 2.0 ハードウェア モジュールを含みません。

4. ハードウェアによる音声パス制御

ハードウェアによる音声パス制御は、ハードウェア ミュートとも呼ばれます。 Cisco 電話ハードウェアは、ハードウェア自体がマイクの状態を物理的にコントロールするように設計されています。 これは、マイクの電気回路がソフトウェアによって上書きできないハードウェアスイッチ (フックスイッチ) またはインジケータ (LED) に直接接続されていることを意味します。 詳しい動作は以下の通りです。

ハンドセット マイク カットオフ メカニズム：ハンドセットフックスイッチが押された状態（受話器がフックにかかっていることを示す）の場合、ハードウェアがマイク回路をハードウェアレベルで切断または無効にします。 ハンドセットが使用されていないときに、マイクをアクティブにするための回路を閉じるソフトウェアとの相互作用はなく、マイクがソフトウェア手段によってリモートでオンにされることはできません。

スピーカー LED ステータス インジケータ: スピーカー キーの LED は、マイクのステータスの信頼できるインジケータとして機能します。 LED が点灯している場合、ハンズフリー マイク回路がアクティブで、音声をキャプチャできることを示します。 逆に、LED がオフの場合、ハードウェアはマイクが非アクティブであることを保証します。 ソフトウェアは、ユーザーに視覚的な合図を提供して、LED を点灯させないと、マイクをアクティブにすることはできません。

これらのハードウェアコントロールにより、デバイスは、ハンドセットがフックにかかっている状態で内部マイクがアクティベートされ、スピーカー LED が点灯することを保証します。 この設計は、マイクがライブであることを示すハードウェア表示 (点灯した LED) をユーザに提供することで、ソフトウェアが侵害されてマイクを秘密裏にアクティベートすることを防ぎます。

これらの手段は、物理的な設計要素を活用して「ハードウェアのルートオブトラスト」を作成し、特定の重要な機能がハードウェアによって厳密にコントロールされ、侵害された可能性のあるソフトウェアの手の届かないところにあることを確実にします。 このアプローチは、会話のプライバシーとデバイスの音声入力メカニズムの整合性について、ユーザに強力なセキュリティ保証を提供します。

5. セキュアな一意のデバイス ID (SUDI)

製造時に、デバイス ID は、デバイスごとにグローバルに一意な X.509 証明書である、セキュアな一意のデバイス ID（SUDI）を使用して、Cisco Trust Anchor モジュール（TPM2 モジュールにより裏付けられた）にプログラムされます。 SUDI はデバイス アイデンティティの拡張機能であり、IEEE 802.1 ワーキング グループによって定義されています。 802.1 AR 標準では、セキュアなデバイス識別子を、デバイスにバインドされ、デバイス ID を表明するために使用される暗号学的なアイデンティティとして定義されています。 SUDI は、Trust Anchor モジュールに永久的にプログラムされ、Cisco によってログに記録され、デバイス認証の目的で使用されます。 Cisco は、シリコン、ソフトウェア、製造パートナーと安全な企業間ネットワークを持ち、サプライヤーと Cisco バックエンド プロセスの間で SUDI などの重要なシステム情報を交換しています。

SUDI により、各 Cisco デスク フォンデバイスは、製造からサポート終了までのライフサイクルを通じてデバイスを認証するために使用される一意で安全な識別子を持ちます。 TPM モジュールによって保護された SUDI は、偽造デバイスや不正アクセスに対する堅牢な防御を提供し、サプライチェーンと運用環境におけるデバイス全体のセキュリティを強化します。

6. セキュア ブートとハードウェアの信頼性チェック

セキュア ブートはシステム オン チップ (SOC) ハードウェアと緊密に統合されているため、起動時に Cisco Desk phone では検証済みで汚染されていないコードのみが実行できます。 ルート オブ トラストの確立により、セキュア ブートはブート プロセスのすべての段階を監視します。 起動時に、セキュア ブート プロセスがマイクロローダー、ブートローダーを認証し、ブートローダーがオペレーティング システムを認証します。 このプロセスにより、マイクロローダーからオペレーティングシステムまでの信頼のチェーンが作成され、ソフトウェアの信頼性と整合性が確立されます。 これらのすべての署名は、RSA 署名を使用して暗号的に検証されます。 デジタル署名の確認に失敗すると、Cisco デバイスはソフトウェアの起動を許可しません。

セキュアブートシーケンスが完了し、ソフトウェアが信頼できると見なされると、PhoneOS ソフトウェアは TPM からセキュア UDI（SUDI）証明書を取得し、チップに問い合わせて、SUDI 証明書が基盤となるプラットフォームに属していることを示す暗号化証明を提供します。 このチャレンジプロセスは、ハードウェアの信頼性チェックまたは偽造防止チェックと呼ばれます。 この機能により、PhoneOS ソフトウェアは、正規の Cisco 9800 電話ハードウェアで実行されているかどうかを判断できます。

この包括的な検証を通じて、ハードウェアとソフトウェアの両方の信頼性がブート時に保証され、ハードウェアとソフトウェアの偽造のリスクから保護されます。

7. チップ保護

サプライチェーン攻撃には、元のシステムオンチップ（SOC）コンポーネントを、トロイの木馬や悪質なコードを含む改ざんされたバージョンに置換することが含まれます。 Cisco チップ保護は、製品のライフサイクルを通じてコンポーネントを識別し、追跡する方法として、Trust Anchor モジュール (TPM2 モジュールによって支援) の内部に保存された一意の識別子を使用することで、この脅威を軽減します。

Trust Anchor モジュールは、インプリント データベースを収容します。これは、回路ボードに固有の SOC チップおよびその他のデバイス タイプの一意の識別子を記録する決定的なカタログです。 これらの識別子は通常、デバイスのシリアル番号または同様の一意の値です。 「信頼できる」値を含むインプリントデータベースは、それが存在するボード専用であり、コンポーネントの真正性を確認する認証プロセスの参照として機能します。 これらの識別子は、SUDI およびセキュアブート手順で使用されるプロセスと同様のプロセスで、製造中に Trust Anchor モジュールに埋め込まれます。

デスクフォンハードウェアの電源が入るたびに、ファームウェアは現在のコンポーネント識別子を収集し、Trust Anchor モジュール内のインプリントデータベースに保存されているものと比較します。 観察された識別子とインプリントデータベースの間の不一致は、潜在的なセキュリティ侵害を意味し、さらなる調査と対応のためにホストシステムへのレポートをトリガーします。

8. ランタイム防御

ランタイム防御は、PhoneOS ソフトウェアの稼働中に、有害なコードの挿入からそれを保護するように設計されているため、ソフトウェアやハードウェアのセットアップの既知の脆弱性を悪用する攻撃者活動を大幅に防止できます。 Cisco の一連のランタイム保護機能には、システムおよびアプリケーションファイルのメモリの場所をランダム化して、攻撃者がメモリベースの脆弱性を予想通りに悪用することをより困難にする、アドレス空間レイアウトランダム化（ASLR）などの技術が含まれます。 ビルトイン オブジェクト サイズ チェック (BOSC) は、オブジェクト サイズをチェックすることでメモリ バッファの整合性を保証するもう 1 つの防御メカニズムであり、バッファオーバーフロー攻撃を防ぐのに役立ちます。 さらに、X-space ランタイム防御は、他の手段と連携して追加のセキュリティ レイヤーとして機能し、未承認のコード実行や他のランタイムの脅威からシステムを強化します。 これらの防御が組み合わさることで、実行時のエクスプロイトに対する堅牢なバリアを形成します。

9. 必須のアクセス制御 - SE Linux

PhoneOS には、セキュリティ強化 Linux（SELinux）フレームワークが組み込まれており、システム内のすべてのプロセスに必須のアクセスコントロール（MAC）を適用します。

最小限の権限で動作する SELinux は、明示的に許可されない限り、デフォルトですべての動作をブロックします。これにより、プロセスはその機能に絶対に必要なリソースのみにアクセスできるため、プロセスが侵害された場合の損害のリスクを最小限に抑えることができます。

その結果、PhoneOS は防御を強化し、ネットワークおよびシステムサービスを効果的に保護および制限し、潜在的に侵害されるアプリケーションを隔離し、潜在的なセキュリティの脆弱性から保護する、より安全な環境を提供することができます。

10. 保管中および使用中のユーザデータを保護する

SIP プロキシ パスワードやアクセス トークンなどのユーザの機密データは、暗号化によって保護され、Cisco Trust Anchor モジュール (TPM2 モジュールによるバックアップ) を利用する安全なデータ レポジトリ内に格納されます。 このモジュールは、暗号化キー、パスワード、ユーザ資格情報、およびデバイスに関連するその他の重要なセキュリティ データを保存するための非常に安全な領域を提供するように設計されています。

デバイスを工場出荷時の設定にリセットすると、すべてのユーザの機密データは暗号消去の対象となり、以前に保存されたデータには事実上アクセスできなくなります。

アクティブなビデオコールの音声およびビデオ情報などのリアルタイムデータは、揮発性メモリに保存されます。暗号キーは通話の間に削除され、システムの再起動時にすべてのデータが消去されます。

デバイスのローカルに保存されたユーザ データは、安全なストレージのために、256 ビット キーの AES (高度暗号化標準) を使用して暗号化されます。

11. ユーザデータのエンドツーエンド暗号化

Cisco Desk phone は、Webex サービスのユーザが作成したデータにアクセスするために、エンドツーエンド暗号化キーをリクエストできます。 Cisco デスク フォンは、以下のサービスでエンドツーエンド暗号化に参加します。

- Webex カレンダーと One Button to Push (OBTP) ミーティング参加機能。
- 今後、より多くのサービスが追加されます。

Webex アプリと同様に、Cisco デスク フォンは Webex キー管理サービスにエンドツーエンド暗号化キーを要求し、これらのキーを使用してコンテンツを暗号化および復号化できます。 エンドツーエンド暗号キー、OAuth アクセストークン、カレンダーのイベントのコンテンツは、PhoneOS に永続的に保存されません。 OAuth リフレッシュトークンは PhoneOS によって安全に保存され、アクセストークンが更新されると更新されます。

Webex カレンダー サービスのエンドツーエンド暗号化の仕組みについての詳細は、 https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/esp/cisco-spark-security-white-paper.pdf を参照してください。

12. ステートフル ファイアウォール

PhoneOS ファームウェアでは、Cisco はステートフル ファイアウォールでオペレーティング システムを強化することにより、電話のセキュリティを改善しています。 ファイアウォールは、電話を悪質な着信トラフィックから保護します。 ファイアウォールは、受信データと送信データのポートを追跡します。 予期しないソースからの着信トラフィックを検出し、アクセスをブロックします。 9800 シリーズおよび 8875 はステートフル ファイアウォールをサポートしています。 メモ: Unified CM に登録されている場合、ステートフル ファイアウォールは機能しません。

13. DoS 防御

PhoneOS には DoS (サービス拒否) 保護が組み込まれており、PhoneOS は DoS 攻撃による中断に対して回復力を維持できます。 以下の 2 つの特定のメカニズムが含まれます。

- トラフィック ストーム コントロール: ブロードキャスト ストーム攻撃から保護します。
- レート制限: 特定の時間内に着信するユニキャスト パケットの数を制限し、過度のトラフィックによるオーバーロードを防ぎます。

メモ:デスク フォン 9800 シリーズと 8875 の両方に DoS 保護があります。 DOS Protection は、Unified CM または Webex Calling のいずれかに登録されている場合にのみ動作します。

14. Webex クラウド サービスへの安全なオンボーディング

Cisco Webex Control Hub は、Cisco デスクフォンのオンボードとアクティベーションを行うためのシンプルなインターフェイスを提供します。 デバイスのオンボーディングは、Webex Control Hub で生成された 16 桁のアクティベーションコードを使用して簡単に実行できます。 デバイスがオンボーディングされると、管理者はこれらのデバイスの詳細と状態を確認できるようになります。 管理者は、Webex Control Hub から選択した構成設定を更新することもできます。

オンボーディング プロセスの開始時に、デバイスは Webex Global Discovery サービスとの TLS 接続を確立し (TLS 接続用の証明書トラスト アンカーは製造中にデバイスにインストールされます)、サービスにアクティベーション コードを送信します。 16 桁のアクティベーション コードは、デバイスが属する組織およびデバイスのマシン アカウントを識別します。 コード中の組織情報は、Webex 検出サービスがデバイスを Webex 通話または ID サービスにリダイレクトするために使用されます。

デスク フォン 9800 シリーズ デバイスは、Webex 通話または ID サービスへの暗号化された TLS 接続を確立します。 TLS インターセプション攻撃に対して追加のセキュリティレイヤーを提供するために、デバイスはセキュア リモート パスワード プロトコル（SRP）を使用して、アイデンティティサービスへの追加の暗号化接続を作成し、このトンネルを使用してデバイスが Webex サービスに登録し、使用するために必要な OAuth トークンと追加の証明書信頼アンカーをダウンロードします。

セキュアリモートパスワードプロトコル (SRP) は、Augmented Password-authenticated Key Agreement (PAKE) プロトコルです (https://tools.ietf.org/html/rfc2945)。 デバイスのアクティベーションコードは、アイデンティティサービスでデバイスを認証するために使用され、デバイスとアイデンティティサービスの間でパスワードエンタングル SRP セッションキーを確立するためにも使用されます。 キー導出関数（KDF）はセッションキーを入力として使用して、デバイスとアイデンティティサービスの間で交換されるデータを暗号化するために使用される対称 AES 暗号キーを作成します。

15. セキュア コール

図 2に示すように、Webex Calling では、SIP エンドポイントとサービス間の SIP コール制御シグナリングは、Transport Layer Security (TLS) と強力な暗号スイートを使用して暗号化されます。

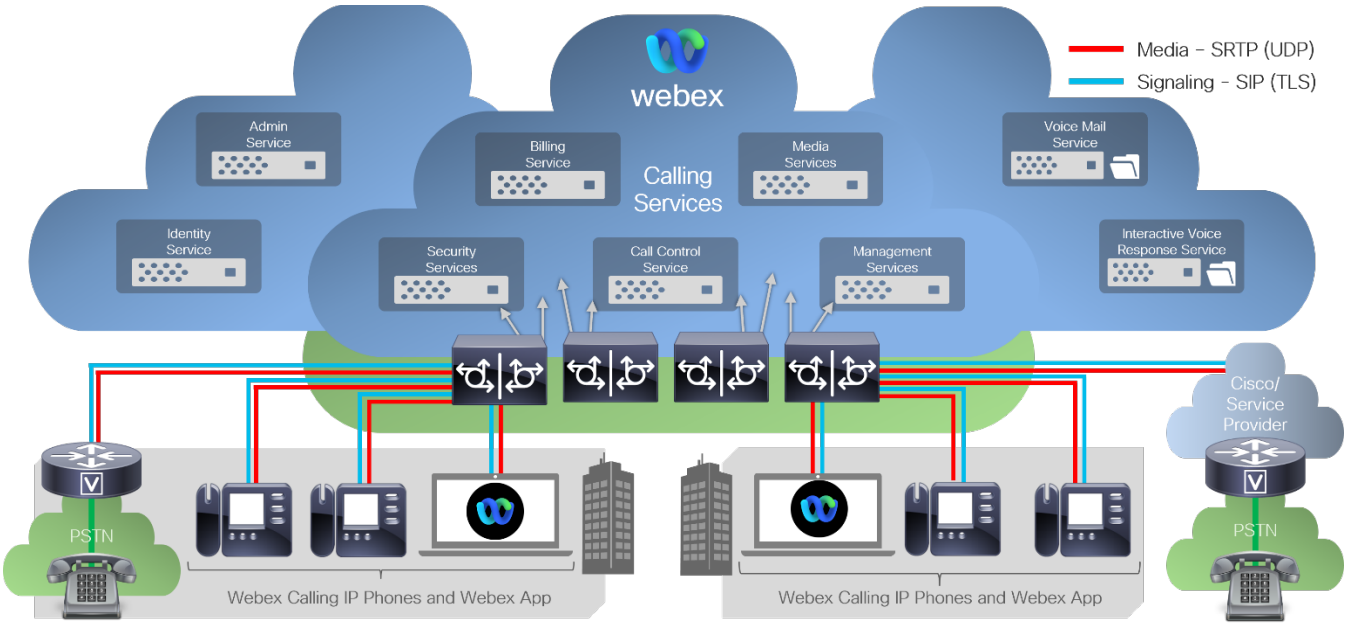

図 2. Webex Calling: SIP TLS シグナリングおよび SRTP UDP メディア

オンボーディング中、9800 シリーズからの接続はアウトバウンドのみで、完全修飾ドメイン名を使用して Webex Calling サービスへのセッションを確立します。 シグナリング トラフィックは、強力な暗号化スイートを使用した TLS によって保護され、Webex サービスは TLS バージョン 1.2 および 1.3 のみをサポートします。 各接続の暗号の選択は、Webex サーバの TLS 基本設定に基づいています。

Webex サービスは以下を優先します。

- キーネゴシエーション用の ECDHE
- RSA ベースの証明書 (2048 ビット以上のキーサイズ)
- SHA2 認証 (SHA384 または SHA256)
- 128 または 256 ビットを使用した強力な暗号化方式 (AES_256_GCM および AES_128_GCM など)

  例:
  TLS 1.2:TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

これらの暗号スイートは、米国国立標準技術研究所（NIST）特別出版 800-52 第 2 版 に定義されたガイドラインに準拠しています。詳細は、『トランスポート 4 レイヤーセキュリティ（TLS）の実装の選択、設定、使用に関するガイドライン』を参照してください。

SIP エンドポイントとサービス間のメディア ストリームは、 RFC 3711 で説明されているように、セキュアな Real-Time Transport Protocol (SRTP) を使用して保護されます。

16. スパム対策 (Webex Calling)

Cisco はアンチスパム サポートを提供することで、電話のセキュリティを向上させました。

Cisco は、電話が Webex 環境にある場合、Webex 通話記録、市内通話記録、市内通話セッション用の新しい技術標準である、セキュアなテレフォニー アイデンティティの再確認（STIR）およびトークンを使用したアサート情報の署名ベースの処理（SHAKEN）をサポートしています。 STIR/SHAKEN は、米国連邦通信委員会（FCC）により義務付けられています。 これらの標準規格では、IP ネットワークを通じて着信コールを認証し、発信者 ID を確認する手順を定義します。 STIR-SHAKEN フレームワークは、エンドユーザが受信する通話の種類を高度に識別および制御できるようにするために開発されました。 これらの標準セットは、コールの検証、コールの分類、発信者の識別情報の信頼をエンドツーエンドで容易にする基盤を提供することを目的としています。 不正な発信者は簡単に特定できます。

スパム通話から消費者を保護するために、サービス プロバイダーはネットワークに STIR/SHAKEN を実装しています。 これは FCC ガイドラインに従い、米国とカナダではすでに実施されています。 これにより、疑わしい通話を特定でき、不明の番号からの着信に対してもユーザーが自信を持って応答できます。 エンドユーザーは、サービス プロバイダーによる発信者 ID の検証から利益を得ます。

Webex サーバー上で STIR/SHAKEN のサポートが実装されている場合、電話機は発信者の STIR/SHAKEN 検証結果に基づいて、発信者 ID の横に追加のアイコンを表示します。

17. セキュアなミーティング

Webex Calling に登録されている場合、Cisco デスクフォン 9800 および 8875 は、ミーティングと従来の通話のマージを保護できます。 これらのセキュリティ機能により、ミーティングの整合性と機密性が保護されます。

たとえば、通話とミーティングを共存させることはできず、電話はこれら 2 つをマージすることを禁止します。 同様に、2 つのミーティングに一緒に参加したり、ミーティングを別の通話に転送することはできません (図 3を参照)。

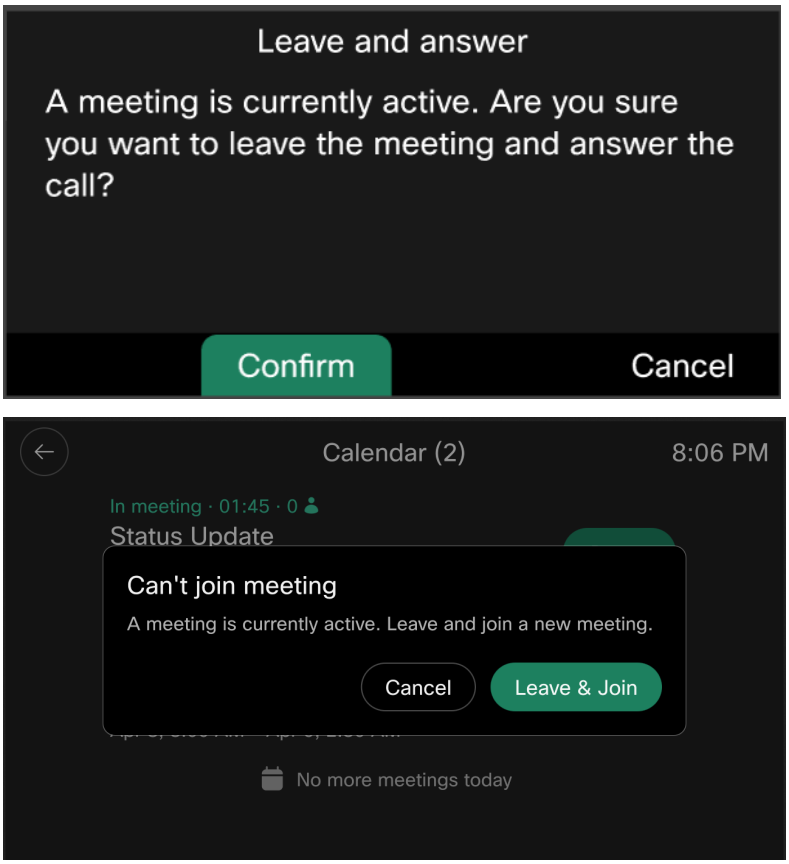

図 3. ミーティングと通話のマージ保護

18. 暗号方式

電話機の TLS アプリケーションが使用する暗号スイートを指定することができます。 指定された暗号リストは、TLS プロトコルを使用するすべてのアプリケーションに適用されます。 構成ファイルで暗号スイートを指定することもできます。

1. Webex Calling Services との接続に使用される TLS 暗号スイート

   9800 シリーズ電話および 8875 から Webex Calling サービスへの TLS 信号接続は、次の優先順位で、次の強力な暗号スイートのみをネゴシエートできます。

   - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
   - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
   - TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
   - TLS_RSA_WITH_AES_256_GCM_SHA384

2. Unified CM との接続に使用される TLS 暗号スイート

   9800 シリーズの電話から Unified CM への TLS シグナリング接続は、次の強力な暗号スイートのみを次の優先順位で Webex サービスとネゴシエートできます。

   TLS 1.2 暗号スイート

   - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
   - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
   - TLS_RSA_WITH_AES_256_CBC_SHA
   - TLS_RSA_WITH_AES_128_CBC_SHA

   TLS 1.3 暗号スイート

   - TLS_AES_128_GCM_SHA256
   - TLS_AES_256_GCM_SHA384
   - TLS_CHACHA20_POLY1305_SHA256

   TLS 1.3 キー交換

   - X25519 [RFC7748]
   - secp256r1 (NIST P-256)
   - secp521r1
   - secp384r1

   TLS 1.3 デジタル署名

   - ecdsa_secp256r1_sha256
   - ecdsa_secp384r1_sha384
   - ecdsa_secp521r1_sha512
   - rsa_pss_rsae_sha256
   - rsa_pss_rsae_sha384
   - rsa_pss_rsae_sha512
   - rsa_pkcs1_sha256
   - rsa_pkcs1_sha384
   - rsa_pkcs1_sha512

19. セキュリティ コンプライアンス

FedRAMP* および FIPS のサポートにより電話のセキュリティが向上します。 9800 シリーズおよび 8875 はすべて FedRAMP および FIPS 140-2 をサポートしています。

* まもなく導入されます。

20. Unified CM – セキュアなメディアとシグナリング

- Cisco Desk Phone 9800 シリーズは SIP OAuth を利用できます。
- X.509v3 証明書は多くのセキュリティ コンテキストでデバイス認証に使用されます。
- 各デスクフォン 9800 シリーズには固有の製造時にインストールされた証明書（MIC）が含まれています。
- MIC は、工場出荷時にインストールされた固有の ID を提供します。
- デスクフォン 9800 シリーズは、電話を顧客の環境に結びつける LSC もサポートします。
- インストールされている LSC は、電話の MIC 証明書よりも優先されます。
- ユーザーがインストールした証明書は、ワイヤレス LAN をサポートする電話だけに含まれる 3 番目の証明書タイプです。
- ユーザーがインストールした証明書は、特定のワイヤレス EAP-TLS に使用されます。
- ユーザがインストールした証明書は、電話ウェブ インターフェイス経由で手動で、または Simple Certificate Enrollment Protocol SCEP を使用して自動的にインストールされます。
- ワイヤレス EAP-TLS は、電話の MIC またはユーザがインストールした証明書の使用をサポートしますが、LSC 証明書はサポートされません。

21. Unified CM – Cisco Expressway Mobile and Remote Access (MRA)

Cisco Expressway MRA は、組織のプライベートネットワークの外部から Unified Communications (UC) サービスへの安全な、VPN なしのアクセスを可能にします。 これは、Cisco Unified Communication Manager に登録されているリモートエンドポイントのファイアウォールと NAT トラバーサルを容易にします。

- 暗号化シグナリングとメディアは、Unified CM が混合モードである必要なく、リモート エンドポイントと Expressway-C の間で確立できます。
- リモート エンドポイントと Unified CM 間の直接暗号化シグナリング、およびリモート エンドポイントとオンプレミス エンドポイント、ゲートウェイ、電話会議ブリッジ間の暗号化メディアの場合、SIP OAuth を使用する場合を除き、Unified CM 混合モードの設定が必要です。

- TLS 暗号化は、SIP シグナリングのプライバシーと整合性を保護するだけでなく、ビジュアル ボイスメール アクセス、ディレクトリ検索、構成ファイルのダウンロードを保護するために使用されます。

22. Transport Layer Security（TLS）

- TLS (トランスポート レイヤー セキュリティ) は、暗号化されたセキュリティ プロファイルで電話がセットアップされている場合、電話と Unified CM または Webex Calling の間のすべての SIP シグナリング メッセージの認証と暗号化の両方に使用されます。
- 認証されたセキュリティ プロファイルを持つ電話の場合、TLS は認証の目的でのみ使用され、SIP シグナリング メッセージは暗号化されません。
- Unified CM または Webex Calling との SIP TLS 通信は相互に認証され、シグナリングが信頼できるエンティティ間で発生し、改ざんから保護されていることを確認します。
- メディア暗号化は、シグナリングが暗号化 TLS セッションで確立された場合にのみネゴシエートされ、有効になります。
- 暗号化されたデバイス間でメディア暗号化のネゴシエートに成功すると、ユーザには南京錠のアイコンが表示され、通話が暗号化されたことを示します。
- 暗号化された SRTP (セキュア リアルタイム トランスポート プロトコル) メディア ストリームは、メディア データの整合性、信頼性、機密性を提供します。

表 1 TLS サポート

機能	7811, 7821, 7841, 7861	8811, 8841, 8845, 8851, 8861, 8865	8875, 9841, 9851, 9861, 9871
TLS 1.0	はい	はい	はい
TLS 1.2	はい	はい	はい
TLS 1.3*	なし	なし	はい

* 8875 は TLS 1.3 をサポートしますが、TPM 2.0 ハードウェアモジュールを活用しません。 Unified CM 15 SU2 以降は TLS 1.3 をサポートします。 詳細については次を参照してください。 https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/15_0/cucm_b_security-guide-release-15/cucm_m_tls-setup_2.html

23. 有線 802.1x

デスク フォン 9800 シリーズは、ネットワーク認証用に標準の 802.1X サプリカント オプションをサポートしています。これには以下が含まれます。

- EAP-FAST (セキュアなトンネリングによるフレキシブル認証)
    - EAP-TLS (トランスポート層セキュリティ)
    - EAP-FAST および EAP-MD5 は、ネットワークアクセスを許可するためのクライアント認証にユーザ名とパスワードを使用します。
- EAP-TLS は、ネットワークアクセスを認証し、許可するために、クライアント証明書が必要です。
- EAP-TLS を使用する有線接続の場合、クライアント証明書は、電話の製造元がインストールした証明書 (MIC) または Unified CM のローカルで有効な証明書 (LSC) のいずれかです
- Unified CM のローカルで有効な証明書 (LSC) は、有線 EAP-TLS のクライアント認証証明書として推奨されています。

24. ワイヤレス 802.1x

デスク フォン 9861 および 9871 には、ワイヤレス (WLAN) 802.1X ネットワーク用の以下のセキュリティ機能と認証方法が含まれます。

- 802.1X ワイヤレスは、安全なデータ転送のための AES (高度暗号化標準) 暗号化を提供します。
- ワイヤレス認証のサポートには、802.1X (EAP) および Wi-Fi Protected Access (WPA) バージョン 3 パーソナルおよびエンタープライズが含まれます
- 802.1X ワイヤレスでサポートされる EAP タイプは以下のとおりです。
    - [EAP-FAST]
    - MS-CHAPv2 (Microsoft チャレンジ ハンドシェイク認証プロトコル バージョン 2) または GTC (汎用トークン カード) とオプションのサーバ検証付き PEAP (保護された EAP)
- EAP-TLS
- EAP-FAST および PEAP は、クライアント認証とワイヤレス ネットワーク アクセスにユーザ名とパスワードを使用します。
- EAP-TLS では、認証とネットワークアクセスにクライアント証明書が必要です。
- ワイヤレス EAP-TLS の場合、クライアント証明書には、電話の製造元がインストールした証明書 (MIC) か、またはエンタープライズ認証局 (CA) またはパブリック CA からユーザがインストールした証明書を使用できます。

- ユーザがインストールした証明書は、電話のウェブ インターフェイスから手動で追加するか、Simple Client Enrollment Protocol (SCEP) を使用して自動的に追加できます。

Unified CM バージョン 10.5.2 以降では、管理者は WLAN プロファイルをプロビジョニングして、エンドユーザによるサービス セット識別子 (SSID)、周波数帯域、資格情報、パスワード、キーなどの設定の変更を防ぐことができます。

25. デバイスと周辺機器のコントロール

Unified CM と Webex Calling は、以下を無効にする機能を提供します。

- Wi-Fi（9861、9871）の有効化/無効化
- 9851、9861、9871 の管理者がコントロールする壁紙をロックする。（Unified CM）。
- 電話設定へのアクセスを有効/無効/制限する（Unified CM）
- 内蔵 Web サーバーの有効化/無効化。サポートと診断のためですが、デフォルトでは無効です。
- PC 音声 VLAN アクセスを有効/無効にします。
- PC ポートからの QoS の再マーク
- USB ポートの有効化/無効化
- USB ポートは音声デバイスに制限されています
    - USB 音声デバイスはデフォルトで有効になっています
    - USB はデバイス ページの Unified CM または Webex Calling から無効にできます
- Bluetooth の有効化/無効化 (9861、9871)
- PC ポートを有効/無効にします。

26. Cisco セキュリティと信頼

Cisco セキュリティ ツールとプロセス

Cisco Secure Development Lifecycle (CSDL)

Cisco では、セキュリティは補足ではありません。 これは、世界クラスの製品とサービスをゼロから構築し、提供するための規律あるアプローチです。 すべての Cisco 製品開発チームは、Cisco Secure Development Lifecycle (CSDL) に従うことが求められます。 これは繰り返し可能で測定可能なプロセスであり、Cisco 製品の耐障害性と信頼性を高めるように設計されています。 開発ライフサイクルのすべてのフェーズで導入されるツール、プロセス、認

識トレーニングを組み合わせることで、多層防御を確実なものにします。 また、製品の復元性に対する総合的なアプローチも提供します。 Webex 製品開発チームは、製品開発のあらゆる段階でこのライフサイクルに情熱を注いでいます。

詳細については、「Cisco セキュア開発ライフサイクルの概要」を参照してください。

Cisco 基礎セキュリティ ツール

Cisco Security and Trust Organization は、セキュリティに関する決定を行う際に、すべての開発者が一貫した立場で判断できるようにするためのプロセスと必要なツールを提供しています。

このようなツールを構築して提供する専門チームを持つことで、製品開発プロセスから不確実性を排除できます。

ツールの例を次に示します。

- 製品が準拠しなければならない製品セキュリティベースライン (PSB) 要件
- 脅威のモデリング中に使用される脅威ビルダー ツール。
- コーディング ガイドライン。
- 開発者が独自のセキュリティ コードを記述する代わりに使用できる、検証済みまたは認定済みのライブラリ。
- 開発後にセキュリティの欠陥をテストするために使用されるセキュリティ脆弱性テストツール (静的および動的分析用)。
- Cisco およびサードパーティのライブラリを監視し、脆弱性が確認された場合に製品チームに通知するソフトウェア トラッキング。
- Webex Calling における個人を特定できる情報（PII）のプライバシー

Cisco プロセスにセキュリティを育成する組織構造

Cisco には、会社全体にセキュリティプロセスを育成し、管理するための専用部門があります。 セキュリティの脅威と課題を常に把握するために、Cisco は次のものを信頼しています。

- Cisco 情報セキュリティ (InfoSec) クラウド チーム
- Cisco Product Security Incident Response Team (PSIRT)
- セキュリティ責任の共有

Cisco InfoSec クラウド

クラウドの最高セキュリティ責任者が率いるこのチームは、安全な Webex 環境を顧客に提供する責任があります。 InfoSec では、Webex を顧客に提供するためのすべての機能に対して、セキュリティ プロセスとツールを定義し、実施することでこれを達成しています。

さらに、Cisco InfoSec Cloud は Cisco 全体の他のチームと連携して、Webex サービスに対するセキュリティの脅威に対応します。

Cisco InfoSec は Webex のセキュリティ体制の継続的な改善にも責任があります。

Cisco Product Security Incident Response Team (PSIRT)

Cisco PSIRT は、Cisco の製品とサービスに関連するセキュリティ問題の管理、調査、報告を行う専任のグローバルチームです。 PSIRT はセキュリティ問題の重大度に応じて、異なる媒体を使って情報を公開しています。 レポートの種類は以下の条件によって異なります。

- この脆弱性に対処するソフトウェアのパッチまたは回避策が存在するか、重大な脆弱性に対処するためのコード修正のその後の公開が計画されています。
- PSIRT では、Cisco の顧客に大きなリスクをもたらす可能性がある脆弱性が積極的に悪用されていることを確認しています。 PSIRT はパッチが完全に利用可能でない場合でも、脆弱性を説明するセキュリティ通知の公開を加速する可能性があります。
- Cisco 製品に影響を与える脆弱性を一般に知らしめることは、Cisco の顧客にとってより大きなリスクにつながる可能性があります。 再度、パッチが完全に入手できない場合でも、PSIRT は顧客に警告を発する場合があります。

いずれの場合も、PSIRT はエンドユーザが脆弱性の影響を評価し、環境を保護するために必要な措置を講じるために必要な最小限の情報を開示します。 PSIRT は Common Vulnerability Scoreing System (CVSS) スケールを使用して、開示された問題の重大度をランク付けします。 PSIRT は、誰かがエクスプロイトを作成できるような脆弱性の詳細を提供しません。

詳細については、『PSIRT のインフォグラフィック』を参照してください。

セキュリティ責任

Webex グループのすべてのメンバーがセキュリティの責任がありますが、主な役割は次のとおりです。

- 最高セキュリティ責任者、Cloud
- バイス プレジデント兼ゼネラル マネージャ、Cisco Cloud Collaboration アプリケーション
- バイスプレジデント、エンジニアリング、Cisco Cloud Collaboration アプリケーション
- バイスプレジデント、製品マネージメント、Cisco Cloud Collaboration アプリケーション

内部および外部ペネトレーションテスト

Webex グループでは、内部評価担当者による厳格な侵入テストを定期的に実施しています。 Cisco InfoSec は、独自の厳格な社内手順のほかに、複数の独立したサード パーティと契約して、Cisco の社内ポリシー、手順、およびアプリケーションに照らして厳格な監査を実施しています。 これらの監査は、商用および政府アプリケーションのミッションクリティカルなセキュリティ要件を検証するように設計されています。 Cisco はまた、サードパーティ

ベンダーを使用して、コード支援による継続的で詳細な侵入テストとサービス評価を行います。 エンゲージメントの一環として、サードパーティは以下のセキュリティ評価を実行します。

- 重要なアプリケーションとサービスの脆弱性を特定し、ソリューションを提案する
- アーキテクチャの改善が必要な全般的な領域を推奨する
- コーディング エラーを特定し、コーディング プラクティスの改善に関するガイダンスを提供する

サードパーティの査定担当者が Webex のエンジニアリング スタッフと直接連携して、調査結果を説明し、修正を検証します。 Webex サービスの侵入テスト証明書は、Cisco Trust Portal の NDA にあります。

27. 透明度

Webex ユーザと顧客は、選択した内容、および顧客が Cisco に委託したデータを Cisco が管理および保護する方法を理解する必要があります。 Cisco はレイヤードモデルの透明性を使用してこれを実現します。 Webex アプリ自体には、ユーザがリアルタイムで意思決定を行うのに役立つ簡単な情報開示が用意されています。 詳細についてはサポートページを参照してください。サポートページは定期的に更新されます。 Cisco がどのような情報を収集し、どのように使用され、どのように保護されているかの詳細については、Cisco Trustportal にあるプライバシーデータシートを参照してください。

Cisco はまた、世界中の法執行機関および国家安全保障機関から受け取った顧客データのリクエストや要求に関するデータを公開することをコミットしています。 Cisco はこのデータを年に 2 回公開しています (1 月から 6 月または 7 月から 12 月のいずれかのレポート期間を対象とする)。 他のテクノロジー企業と同様に、Cisco はレポートのタイミングに関する制限に従い、指定されたレポート期間の終了から 6 か月後にこのデータを公開します。

詳細については、https://trust.cisco.com にある Cisco Trust Center の透明性セクションからアクセスできます。

Cisco はまた、管轄区域を越えてデータの合法的な使用を可能にするために、以下を含むいくつかのデータ転送手段に投資しました。

- 拘束的社内規則 (管理者)
- APEC クロスボーダープライバシールール
- 処理者のための APEC プライバシー承認
- EU 標準契約条項

28. サマリー

Cisco Desk Phone 9800 シリーズは、豊富なセキュリティ機能を備えています。 管理者はこれらのセキュリティ機能を展開の要件に合わせてカスタマイズできます。

29. 購入方法

購入オプションを確認し、Cisco のセールス担当者と話すには、「Cisco 製品の購入のご案内」をご覧ください。

30. 詳細情報

Cisco 信頼性のあるテクノロジーデータシート