

Cisco Collaboration ビ デオデバイスセキュリティ ティ

Cloud Collaboration セキュリティ技術文書

2023 年 5 月

目次	
1. はじめに	4
2. RoomOS ソフトウェア	4
3. セキュアデータストレージ	5
4. ユーザーが生成するコンテンツの Webex エンドツーエンド暗号化	5
5. Cisco Collaboration ビデオデバイスから Webex へのオンボーディング	6
6. Webex サービスに接続する	7
7. Cisco Collaboration ビデオデバイスのセキュア メディア	11
8. Cisco Collaboration デバイスの設定	16
9. RoomOS ウェブ エンジン	18
10. エンタープライズ ネットワーク セキュリティ	20
11. Cisco Collaboration デバイス: Webex アプリとのペアリング	21
12. Cisco Collaboration ビデオデバイスのプライバシー	24
13. Cisco Collaboration ビデオデバイス - 物理的セキュリティ	28
14. Cisco のセキュリティ モデル	29
15. Webex セキュリティと信頼	30
16. データプライバシー	32
17. 透明度	32
18. 業界標準と認証	33
19. 結論	33
20. 購入方法	34
21. 詳細情報	34



Cisco の Webex は、メッセージング、通話、ミーティングの機能を提供するクラウド コラボレーション プラットフォームです。このテクニカル ペーパーでは、Webex クラウドに登録されている Cisco Collaboration ビデオデバイスのセキュリティ機能の概要を説明しています。

1. はじめに

Cisco Collaboration ビデオデバイスは、リアルタイムのビデオ会議、コンテンツ共有、ホワイトボードなどの機能が豊富なコラボレーションデバイスです。これらのデバイスは、リモートのチームメンバーも参加できる機会を提供します。

Cisco Collaboration ビデオデバイスは、いくつかの形式で利用できます。

- [Cisco Desk シリーズ](#)
- [Cisco Board シリーズ](#)
- [Cisco Room シリーズ](#)

このドキュメントでは、Webex で登録された Cisco ビデオデバイスのセキュリティ実装について説明します。

メモ: このペーパーでは、RoomOS を実行している Webex 登録済みの Cisco Desk、Cisco Board、および Cisco Room シリーズのデバイスを対象としています。このドキュメントでは、これらのデバイスをまとめて「Cisco Collaboration ビデオデバイス」または「Cisco ビデオデバイス」と呼びます。

2. RoomOS ソフトウェア

RoomOS デバイスは工場からソフトウェアと共に届きます。通常、このソフトウェアは Webex へのオンボーディングが可能な最新の状態に保たれています。古いソフトウェアがインストールされている場合、デバイスが Webex に登録しようとしたときに、自動的に更新されます。または、オンボーディングの前に、最新のソフトウェアイメージを Cisco.com からダウンロードし、プライベート ネットワーク上のデバイスのウェブ インターフェイスを通じてアップロードできます。

図 1 に示すように、新しいソフトウェアがデバイスにロードされると、デバイスはまずインストールされるファイルの整合性チェックを実行し、インストールする前にファイルの署名を確認します。ソフトウェアが Cisco により署名されていない場合、デバイスにソフトウェアをインストールすることはできません。デバイスはまた、起動中にソフトウェアの署名を再確認します。

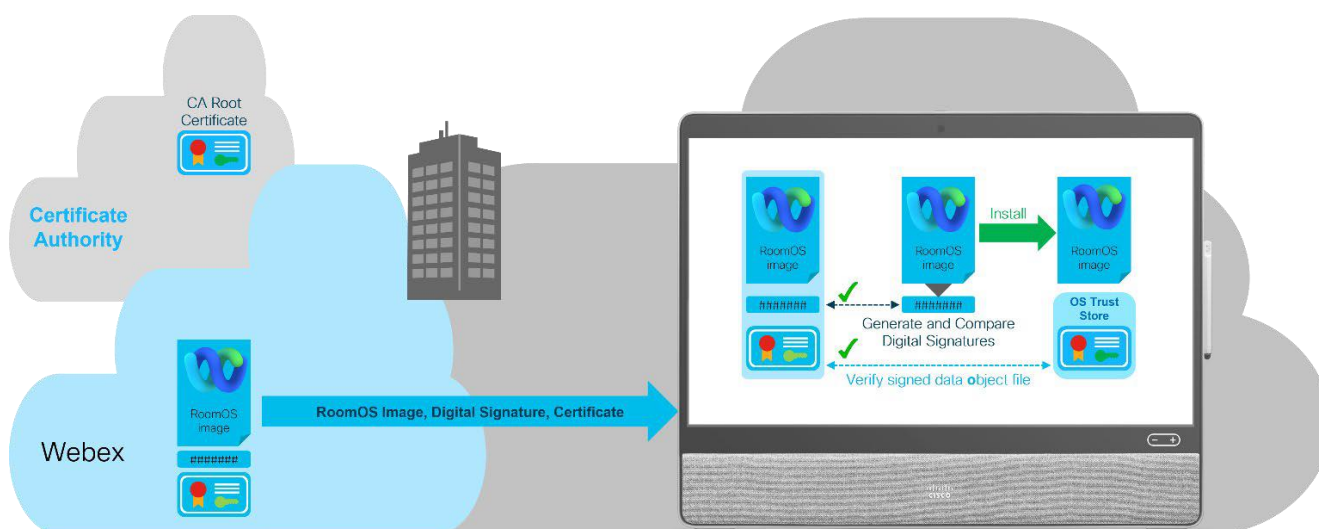


図 1. RoomOS ソフトウェア検証: デジタル署名の検証

デフォルトでは、デバイスにユーザーがアクセスできるアカウントはなく、デバイスのソフトウェアが実行されるサービス アカウントのみが存在します。特に、デバイスにルートユーザーアカウントがありません。

3. セキュアデータストレージ

設定や画像などの Cisco Collaboration ビデオデバイス構成データは暗号化され、非揮発性メモリに保存されます。このデータの暗号キーはデバイスの EEPROM に保存され、デバイスの工場出荷時設定へのリセット時に削除されるため、保存されたデータにアクセスできなくなります。アクティブなビデオ コールの音声とビデオの情報などのリアルタイム データは、揮発性メモリにのみ保存されます。このタイプのデータの暗号キーも、揮発性メモリにのみ保存され、通話が終了すると削除されます。デバイスが再起動されると、揮発性メモリ中のデータは削除されます。デバイス上の情報へのアクセスは、「[Cisco Collaboration デバイスの設定](#)」の項に記載された方法に限定されます。それ以外の場合、特別なソフトウェアや特別なハードウェアがなければアクセスできません。これらは市販で入手することはできません。

ビデオデバイスがファイルまたはホワイトボードにアクセスできる場合、これらは Webex クラウドに保存されます。ユーザーが生成したコンテンツのこの保存期間は、組織の Control Hub で指定された保存期間に従います。共有モードのデバイスで作成されたホワイトボードは、毎晩デバイスから自動的に削除されます。ホワイトボードが作成され、スペースに追加された場合、ホワイトボードはデバイスに所有されていないため、この夜間のデータ削除の影響を受けなくなります。

4. ユーザーが生成するコンテンツの Webex エンドツーエンド暗号化

Cisco ビデオデバイスは、Webex メッセージングおよびカレンダー サービスのユーザーが作成した安全なコンテンツにアクセスするために、エンドツーエンド暗号キーを要求できます。Cisco ビデオデバイス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。

- カレンダーおよび One Button to Push (OBTP) ミーティング参加機能
- ホワイトボード機能
- Webex メッセージングスペースで共有されているファイルの取得と表示

Webex アプリと同様に、Cisco ビデオデバイスは Webex キー管理サービス (KMS) からエンドツーエンド暗号キーを要求し、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。Webex メッセージング スペースとカレンダー イベントのエンドツーエンド暗号キー、OAuth アクセス トークン、コンテンツは、RoomOS に永続的に保存されるわけではありません。OAuth リフレッシュトークンは RoomOS 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 メッセージングとカレンダー 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、次を参照してください。

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/esp/cisco-spark-security-white-paper.pdf

Cisco ビデオデバイスは、ゼロ トラスト ベースのエンドツーエンド暗号化ミーティングの一時的なコンテンツに使用されるメッセージ レイヤー セキュリティ (MLS) エンドツーエンド暗号キーにもアクセスできます。詳細については、「[ゼロトラストセキュリティ : Webex Meetings のエンドツーエンド暗号化](#)」を参照してください。

5. Cisco Collaboration ビデオデバイスから Webex へのオンボーディング

Control Hub は、Cisco ビデオデバイスをオンボードしてアクティベートするためのシンプルなインターフェイスを提供します。デバイスは、管理者によって 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オンボーディングできます。エンドユーザは <https://settings.webex.com> または Webex アプリ内から、個人用の Cisco ビデオデバイス用の 16 桁のアクティベーションコードを生成することができます。

デバイスがオンボーディングされたら、管理者は Control Hub 経由でデバイスの詳細を表示したり、選択した構成設定を更新したりできます。

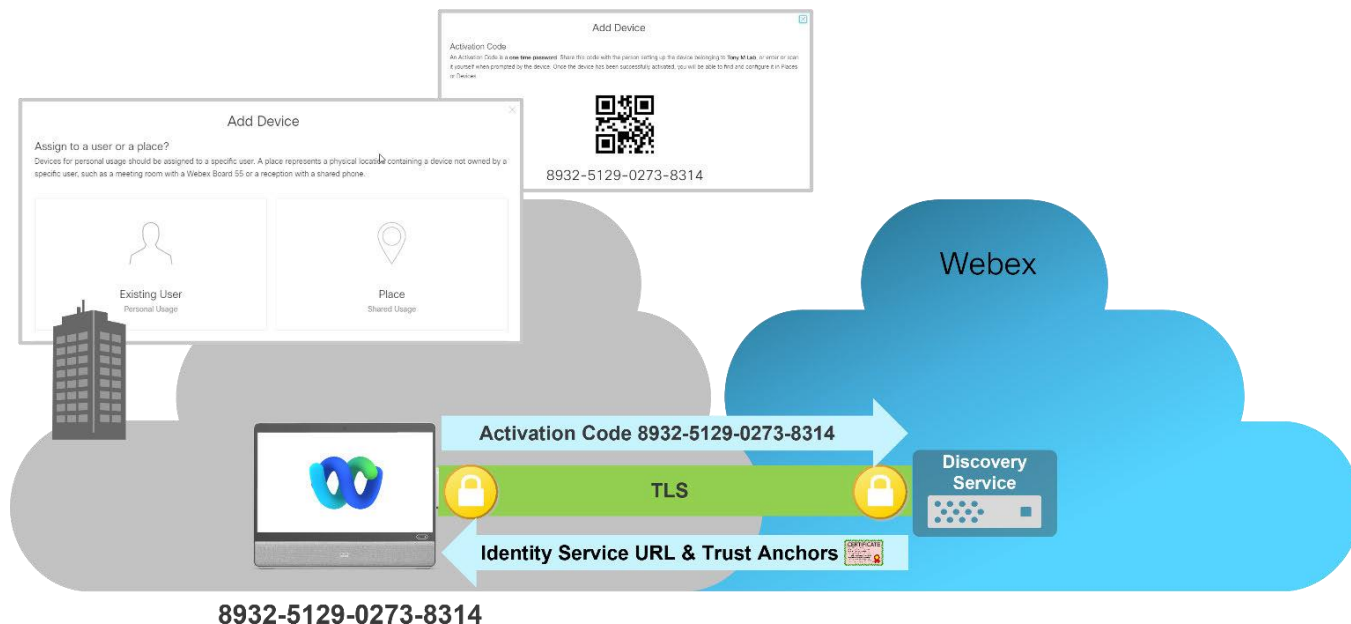


図 2. Cisco Collaboration ビデオ デバイス オンボーディング：アクティベーションコード、検出サービス

図 2 のように、オンボーディングプロセスの開始時に、Cisco ビデオデバイスは Webex Global Discovery Service (GDS) との TLS 接続を確立し (TLS 接続のための証明書信頼アンカーは製造時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により、GDS はデバイスの組織とマシン アカウントを識別できます。コードの組織情報は、Webex GDS がデバイスを Webex アイデンティティ サービスにリダイレクトするために使用されます。

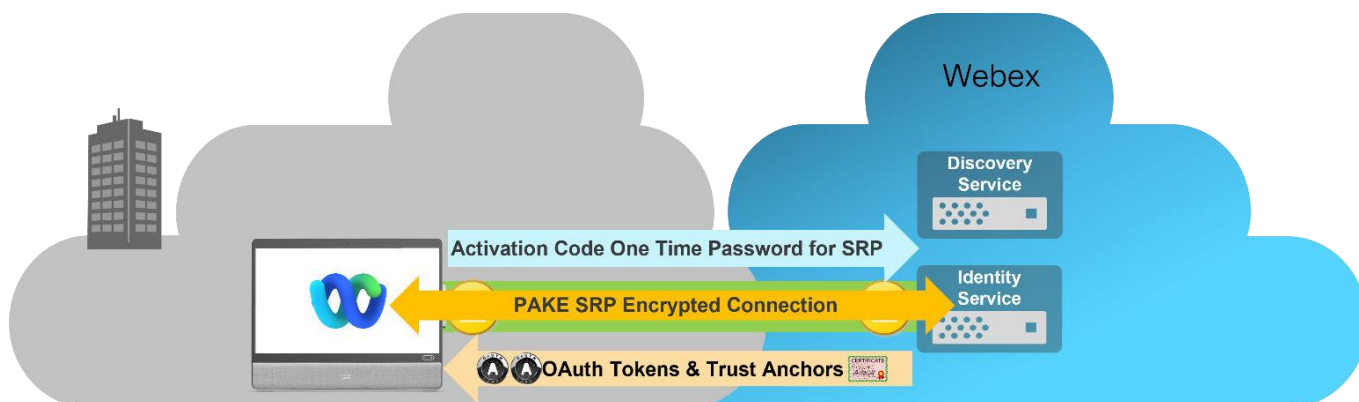


図 3. Cisco Collaboration ビデオデバイス: アイデンティティ サービスへのセキュアな Remote Password Protocol (SRP) 接続

図 3 に示すように、Cisco ビデオデバイスは Webex アイデンティティ 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、ID 認証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。

安全なリモートパスワードプロトコルとして、Augmented Password-authenticated Key Agreement (PAKE) プロトコルを利用します ([RFC 2945](#))。Cisco ビデオデバイスのアクティベーションコードは、ID 認証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 ID 認証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。

このオンボーディングの段階で、エンタープライズ CA 証明書のトラストアンカーを ID 認証サービスからデバイスにダウンロードして、エンタープライズ プロキシ サーバーによる Webex Room シリーズのシグナリングトラフィックの TLS 検査を許可することもできます。(顧客は Cisco TAC でサービスリクエストを開き、エンタープライズ CA 証明書をアップロードする必要があります)

Cisco ビデオデバイスは、Webex サービスからの TLS サーバー証明書を確認するためにインストールされた信頼する証明書のアンカー、および Webex サービスへの認証および許可された登録の証明として OAuth トークンを使用します。

6. Webex サービスに接続する

Cisco Collaboration ビデオデバイスは TLS を使用して、Webex クラウドのサービスへの暗号化シグナリング接続を確立します。

オンボーディング中、Cisco Collaboration ビデオデバイスからの接続はアウトバウンドのみであり、完全修飾ドメイン名を使用して Webex 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 によって保護されます。Webex クラウド サービスは、TLS バージョン 1.2 および 1.3、および限定された暗号スイート セットをサポートします。

Webex で使用される TLS 暗号スイート

各接続の暗号の選択は、Webex サーバーの TLS 基本設定に基づいています。

図 4 は、TLS セッションの確立中に、デバイス (TLS クライアント) が Webex サービス (TLS サーバー) への Client Hello メッセージで優先順位に従ってサポートされている暗号スイートのリストを送信することを示しています。サーバーは、クライアントとサーバーの両方がサポートする暗号スイートのサブセットとサーバーの優先度に基づいて、1 つの暗号スイートを選択し、この選択された暗号スイートを Server Hello メッセージでデバイスに返します。

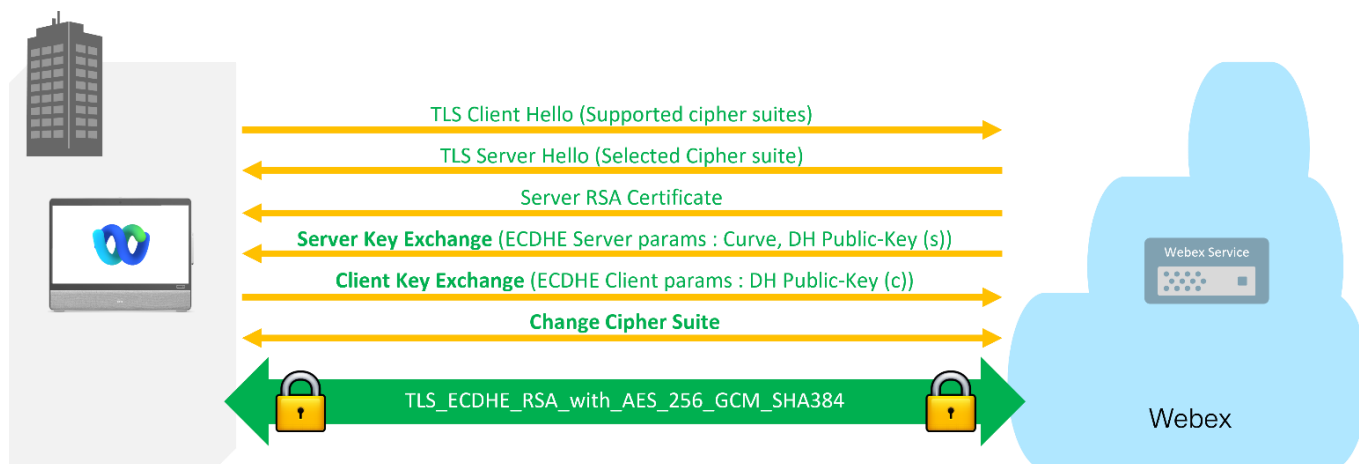


図 4. Cisco Collaboration ビデオデバイスから Webex への TLS セッションの確立

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、AES_128_GCM および CHACHA20_POLY1305 など)

例：

TLS 1.2: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

TLS 1.3: TLS_AES_256_GCM_SHA384

これらの暗号スイートは、米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。

図 5 は、TLS 1.2 のセキュアな接続において、Webex サービスが TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 を選択するところを示しています。

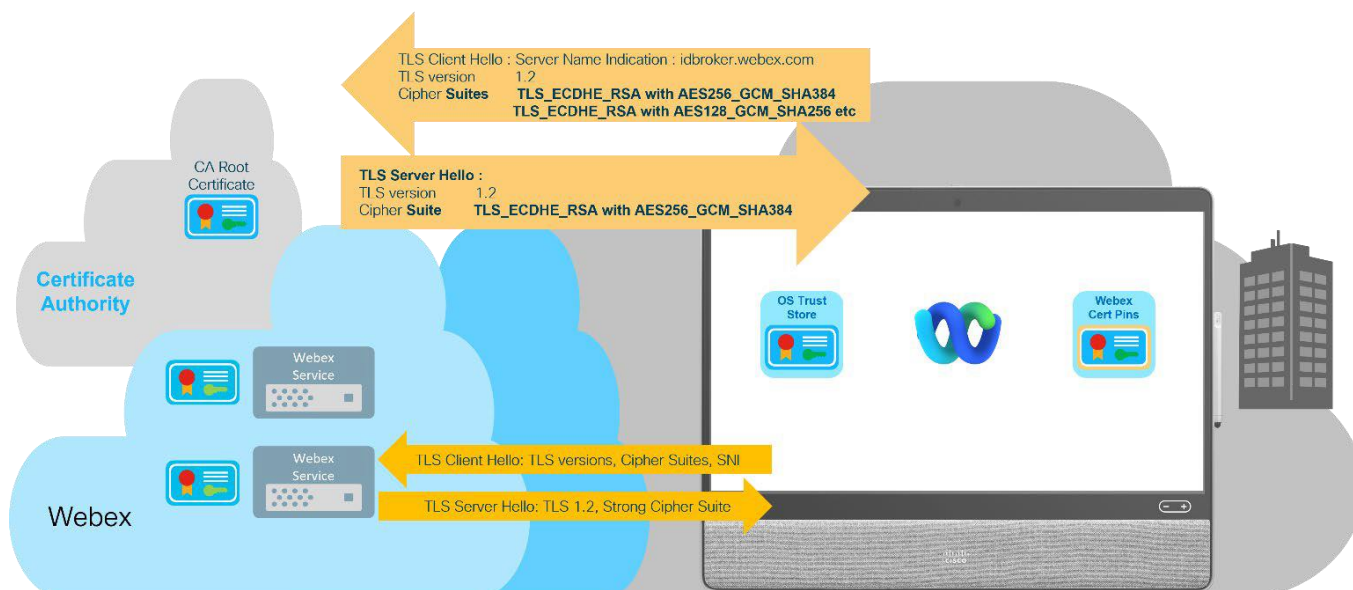


図 5. Cisco Collaboration ビデオデバイス: クライアントからサーバーへの TLS 暗号スイートのネゴシエーション

Webex サービスを認証する

Cisco Collaboration ビデオデバイスが Webex への TLS 接続を確立するとき、Webex サーバーは CA 署名サーバー証明書、CA ルート証明書、および中間証明書を Cisco ビデオデバイスに送信します（図 6 を参照）。TLS ハンドシェイクを実行する前に、デバイスは証明書チェーンを確認して Webex サービスの真正性を確認します。

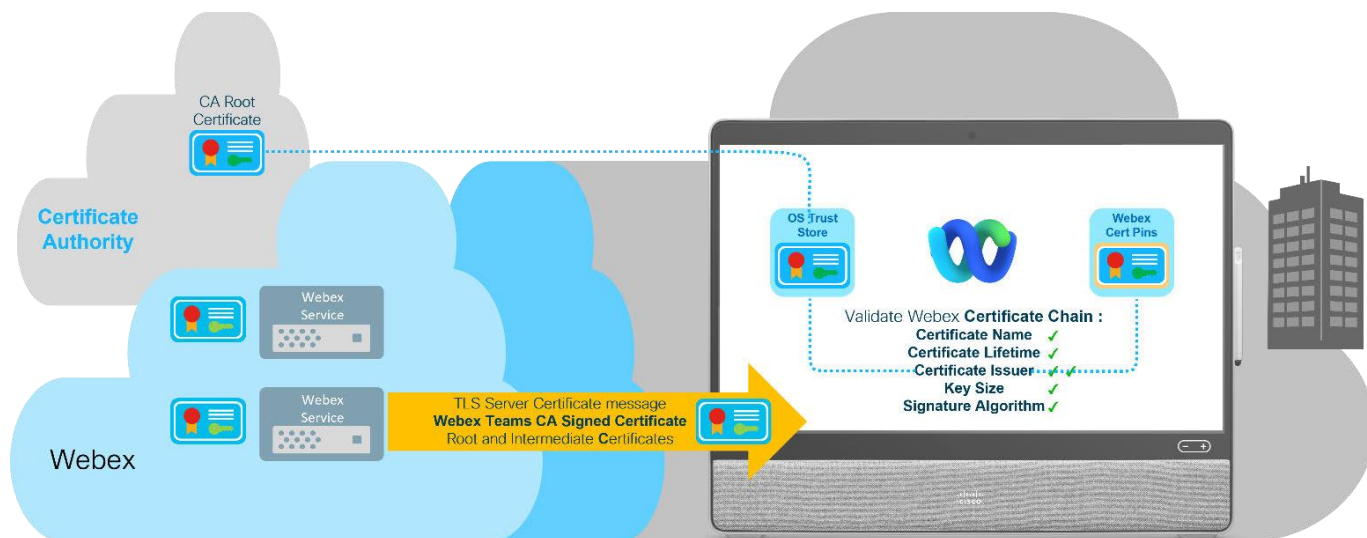


図 6. Webex サービスの真正性を確認する

Cisco Collaboration ビデオデバイス - 証明書の検証

TLS ハンドシェイク中に、サーバーは CA 署名のサーバー証明書、中間証明書、およびルート証明書を含む証明書メッセージをデバイスに送信します。Cisco ビデオデバイスは、図 7 に示すように、一連のチェックを実行して、受け取った証明書を検証し、Webex サービスを認証します。

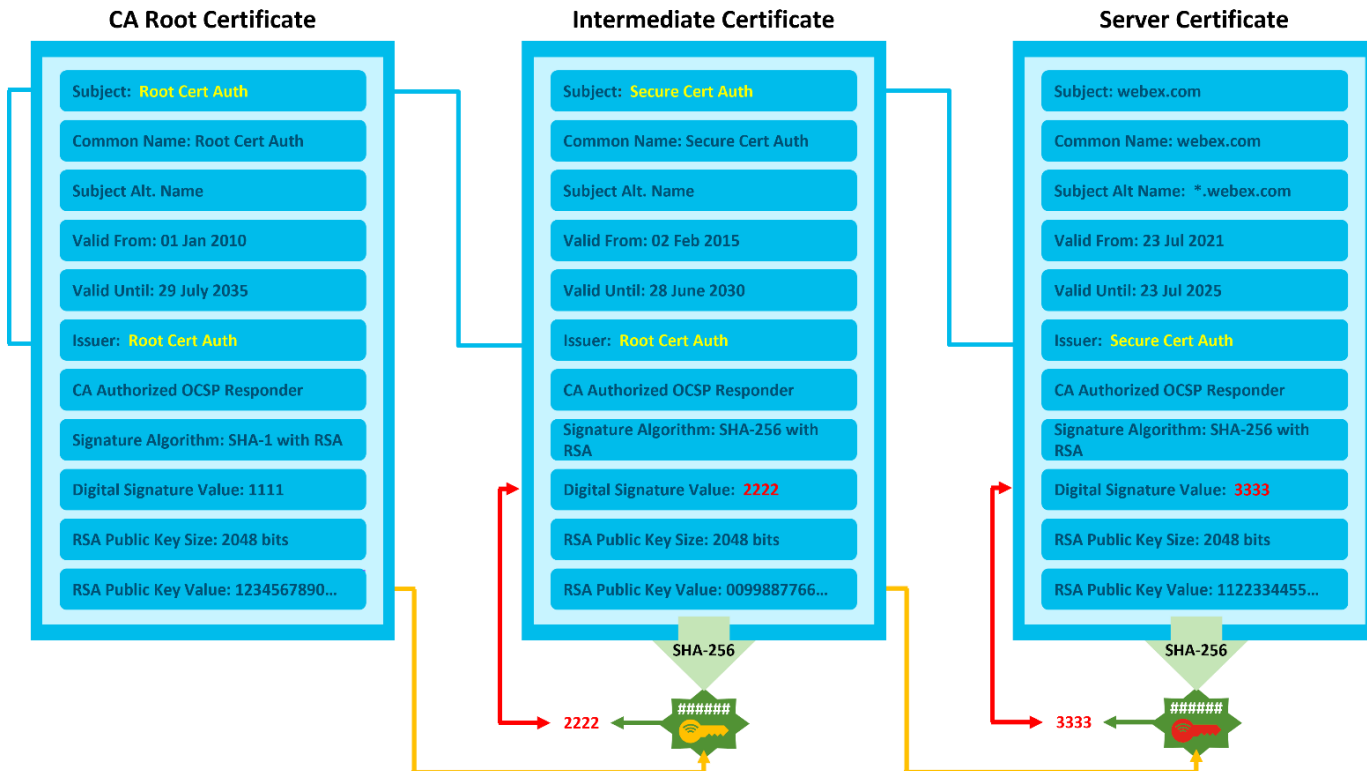


図 7. 証明書と証明書チェーンの検証

デバイスに送信される証明書のチェーンの整合性を検証するために使用される主なプロセスは次のとおりです。

証明書チェーン - デジタル署名の検証

CA ルート証明書から始めて、証明書の公開鍵を使用して最初のサブルート中間証明書のデジタル署名を解釈し、そのハッシュ値を生成します。中間証明書のハッシュが計算され、解釈されたハッシュ値と比較され、一致する場合、中間証明書の整合性が検証されます。サーバー証明書に到達するまで、他の中間証明書についても同じプロセスが繰り返されます。最後のステップとして、サーバー証明書に署名した中間証明書の公開鍵を使用して、サーバー証明書のデジタル署名を解釈し、そのハッシュ値を生成します。サーバー証明書のハッシュが計算され、復号化されたハッシュ値と比較されます。一致する場合、サーバー証明書の整合性が検証されます。

証明書発行者の確認

サーバー証明書の発行者名が、署名する中間証明書のサブジェクトフィールドの名前と値が一致するかどうか比較されます。このプロセスは、ルート CA 証明書によって署名された中間証明書の発行者名が CA ルート証明書のサブジェクトフィールドの名前と比較されるまで、証明書チェーンを続けます。最後に、自己署名 CA ルート証明書の発行者名とサブジェクト名が一致する必要があります。

証明書の有効期間

各証明書の [開始日] と [終了日] の値がチェックされ、各証明書が期限切れになっていないことを確認します。

サーバーホスト名の検証

Cisco ビデオデバイスは、接続先のサービスの名前が、サーバー証明書の [サブジェクト (Subject)] フィールドまたは [サブジェクト代替名 (Subject Alternative Name)] フィールドの名前と一致することを確認します。

7. Cisco Collaboration ビデオデバイスのセキュア メディア

Cisco ビデオデバイスは、音声、ビデオ、およびコンテンツ共有ストリームにリアルタイム メディアを使用します。通常、Cisco ビデオデバイスからのメディアは、ユーザーのロケーションから Webex クラウドのメディアノードに転送され、そこでストリームが切り替えられて配信されます。これはすべてのコールタイプに当てはまります。たとえば、他の 1 人への通話、マルチパーティコールなどです。オプションで、Webex クラウドのメディア ノードの代わりに、オンプレミスの Webex ビデオ メッシュ ノード (VMN) を展開して、メディアをローカルに切り替えて配信することもできます。

Secure Real-Time Transport Protocol (SRTP)

Cisco ビデオデバイスは、[RFC 3711](#) で説明されている Secure Real-time Transport Protocol (SRTP) を使用してメディアストリームを保護します。音声とビデオのコーデック、メディア暗号化暗号スイート、暗号キーは、[RFC 4568](#) で説明されている SDES を使用して、HTTPS で安全にネゴシエートされます。

Cisco ビデオデバイスは次のメディア暗号化をサポートしています (下記の優先順位で利用します):

- AES-256-GCM
- AES-128-GCM
- AES-CM-128-HMAC-SHA1

クラウド登録 Cisco ビデオデバイス間の 1:1 の通話、および Webex アプリとクラウド登録 Cisco ビデオデバイス間の 1:1 の通話では、メディア暗号化暗号として AES-256-GCM が使用されます (図 8)。同様に、クラウド登録 Cisco ビデオデバイスから Webex Meetings への通話でも、メディア暗号化暗号として AES-256-GCM を使用します (標準およびエンドツーエンド暗号化ミーティングの両方)。

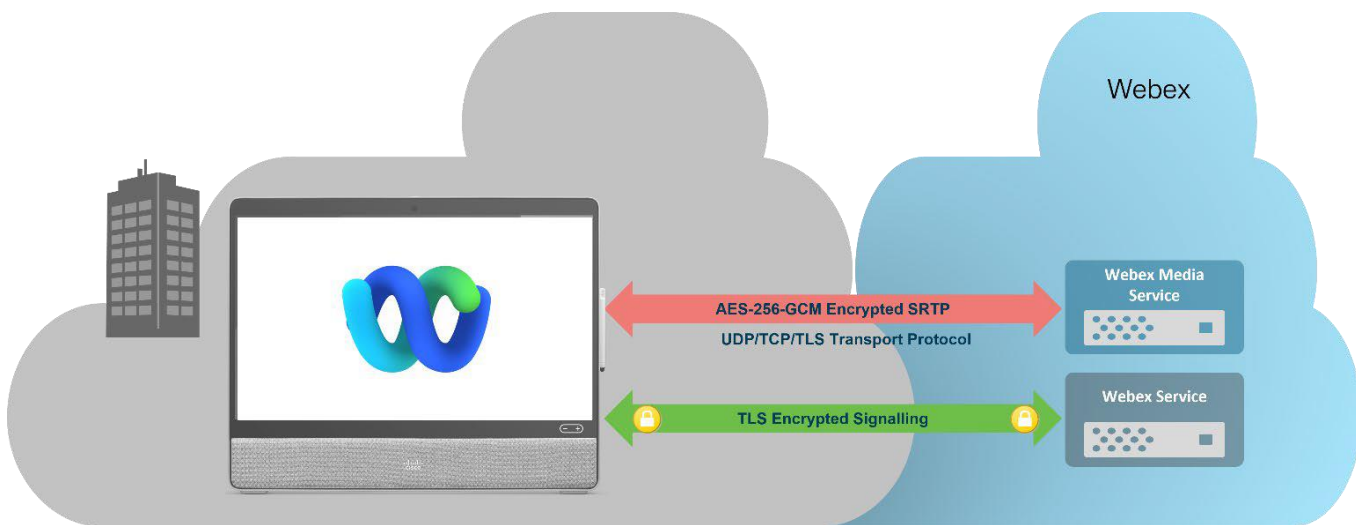


図 8. Cisco Collaboration ビデオデバイスの暗号化メディアと Webex へのシグナリング接続

AES-CM-128-HMAC-SHA1 暗号化暗号は、SIP およびメディアにこの暗号化暗号のみを優先またはサポートするサードパーティ製デバイスとの相互運用性のためにサポートされています。

暗号化メディアの転送プロトコル

Cisco ビデオデバイスは、メディアのトランスポート プロトコルとして UDP、TCP、TLS をサポートしています。

[RFC 3550](#) (RTP : リアルタイム アプリケーション用トランスポートプロトコル) に従い、Cisco は音声およびビデオのメディアストリームに優先的なトランスポートプロトコルとして UDP を使用しています。コネクションレス型のトランスポートプロトコルであるため、UDP はすべてのパケットが上位レイヤーに配信されること、または送信された順番で配信されることを保証しません。アプリケーション (この場合は音声またはビデオのコーデック) 。しかし、UDP がメディア トランスポート プロトコルとして使用される場合、コーデックは、ジッターバッファ容量を超える順序の乱れたパケットを無視し、途中で失われたか、受信が遅すぎたパケットを隠します。これにより、リアルタイムのメディアストリームをできるだけ遅延を少なくするためにレンダリングします。

Cisco ビデオデバイスは、フォールバック メディア トランスポート プロトコルとして TCP もサポートしています。ただし、Cisco では、音声およびビデオ メディア ストリームのトランスポート プロトコルとして TCP を推奨していません。TCP はコネクション指向であり、正しく順序付けられたデータを上位層アプリケーションに確実に配信するように設計されているためです。TCP を使用する場合、送信側は紛失パケットを確認応答されるまで再送し、受信側は紛失パケットが回復するまでパケットストリームをバッファします。メディア ストリームの場合、この動作は遅延の増加やジッターとして現れ、通話の参加者のメディア品質に影響を与えます。

Cisco ビデオデバイスは、メディア転送の最後の手段として TLS (セキュア TCP) もサポートしています。Cisco ビデオデバイスから TLS 経由でメディアが送信される場合、デバイスで設定されている場合でも、それは TLS プロキシサーバーを通過しないということに注意してください。

Cisco ビデオメディアは、Webex クラウドにアウトバウンドする対照的に内部開始された 5 タプル (送信元 IP アドレス、宛先 IP アドレス、送信元ポート、宛先ポート、プロトコル) ストリームを使用して双方向に流れます。

Cisco ビデオ はまた、ファイアウォールトラバーサルとメディアノードの到達可能性テストに STUN ([RFC 5389](#)) も使用します。

メディア転送プロトコル : 送信元と宛先のポート番号

表 1 は、Cisco Collaboration ビデオデバイスで使用されるリアルタイムメディアの送信元と送信先のトランスポートプロトコルのポート番号を示しています。Webex クラウドメディアサービスで使用される IP サブネットは、[『Webex サービスのネットワーク要件』](#)の記事で確認できます。

表 1. Cisco Collaboration ビデオデバイス: メディア転送プロトコルとポート

転送プロトコル	ソースポート	宛先ポート
UDP	音声: 52050-52099	5004, 9000
	ビデオ: 52200-52299	
TCP	エフェメラル	5004
TLS	エフェメラル	443

メディア ストリームの DSCP 値

Cisco ビデオデバイスは、メディアトラフィックに次の Differentiated Services Code Point (DSCP) 値を使用します。

- 音声:優先転送 (EF)、DSCP 46
- ビデオ : Assured Forwarding (AF41) 、 DSCP 34

Cisco ビデオデバイスで使用される DSCP 値は、[RFC 4594](#) (『DiffServ サービスクラスの設定ガイドライン』) と一致します。

Cisco ビデオデバイスによって送信されるメディアトラフィックの DSCP 値は、エンタープライズ ネットワークを横断する音声およびビデオ ストリームをキューに入れ、優先的に処理するために使用できます。インターネットを通過する Webex メディア ストリームは、通常、インターネット サービス プロバイダによって DSCP 値が 0 に設定されます。UDP を使用するメディアインターネット経由で送信されるリターンメディアストリームのゼロに設定された DSCP 値は、音声とビデオストリームを識別するために UDP ソースポート範囲を使用して、エンタープライズ エッジ ルーターによって再割り当てできます。

Cisco Collaboration ビデオデバイス: メディア ノード到達可能性テスト

Cisco ビデオデバイスは、起動時、ネットワーク接続の変更時、およびその後定期的に、メディア ノード検出プロセスを使用して、組織で使用可能なメディア ノード クラスター (クラウド メディア ノードおよびオンプレミス ビデオ メッシュ ノード) の到達可能性を判断します。通話の確立中に、Cisco ビデオデバイスは到達可能性レポートを Webex クラウドに送信します。利用可能なトランスポート プロトコル (UDP/TCP/TLS)、往復時間 (RTT)、およびリソースの可用性に基づいて、Webex クラウドは各デバイスで使用されるメディア ノードを決定します。

図 9 に示すように、メディアカスケード接続は、1 回の通話で複数のメディアサーバーが使用される場合に確立されます。

メモ : Microsoft Teams 用の Webex ビデオ統合 (VIMT) の場合、ビデオインテグレーション通話のメディアパスは、他の Webex Meetings 通話フローとは異なります。Azure データセンターの専用メディアクラスターがこのコールタイプを処理するためです。VIMT の専用メディア クラスターは、Webex 登録済みデバイスが実行する到達可能性テストの一部ではありません。代わりに、統合は発信者の発信元に基づいて、各通話に最適なメディア クラスターを使用しようとします。詳細については、「Microsoft Teams 用の Webex ビデオ統合を展開する」を参照してください。

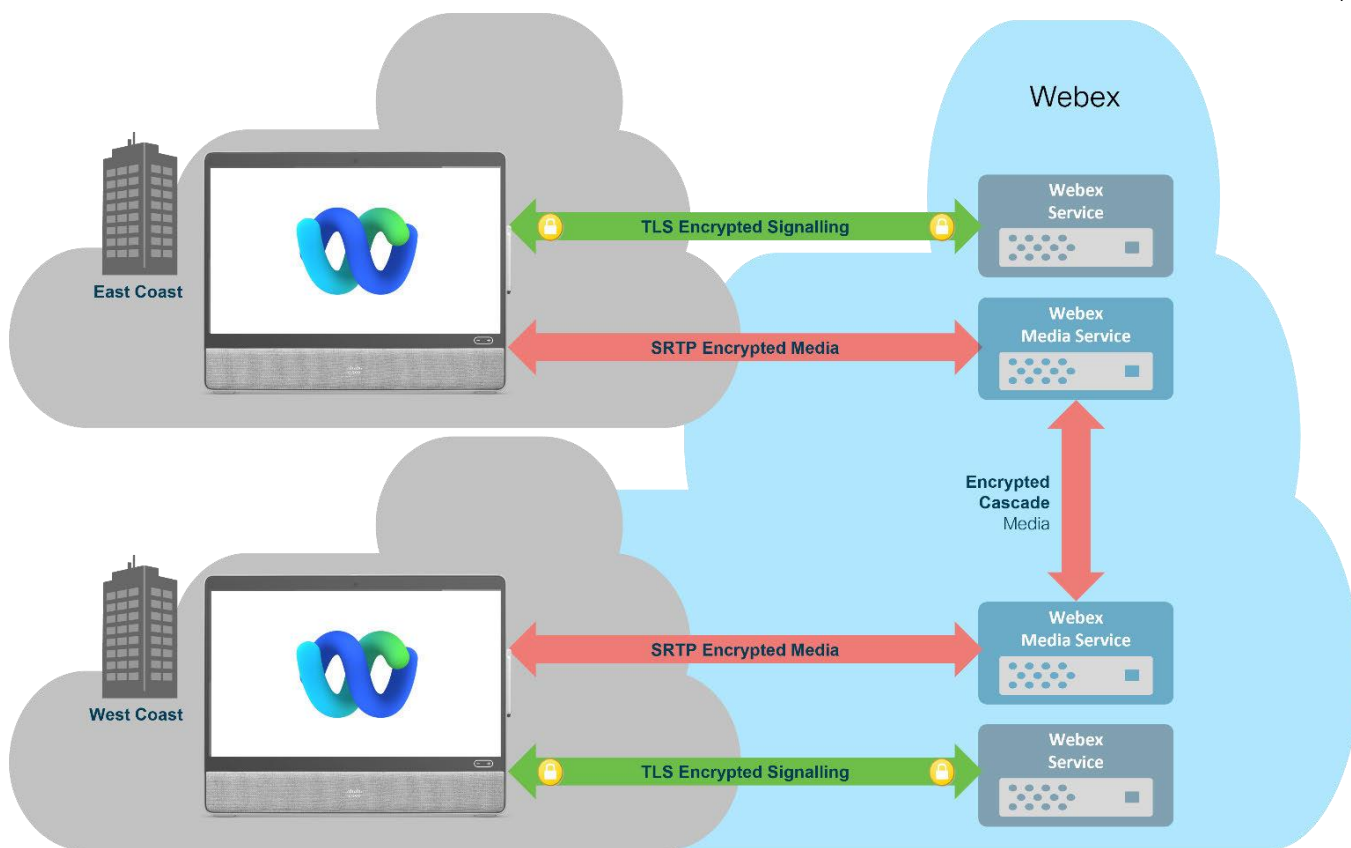


図 9. メディアとシグナリング: 2 台の Cisco Collaboration Video デバイス間の通話

ゼロトラストセキュリティ: Webex Meetings のエンドツーエンド暗号化

Webex Meetings のゼロトラストセキュリティは、業界標準の暗号化プロトコルに基づいて構築されたエンドツーエンド暗号化の新しいフレームワークです。ゼロトラストセキュリティにより、Cisco のビデオデバイスと Webex アプリは、Cisco がミーティング暗号キーにアクセスできない新しい標準ベースの形式のエンドツーエンド暗号化 (E2EE) を使用して Webex Meetings に参加できます。

ゼロトラストセキュリティは、標準の SRTP メディア暗号化とシングル サインオン (SSO) 認証に加えて、エンドツーエンドの保護レイヤーを追加します。

- **キー交換**: E2EE ミーティングに参加するデバイスは、ビデオ会議プロバイダがこれらのキーにアクセスできないように、E2EE のキーをセットアップする必要があります。Webex Meetings のゼロトラストセキュリティでは、キー交換に [Messaging Layer Security \(MLS\)](#) プロトコルを使用します。MLS は、オープンソースコミュニティで開発された技術を基にした標準であり、それらを [厳格で](#)、[正式に確認された](#) 環境に適用します。MLS により、Webex は forward secrecy と post-compromise security をミーティングの参加者に提供します。
- **コンテンツ保護**: エンドツーエンド暗号化を使用して Webex ミーティングのメディアを保護します。ゼロトラストセキュリティは、セキュアフレーム (SFrame) を使用します。これは、リアルタイムメディアを暗号化するための、高速でシンプルな暗号化フレームワークで、最小限のオーバーヘッドで追加の暗号化レイヤーを追加できます。

ゼロトラストセキュリティ: E2EE Webex Meetings のエンドツーエンド アイデンティティ

エンドツーエンド暗号化に加えて、Webex Meetings のゼロトラストセキュリティはエンドツーエンド (E2E) アイデンティティも提供します。これにより、Webex 以外の認証局または ID プロバイダによって、ユーザーとデバイスのアイデンティティを個別に確認できます。

E2E の ID を使用するには、Cisco Collaboration ビデオデバイスと Webex アプリに、ID を証明する資格情報が必要です。

Webex Meetings の Cisco ビデオデバイスの E2E の ID は、Automated Certificate Management Environment (ACME) プロトコルといくつかの拡張機能を使用して、エンタープライズ ID システムを活用して、Webex がシームレスなユーザーエクスペリエンスで高品質な ID 確認を提供できるようにします。

将来的には、Webex Meetings の Webex アプリの E2E の ID は、「[ユーザー情報の検証可能な資格情報](#)」の新しいオープン ID 接続標準を使用します。この標準は MLS と統合され、強力でスムーズなユーザー認証を提供します。

図 10 のように、Webex E2EE ミーティングの各参加者の ID 確認の状況がミーティング名簿に表示され、各参加者は一目で各ユーザーの ID がどのように検証されたかを確認し、参加者の ID の特定の詳細を確認するためにドリルダウンすることができます。

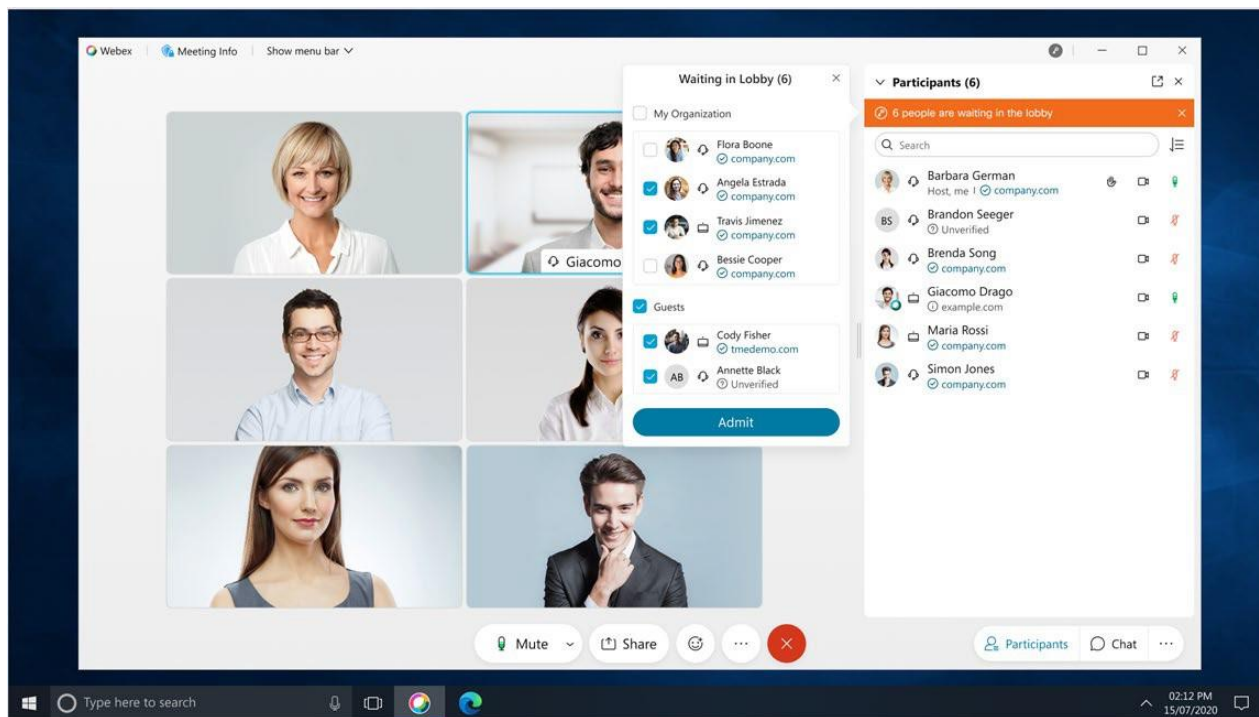


図 10. Webex Meetings 参加者：ID の可視性

Webex のゼロトラストセキュリティの詳細については、次を参照してください。

<https://www.cisco.com/c/en/us/solutions/collateral/collaboration/white-paper-c11-744553.html>

8. Cisco Collaboration デバイスの設定

デバイスが Control Hub にオンボードされた後、管理者は多くの場合、構成の変更を行う必要があります。デバイスの設定はいくつかの方法で行うことができます。

- [Control Hub](#)
- [ビデオデバイス ウェブ インターフェイス](#)
- [アプリケーション プログラミング インターフェイス \(API\)](#)

以下の項では、各設定ソースをセキュリティの観点から説明します。

Control Hub

Control Hub には、次を含むいくつかのセキュリティ関連の構成オプションが用意されています。

- 顔認証 - 名前ラベル
- Webex Assistant
- 自動クラッシュレポート
- デバイス構成
- リモートアクセスキー

組織の Control Hub から顔認証を有効にすると、ユーザーを招待するメールを送信できます。これには、ユーザーが自分の写真を撮影してサインアップするために使用できるリンクが含まれています。組織設定が有効になり、ユーザーが登録され、そのユーザーが Room、Board、または Desk シリーズのデバイスで表示されると、そのユーザーは Webex で認識されます。顔認証のセキュリティの詳細については、[Cisco Collaboration Video Device のプライバシー](#) セクションを参照してください。

Control Hub から Webex Assistant を有効にすると、誰でもすばやく簡単に音声で Room、Board、および Desk シリーズのデバイスを操作できるようになります。Webex Assistant のセキュリティに関する詳細は、下記の Webex Assistant のセクションを参照してください。

自動クラッシュ レポートにより、ビデオデバイスがクラッシュした場合に、デバイスはログを Cisco にアップロードできます。これにより、Cisco は、上げられたサポートケースとは独立して問題を診断できます。クラッシュ レポートには、ユーザーおよび組織の識別子、ユーザーエージェント文字列、サニタイズされたブラウザ文字列、クライアント IP アドレス、ユーザーデバイスの MAC アドレスが含まれます。すべての情報は機密情報として取り扱われ、製品の品質向上のためにのみ使用されます。

Control Hub から直接、個々のビデオデバイスの高度な構成のサブセットにアクセスできます。一部の構成は読み取り専用として表示され、Control Hub からは変更できませんが、その他は表示と編集が可能です。変更はその後、上記で説明されているのと同じ安全な通信方法を使用してビデオ デバイスで行われます。

Control Hub では、ビデオデバイスのリモート サポート キーを生成することもできます。このキーの使用は、問題をトラブルシューティングするために、Cisco Technical Assistance Center (TAC) によって要求される場合があります。キーが生成されたら、それを TAC に送信する必要があります。TAC は、内部ツールを使用して、これをビデオ デバイスで直接認証方法に変換します。これにより、ユーザーアカウントを生成したり、ビデオデバイスに資格情報を提供する必要がなくなります。サポート終了後にキーをリセットすることで、無効化することができます。

リモートサポートユーザーの状態は、`xCommand UserManagement RemoteSupportUser GetState` を使用して確認することができます。必要に応じて、Remote Support ユーザーの生成を永久的に無効にすることも可能です（機能を再度有効にするには、工場出荷時の状態へのリセットが必要です）`xCommand UserManagement RemoteSupportUser DisablePermanently`。

TAC が RemoteSupport を使用して Cisco Collaboration デバイスにアクセスできるようにするには、TAC エージェントが、IP 接続された PC を介してターゲット デバイスに接続されている必要があることに注意してください。オンサイトでデバイス接続が可能なユーザとTACエージェントがオンラインミーティングを実施することで実現することができます。

Cisco TAC は、ターゲット デバイスへの IP 接続がない場合、RemoteSupport を使用できません。

ビデオ デバイス ウェブ インターフェイス

デフォルトでは、ビデオデバイスのすべてのローカルユーザーアカウントがオンボーディング中に非アクティブ化されるため、ビデオデバイスのウェブ インターフェイスに直接アクセスすることはできません。CLI コマンド `xCommand Webex Registration Start` and specifying `SecurityAction: NoAction` を指定するか、または Cisco ビデオ デバイス コネクタ ソフトウェアを使用することで、デバイスをローカルユーザーアカウントでオンボーディングすることができます。また、工場出荷時の状態にリセットするデバイスにローカルアカウントを作成し、デバイスを Control Hub に登録する際にそのアカウントを保持することも可能です。デバイスの WebUI にデバイス アクティベーション トークンを入力し、[ローカルユーザーとインテグレーションを無効にする (Disable local users and integrations)] チェックボックスをオフにします。デフォルトの管理者アカウントにパスワードが設定されていない場合、上記のチェックボックスのチェックを外しても、パスワードがないためにアカウントが非アクティブになります。

アクティブなユーザーアカウントがない場合は、Control Hub の [デバイス] の下にある [ウェブポータルを起動] オプションを使用してビデオデバイスのウェブインターフェイスにアクセスできます。これにより、ブラウザセッションをビデオデバイスに直接クロス起動し、一時的なローカルユーザー *Webex Admin* が作成されます。このプロセスには、Webex およびウェブブラウザ経由で Cisco Collaboration デバイスに渡される一時トークンの作成が含まれます。Cisco Collaboration デバイスへの直接接続が確立されると、PC は Cisco デバイスと同じサブネット上にあるか、Cisco デバイスへのルーティング可能なネットワーク上にある必要があります。デバイスが到達不能な場合（たとえば、間にルーティングがない 2 つの異なるネットワーク）、Control Hub は接続に失敗し、デバイスが利用できないことをユーザーに通知します。HTTPS を使用できるように Cisco Collaboration デバイスに有効な証明書をアップロードすることで、このプロセスの安全性を高めることができます。

ウェブ インターフェイスに接続したら、管理者アカウントをアクティベートするか、新規ユーザーを作成することができます。ユーザーは複数の役割を持つことができます: *管理者*、*監査*、*会議室コントロール*、*インテグレーター*、および *ユーザー*。役割とその機能の詳細については、ビデオデバイスの管理者ガイドを参照してください。可能な限り最も制限された役割を持つユーザーを使用することをお勧めします。

デフォルトでは、ウェブ インターフェイスは HTTPS を使用します。古いウェブブラウザをサポートするために、ウェブサーバーが使用できる TLS の最小バージョンは 1.1 ですが (TLS 1.1 は無効にできます)、最新のブラウザは TLS 1.2 または 1.3 をネゴシエートします。

ビデオデバイスには、事前にインストールされた自己署名証明書と認証局証明書のセットがあります。サービス証明書と認証局はウェブ インターフェイスまたは API 経由で追加できます。サービス証明書は、HTTPS、監査、および 802.1X の目的で使用するか、機能ごとに別の証明書を使用できます。サービス証明書は PEM 形式を使用し、パスフレーズの有無にかかわらず、RSA または DSA 暗号化秘密鍵を含む場合があります。代わりに、証明書と秘密鍵を別々にアップロードすることもできます。Certificate Authority の証明書は、PEM 形式で、単一ファイルに 1 つ以上の証明書と共にエンドポイントに追加できます。

アプリケーション プログラミング インターフェイス (API)

デバイス API にアクセスするには、いくつかの方法があります。

- SSH
- HTTP/HTTPS
- WebSocket
- RS-232 / シリアル接続
- Bot / Webex ユーザー

SSH はデフォルトで有効になっていますが、ビデオデバイスでユーザーがアクティベートされた場合、または公開鍵認証が使用されている場合にのみ、認証が可能になります。デフォルトのホストキー方式は 2048 ビットのキーサイズの RSA (Rivest-Shamir-Adleman) です。NIST 曲線 P-384 による ECDSA (楕円曲線デジタル署名アルゴリズム) および Ed25519 署名スキーマによる EdDSA (Edwards-curve デジタル署名アルゴリズム) は、必要に応じて有効にできます。

HTTP/HTTPS API アクセスは、上記のウェブ インターフェイスのセクションで説明したのと同じ原則に従います。ユーザーが API にアクセスするには、*admin* ロールを持つユーザーとして HTTP 基本アクセス認証を使用して認証する必要があります。

API WebSocket 接続はデフォルトで無効になっています。使用するにはアクティベートする必要があります。その後、接続の HTTP/HTTPS 設定に従います。HTTPS のみが有効な場合、暗号化された WebSocket 接続のみが許可されます。認証は、基本認証と auth プロトコル ヘッダーを使用してサポートされます。

シリアル接続は、デバイスに応じて USB または COM ポート経由で提供されます。シリアルはデフォルトで有効になっていますが、API にアクセスする前にデフォルトで認証が必要です。そのため、これが可能になる前にユーザーをアクティベートする必要があります。

Control Hub の完全な管理者またはデバイス管理者は、クラウド経由でデバイス API にアクセスする権限があります。詳細は、<https://developer.webex.com/docs/api/v1/device-configurations> を参照してください。

xConfiguration Network [n] RemoteAccess Allow 設定を使用すると、特定のリモート IPv4/IPv6 アドレスからのデバイスでの HTTP、HTTPS、WebSocket、SSH または Telnet へのリモートアクセスを制限することができます。クラウド API アクセスはこの設定の影響を受けないことに注意してください。

9. RoomOS ウェブ エンジン

RoomOS ウェブエンジンは、Cisco ビデオデバイス上で動作するシングルタブの Chromium ブラウザです (図 11 参照)。Web エンジンは以下の機能を提供するために使用されます。

- サードパーティのウェブ アプリ (Miro、Jira、Trello、Realtime Board など)
- デジタル サイネージ
- WebRTC サードパーティ通話 (Microsoft Teams、Zoom、Google など)
- Webex 埋め込みアプリ
- マクロおよびサードパーティの拡張機能から開いたウェブの表示 (建物マップ、退出マップ、説明ビデオなど)
- エンタープライズ コンテンツ管理 (クラウドドキュメントはインテグレーションとして利用可能)

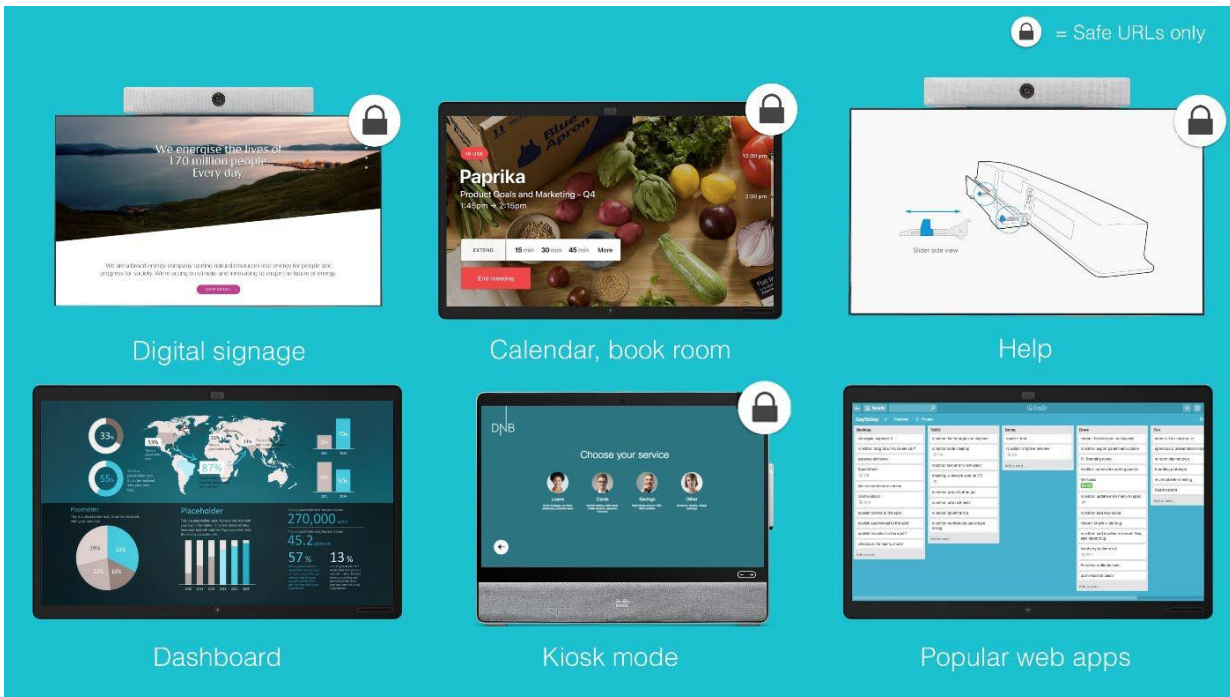


図 11. Cisco Collaboration ビデオデバイス:ウェブエンジン

ウェブエンジンは Linux サンドボックスを使用して Chromium を実行します。サンドボックス化により、Chromium インスタンスをデバイス上の他のプロセスから隔離することで、コードの実行によってホストの恒久的な変更を行ったり、ホストの機密情報にアクセスしたりすることはできません。ウェブエンジンはファイルシステムにアクセスできず、ユーザーのプライバシーを保護するために、ログからブラウザ履歴が削除されます。ウェブプロキシが Webex Room シリーズ デバイスで設定されている場合、Web エンジンはトラフィックをこのプロキシに送信します。

ウェブ機能は通常、ユーザーデータを Cookie、キャッシュ、ローカルストレージなどに保存します。これらのデータは、機能に応じて異なる方法で管理されます。

- サイネージ：データは永続し、自動的に削除されることはありませんが、手動で削除することはできます。
- ウェブアプリ：データは保持されますが、デフォルトでは 1 日に 1 回削除されます。これは、[xConfiguration RoomCleanup AutoRun ContentType WebData](#) を [オフ (Off)] に設定することで無効にできます。これは、パーソナルモードで登録されたデバイスに推奨されます。すべてのウェブアプリは同じプロファイルを共有するため、ウェブアプリのデータを個別に削除することはできません。
- WebRTC:データは通話が終了すると削除されます。
- プログラムによるウェブビュー: ウェブアプリと同じです。
- 埋め込みアプリ: 通話が終了すると、データは削除されます。

ウェブデータは xapi コマンド [xCommand: WebEngine DeleteStorage](#) を使って手動で削除することができます。

RoomOS ウェブエンジンの詳細については、<https://roomos.cisco.com/doc/TechDocs/WebEngine> を参照してください。

RoomOS ウェブエンジンの xapi コマンドについては、<https://roomos.cisco.com/xapi/domain/?domain=WebEngine> を参照してください。

10. エンタープライズ ネットワーク セキュリティ

ほとんどの企業では、内部ネットワークとデータを保護し、外部アクセスを制御するために、複数のセキュリティ製品と機能を実装しています。Cisco Collaboration デバイスは、次のエンタープライズ ネットワーク セキュリティ機能、プロトコル、および製品をサポートします。

- VLANs: CDP, 802.1Q
- ネットワークアクセスコントロール (802.1X): EAP-FAST、EAP-TLS
- Wi-Fi セキュリティ: EAP-FAST/TLS/TTLS/PEAP、WPA/WPA2/WPA3 パーソナル/エンタープライズ (CCMP128 準拠)
- NAT/ファイアウォール トラバーサル
- Proxy Server - 認証および TLS 検査

これらのセキュリティ機能については、このドキュメントで概観レベルで説明します。メディア用の Webex IP サブネットおよびサービスへのシグナリング用の URL を含む Webex サービスのエンタープライズ ネットワーク要件の詳細については、[「Webex サービスのネットワーク要件」](#)の記事を参照（およびサブスクライブ）してください。

ファイアウォールとプロキシ トラバーサル

セキュリティを重視する顧客のほとんどは、ファイアウォールとプロキシサーバーの両方を展開して、エンタープライズ ネットワーク内のアプリケーションやデバイスからインターネットおよび Webex などの関連するクラウドサービスへのアクセスを制御します。実装はさまざまですが、図 12 に示すように、一般的な導入では、すべての HTTP/TLS ベースのトラフィックがプロキシサーバーを強制的に経由し、プロキシサーバーから発生した HTTP/TLS トラフィックのみがファイアウォールを通過し、インターネットに到達することを許可します。Cisco ビデオデバイスからの UDP、TCP、TLS ベースのメディアなど、他のトラフィック タイプはファイアウォールを直接通過し、プロキシサーバーには送られません。

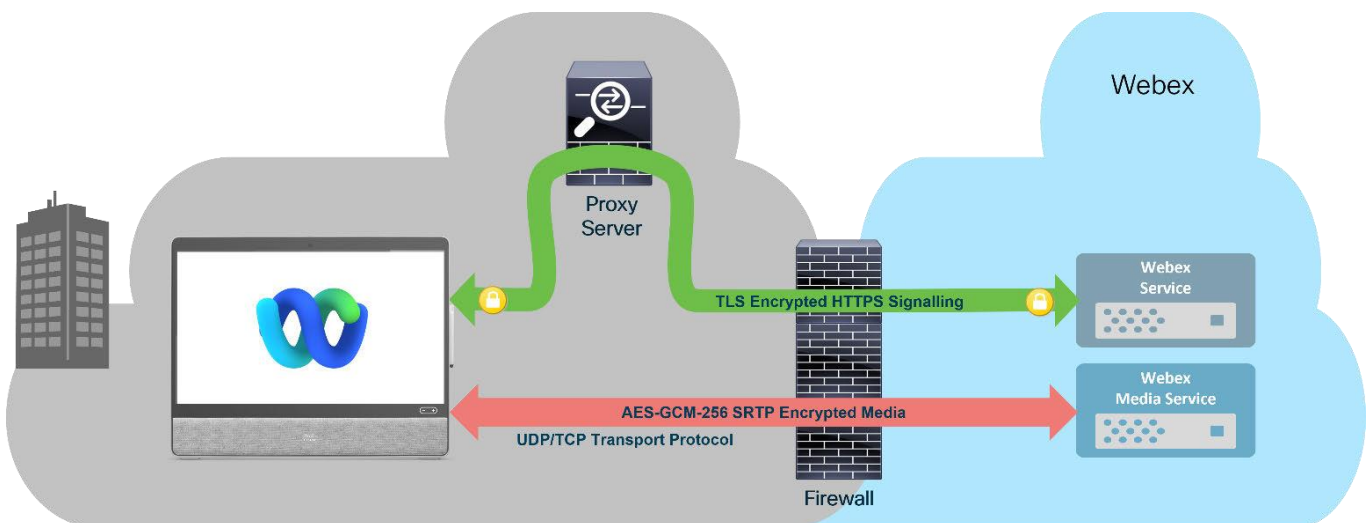


図 12. プロキシおよびファイアウォールデバイスを通る典型的な Webex トラフィックフロー

メモ: すべての Cisco Collaboration ビデオデバイスは、エンタープライズネットワークから Webex サービスへの Outgoing 接続のみを開始します。

HTTP プロキシ トラフィック検査および証明書ピニング

プロキシがサーバーを通過する TLS/HTTPS トラフィックを復号、検査、および再暗号化する、プロキシサーバーによるトラフィック検査は、セキュリティを重視する顧客によって一般的に使用されます。Cisco ビデオデバイスのトラフィックでは、プロキシサーバーによるトラフィック検査の価値が制限されます。トラフィックの解読と検査ではシグナリング情報しか明らかにならないためです。

図 13 に示されているように、プロキシサーバーは Cisco ビデオデバイスに Webex サービス証明書の代わりに、エンタープライズ CA 署名付き証明書を提示します。これにより、プロキシサーバーは Cisco ビデオデバイスとの TLS 接続を直接確立し、TLS トラフィックを解読して検査することができます。同様に、プロキシサーバーと Webex サービス間のトラフィックも暗号化/復号化して検査できます。

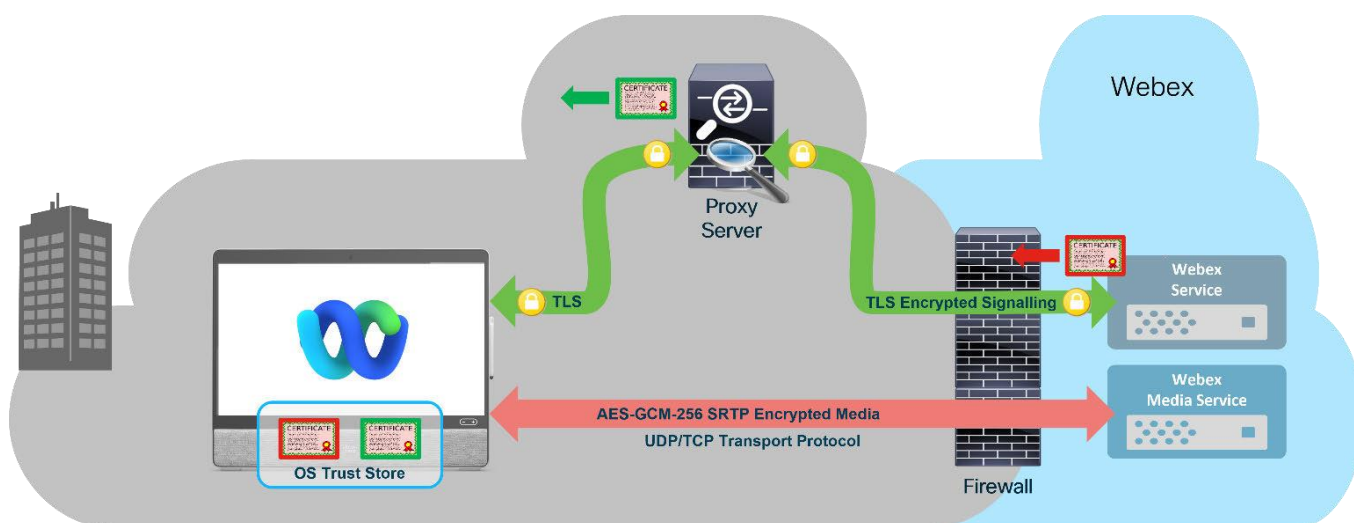


図 13. プロキシサーバーの TLS トラフィック検査

Cisco Collaboration デバイスは、TLS セッションの確立中に証明書を検証し、Webex サービスから発信されたことを確認します。プロキシサーバーによるトラフィック検査では、プロキシによって送信されたエンタープライズ CA の署名付き証明書は、期待されるパブリック CA の署名付き Webex サーバー証明書と一致しません。この場合、Cisco ビデオデバイスは、その信頼ストアでプロキシサーバーから受信した証明書と一致する証明書を検索します。一致する証明書が見つかった場合、ビデオデバイスからプロキシサーバーへの TLS 接続の確立が許可されます。

[「Webex への Cisco ビデオデバイスのオンボーディング」](#) で説明したように、Cisco ビデオデバイスのオンボーディングでは、エンタープライズ CA 証明書のトラストアンカーは、Webex ID サービスからデバイスにダウンロードすることもできます。これにより、エンタープライズ プロキシ サーバーによる Cisco ビデオデバイスのシグナリングトラフィックの TLS 検査が可能になります。顧客は Cisco TAC でサービス リクエストを開き、Webex クラウド アイデンティティ サービスにエンタープライズ CA 証明書をアップロードする必要があります。

11. Cisco Collaboration デバイス: Webex アプリとのペアリング

Webex デスクトップおよびモバイル アプリケーションは、デバイス コントロールとコンテンツ共有のために Cisco Collaboration デバイスとペアリングできます。

Cisco Desk、Board、Room シリーズのデバイスは、超音波信号とトークンを使用して Webex アプリとペアリングします。図 14 では、固有のトークンが 30 秒ごとに Webex クラウドによって生成され、TLS 経由で安全に Cisco Collaboration デバイスに送信されます。Cisco Collaboration デバイスは、超音波信号を使用してデバイススピーカーからトークンを発行します。超音波信号の範囲内にある Webex アプリは、トークンを Webex クラウドサービスに送信することで、受信したトークンを使用して Cisco Desk、Board、または Room シリーズのデバイスとペアリングできます。Cisco Collaboration デバイスと Webex アプリがペアリングされたら、新しく発行されたトークンは、ペアリングされた接続を維持するために、Webex アプリによって受信され、Webex クラウドサービスに送信される必要があります。

デバイスの検出に超音波信号を使用する理由の 1 つは、範囲が限定されていることです。超音波信号は通常壁を通過しないため、ペアリングトークンの範囲は、エンドポイントが配置されている閉じた部屋に制限されます。

Cisco Desk、Board、Room シリーズのデバイスとの自動ペアリングは、超音波の音量を 0 に設定することで無効にできます。

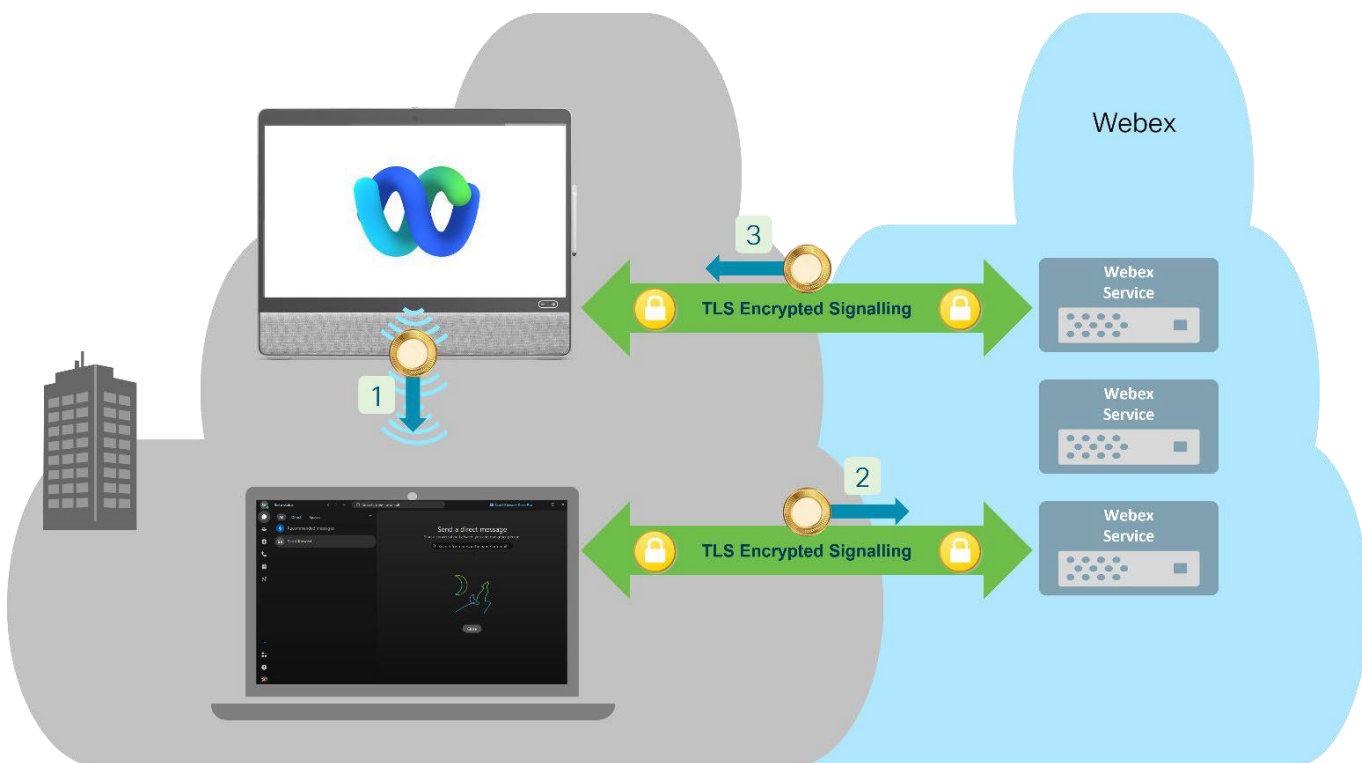


図 14. Webex アプリと Cisco Collaboration 端末間の超音波ペアリング

図 15 は、Cisco Desk、Board、または Room シリーズのデバイスと Webex アプリの間でペアリングされた接続が Webex クラウドを使用して確立されると、Webex アプリは Cisco Collaboration デバイスをコントロールし、発信、ミーティングに参加、コンテンツの共有、デバイスのマイクのミュートなどを行います。Webex アプリと Cisco Collaboration は両方とも、Webex クラウドへの既存の TLS 接続を使用して、コンテンツ共有のためにコール制御シグナリングとメディアを交換します。

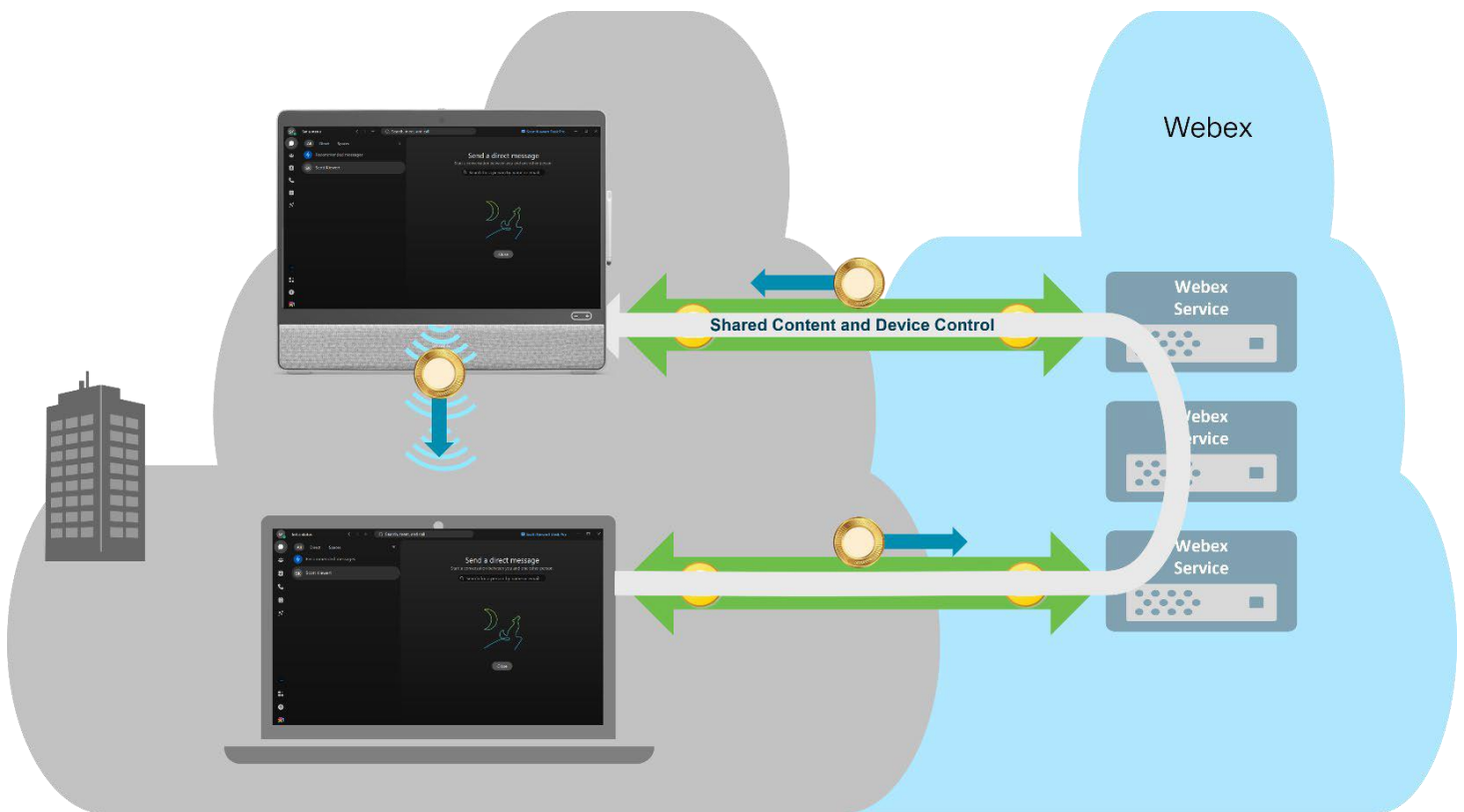


図 15. Webex アプリと Cisco Collaboration 端末間のコンテンツ共有

その他の Cisco Collaboration ビデオデバイス検出メカニズム

Webex アプリは、Wi-Fi を使用して Cisco Desk、Board、および Room シリーズ デバイスを検出し、PIN を使用して手動で接続することもできます。詳細については、次の記事を参照してください。

- [近くの Webex デバイスの検出を管理する](#)
- [Webex アプリ デバイスに接続する](#)

Apple AirPlay を有効にして、iPhone、iPad、Mac などの Apple デバイスで、Webex アプリを必要とせずに、有効な Cisco Collaboration デバイスを検出して共有できるようにすることもできます。

詳細については [AirPlay でワイヤレス共有を設定する](#) の記事を参照してください。デフォルトでは、Apple AirPlay を利用するオプションは無効になっています。エンドユーザーが利用できるようにするには、Control Hub を使用した IT の介入が必要です。

また、Miracast® を有効にして、Windows ベースの PC および一部の Android ベースのモバイル デバイスで、Webex アプリを必要とせずに、有効な Cisco Collaboration デバイスを検出して共有できるようにすることもできます。Miracast をサポートするためには、Cisco Collaboration デバイスを有線ネットワークに接続する必要があります。IT 部門が有効にすると、エンドユーザーは Windows PC/Android モバイル デバイスと Cisco Collaboration デバイス間の Wi-Fi Direct 接続を使用して、通話中および通話外の両方で共有できるようになります。詳細については、[「Miracast® でワイヤレス共有を設定する」](#)の記事を参照してください。デフォルトでは、Miracast 経由で共有する機能は無効になっているため、Control Hub 管理者が有効にする必要があります。

Apple AirPlay および Miracast® の両方を使用するには、RoomOS 11 が Cisco Collaboration デバイスに展開されている必要があります。

12. Cisco Collaboration ビデオデバイスのプライバシー

Webex は、Webex 通話または Webex ミーティングのユーザーエクスペリエンスを向上させる AI 機能の範囲を提供します。

- 周囲のノイズの除去
- 音声の最適化
- ミュージックモード
- ジェスチャー認識
- 顔認証
- 言語インテリジェンス:
 - Webex Assistant
 - クローズドキャプション
 - リアルタイム翻訳
 - ミーティングの議事録
- ルーム解釈
- 人の検知
- 近接通信のペアリング

Cisco ビデオデバイスは、ほとんどの AI 機能で音声とビデオをローカルで処理します。Webex は、ユーザーが通話またはミーティングを行っているときにのみ、クラウドにメディアをストリーミングします。次のいくつかのセクションでは、Webex AI 機能の一部に関する追加情報を提供し、表 2 では、これらの機能を容易にするために、メディアがローカルで処理される、またはクラウドにストリーミングされる場合について説明します。

Webex 音声インテリジェンス：バックグラウンドノイズの除去と音声の最適化

音声インテリジェンスは通話中またはミーティング中にのみ使用され、音声はデバイス上でローカルに処理されます。バックグラウンドノイズリダクションは、キーボードの打鍵音、犬の鳴き声などの不要なノイズを除去します。音声最適化機能は、バックグラウンドで話している人の声を抑制したり、音楽の音声を最適化したりするために使用されます。ユーザーが通話中にマイクをミュートしている場合、デバイスはマイクへのアクセスを維持し、音声をサンプリングして、マイクがミュートされていることをユーザーに通知できるように、話しているかどうかを判断します。デバイスがミュートになっている場合、音声サンプルが Webex クラウドに送信されることはありません。

ジェスチャー認識

ジェスチャー認識は、Webex Meetings とウェビナーでのみ使用されます。Cisco ビデオデバイスは、カメラとオンボードソフトウェアを使用して、ミーティング参加者が挙手、親指を立てたり下げたり、拍手したりしたときにそれを検出します。これらのジェスチャーは、一時的に画面上のアイコンとしてミーティングの参加者に表示されます。この機能の処理はローカルで行われ、メディアはクラウドに送信されません。Cisco Desk シリーズでのジェスチャー認識の使用に関する詳細は、[「Desk シリーズのジェスチャー認識」](#)を参照してください。

顔認証

顔認証は、ミーティング参加者の名前ラベルの作成と表示に使用されます。組織で顔認識が有効になっている場合、Cisco ビデオデバイスはカメラからの画像を使用して、ユーザーの顔を表すベクトル データ セットを作成します。このデータ セットは Webex クラウドの顔認証サービスに送信されます。Cisco ビデオデバイスは、ユーザーがミーティングのアクティブな参加者である場合にのみ、ユーザーの顔を検出しようとし、この機能を有効にした場合は、ユーザーの顔のみを検出して名前ラベルを提供します。顔認証技術がユーザーの画像を顔認証サービスにストリーミングすることはありません。

言語 インテリジェンス

言語インテリジェンスは、Webex Assistant および Webex Meetings の字幕、リアルタイム翻訳、ミーティングの議事録に使用されます。

デバイス用の Webex Assistant は、「OK Webex」または「Hey Webex」のウェイクワードによりアクティベートされます。アクティベートされると、ユーザーは Webex Assistant を口頭で「start meeting (ミーティングを開始)」、「increase volume (音量を上げて)」、「call a number (番号にかけて)」などのコマンドを与えることができます。Webex Assistant の使用時、Cisco ビデオデバイスはローカルで処理されるウェイクワードのみを聞き取ります。デバイスは、Webex クラウドにメディアを継続的にストリーミングしません。ミーティングとウェビナー主催者は、またミーティング中に Webex Assistant をアクティベートすることができます。Webex Assistant が有効になると、デバイスはユーザーの口頭での指示を音声ストリームで Webex クラウドに送信し、解釈と実行を行います。

さらに、ミーティングとウェビナーをよりアクセスしやすくするために、Webex ではユーザーが Webex Assistant を有効にしなくても、字幕をライブで自動化できるようにしています。参加者が発言すると、ミーティングまたはウェビナーのコントロールの上に字幕が表示されます。Webex Assistant も有効になっている場合、上記で説明したように、ユーザーはハイライトを作成したり、音声コマンドを使用したりできます。

Webex Assistant と自動クローズキャプションの比較については、[「Webex Assistant と自動クローズキャプションを比較する」](#)を参照してください。

Webex Meetings は次の目的でも言語インテリジェンスを使用します。

- [複数言語のリアルタイム翻訳](#)
- [ミーティングの音声テキスト](#)

ルーム解釈 - 人数カウント

人数カウントは Cisco ビデオデバイスのカメラとソフトウェアを使用してヘッド検出を行い、結果を Webex クラウドに送信します。Cisco は誰が会議室にいたのかを記録しません。検出された平均人数のみを記録します。必要に応じて、人数カウント機能を通話またはミーティングの外で有効にできます。

人の検知

Cisco ビデオデバイスはスピーカーを使用して超音波オーディオシグニチャを放出し、マイクを使用して返される音の変化を監視します。

超音波ペアリング

Cisco ビデオデバイスは超音波信号を使用して、近くの Webex アプリにビーコンを送信します。これにより、ユーザーはデバイスを Webex アプリとペアリングして、デバイスで発信したり画面を共有したりできます。Webex アプリは、パーソナル コンピューターまたはモバイル デバイスのマイクを使用して、これらの超音波ビーコンを検出します。超音波ペアリングが有効な場合、Webex アプリで使用されるマイクは、ビーコンをリスンするために有効になりますが、音声は Webex クラウドに送信されません。

Wi-Fi ベースのデバイスの検出とペアリング

Wi-Fi ベースのデバイス検出とペアリングにより、Webex アプリは近くにある Cisco ビデオデバイスを操作できるようになります。ミーティングへの参加、発信、画面の共有をデバイス上で行うことができます。

表 2 は上記の Webex の高度なコラボレーション機能の説明、および基本的な設定および操作情報を示します。

表 2. Webex の高度なコラボレーション機能のコントロール

Webex の高度な コラボレーション 機能	サポート元	この機能に対して Webex クラウド に送信される音声 またはビデオ	この機能を設定で きる場所	デフォルト設定
バックグラウンド ノイズ除去	Cisco ビデオデバイス Webex アプリ	なし	エンドユーザー設定	オン
自分の声/すべ ての声に最適化	Cisco ビデオデバイ ス (自分の声) Webex アプリ	なし	エンドユーザー設定	オフ
ミュージック モード	Cisco ビデオデバイス Webex アプリ	なし	エンドユーザー設定	オフ
ジェスチャー認識機能	Cisco ビデオデバイス Webex アプリ	なし	エンドユーザーのミ ーティング中のコン トロール	オフ
顔認証	Cisco ビデオデバイス	なし	Webex 管理者 (組織 のグローバル設定) とエンドユーザーの 設定	組織 : オフ、 ユーザー : オフ
言語インテリジェンス Webex Assistant (WXA)	Cisco ビデオデバイス Webex アプリ	はい - ただし、ウェイ クワードを使用して アクティベートされて いる場合、またはミー ティング中にアクティ ベートされている場合 のみ。	Webex 管理者 (組織 およびサイトの設定) およびエンドユーザ ーのミーティング内 コントロール	サイト: オフ ユーザー: オフ
ランゲージ インテ リジェンス リアル タイム翻訳	Cisco ビデオデバイス Webex アプリ	はい - Webex ミーティ ング中に使用	Webex 管理者 (サイト 設定) およびエンドユ ーザーのミーティング内 コントロール	組織 : オフ、 ユーザー : オフ
言語インテリジェン ス ミーティングの 音声テキスト	Cisco ビデオデバイス Webex アプリ	AI を使用してミー ティングの録画を音 声テキストに変換	Webex 管理者 (組織 のグローバル設定) とエンドユーザーの 設定	組織: オン ユーザー: オン
言語インテリジェン ス クローズドキャ プション	Cisco ビデオデバイス Webex アプリ	はい - Webex ミーティ ング中に使用	Webex 管理者 (組織 のグローバル設定) およびエンドユーザ ーのミーティング内 コントロール	組織 : オン、 ユーザー : オフ

ルーム解釈 - 人数カウント	Cisco ビデオデバイス	なし	Webex 管理者 (組織のグローバル設定)	組織：オフ、 通話中：オフ 通話中以外：オフ
人の検知	Cisco ビデオデバイス	なし	Webex 管理者 (組織のグローバル設定)	組織：オフ
超音波ベースのペアリング	Cisco ビデオデバイス Webex アプリ	なし	Webex 管理者 (組織のグローバル設定) Cisco ビデオデバイス設定 Webex アプリ：エンドユーザーの設定	組織：オン、 デバイス：オン デスクトップアプリ：オン、 モバイルアプリ：オフ
Wi-Fi ベースのペアリング	Cisco ビデオデバイス Webex アプリ (デスクトップのみ)	なし	Cisco ビデオデバイスの設定 Webex アプリ (デスクトップ): エンドユーザーの設定	組織：オン、 デバイス：オン、 アプリ：オン

Cisco Collaboration ビデオデバイス - リモート監視オプション キー

リモート監視機能により、管理者は Cisco Collaboration デバイスのウェブ インターフェイスから会議室を監視することができます。前に説明したリモート サポート アクセス機能と同様に、Cisco Collaboration デバイスのリモート モニタリングは、デバイスがネットワークに到達できる場合（例えば、企業ネットワーク上）にのみ可能です。この機能を有効にするには、デバイス用のオプション キーを購入し、インストールする必要があります。この購入手続きの一環として、この機能を使用するには、購入者は地域の法律および規制を遵守する必要があることが明確になります。リモート監視は、別の場所からビデオデバイスをコントロールする場合に役立ちます。

カメラからのスナップショットがウェブ インターフェイスに表示されるため、会議室にいなくてもカメラ ビューを確認したり、カメラをコントロールしたりできます。有効な場合、スナップショットは約 5 秒ごとに自動的に更新されます。リモート監視は便利な機能を提供しますが、この機能を有効にする前に、地域の法律および規制およびユーザー通知を考慮する必要があります。

リモート監視オプションを有効にする場合は、地域の法律および規制を遵守し、システム管理者がカメラとスクリーンを監視およびコントロールできることをシステムのユーザーに適切に通知する必要があることに注意してください。この機能を使用する場合、適用される法律および規制を遵守することは、組織の管理者の責任です。Cisco は、本機能の不法な使用に対するいかなる責任も負わないものとします。

13. Cisco Collaboration ビデオデバイス - 物理的セキュリティ

Cisco Collaboration ビデオデバイス - 物理ポートとインターフェイスのセキュリティ

Cisco ビデオデバイスは、ミーティングや通話のエクスペリエンスを強化するために、マイク、スピーカー、カメラ、ナビゲーター、PC などの外部デバイスに接続するために使用できるいくつかの物理ポート タイプをサポートしています。

Cisco ビデオデバイスがサポートする音声、ビデオ、およびデータ接続の一般的なインターフェイス タイプには、次のものが含まれます。

- ミニジャック (3.5mm)
- イーサネット
- ユーロブロック (Phoenix)
- USB
- HDMI
- SDI

該当する場合、ビデオ デバイス インターフェイスは、API またはデバイスの WebUI を介して有効または無効にすることができます。Cisco ビデオデバイスの物理的インターフェイスの完全なリストおよび設定オプションについては、製品別のデータシート ([Desk](#) / [Room](#) / [Board](#)) と最新の[コマンドリファレンス](#)を参照してください。

現在の Cisco ビデオデバイスは、ラップトップなどの接続された周辺機器とネットワーク接続を共有する機能を備えていません。詳細については、[「Cisco RoomOS デバイスを介してネットワーク境界の侵害リスクを評価する」](#)を参照してください。

イーサネットポート

一部のビデオデバイスには複数のイーサネットポートがあります。Cisco Desk Pro は、スイッチとして機能する追加のネットワーク ポートを提供します。これにより、デバイスへの単一のイーサネット接続を PC などの別のデバイスと共有できます。Cisco Room シリーズおよび Cisco Board シリーズには、デバイスにローカル ネットワークを提供するだけのイーサネット ポートが 1 つ以上ある場合があります。PC をこれらのターシャリ ネットワークポートの 1 つに接続し、例えば SSH を使用して Cisco Collaboration デバイスにアクセスすることが可能ですが、認証要件は同じままです。

ワイヤレス インターフェイス

最新の Cisco Desk、Room、Board シリーズのビデオデバイスは、以下のワイヤレス インターフェイスも提供します。

- Wi-Fi - 802.11a/b/g/n/ac (2.4 GHz および 5 GHz 帯域)
- Wi-Fi - 802.11ax (6 GHz 帯域) - サポートされているモデルについては、製品データシートを参照してください。
- Bluetooth® 注: ワイヤレスネットワーク接続の使用も柔軟に選択できますが、高いパフォーマンスを得るためにはイーサネット接続が推奨されます。

Cisco Collaboration ビデオデバイスの非無線バージョンは、Wi-Fi および Bluetooth® 無線が制限されている場所での安全な展開に利用できます。

モデル固有のサポート情報については、製品データシートを参照してください ([Desk](#) / [Room](#) / [Board](#)) 。

14. Cisco のセキュリティ モデル

Cisco は、クラウド セキュリティのリーダーであり続けるために、断固として取り組んでいます。Cisco の Security and Trust 組織は、全社のチームと協力して、セキュリティ、信頼、透明性をフレームワークに構築し、コアインフラストラクチャの設計、開発、運用を支えるフレームワークを作り、Cisco のすべてにおいて最高レベルのセキュリティを満たすようにしています。

この組織は、サイバーセキュリティのリスクを軽減し、管理するために必要な情報を顧客に提供することに専念しています。

Webex セキュリティモデル (図 16) は、Cisco のプロセスで深く刻まれているのと同じセキュリティ基盤の上に構築されています。

Webex 組織は、Webex サービスを安全に開発、運用、監視するための基本要素に従っています。

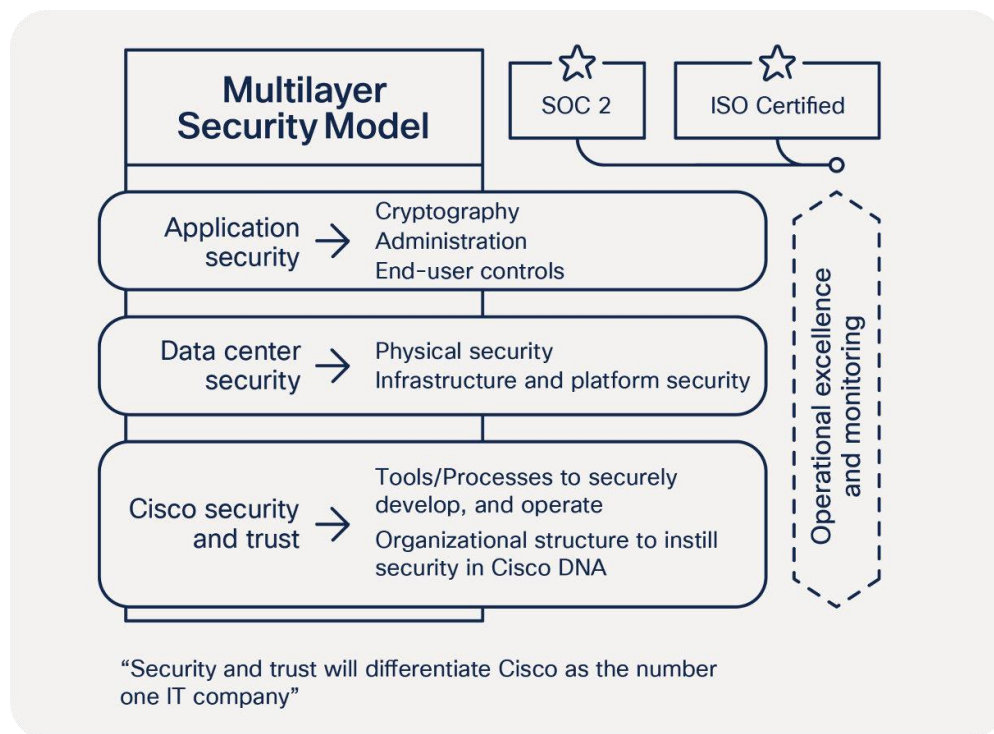


図 16. Webex セキュリティモデル

15. Webex 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

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 はエンドユーザー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 Scoring 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。

16. データプライバシー

Webex は顧客データの保護を重視しています。Cisco は、[Cisco プライバシーステートメント](#) および [Cisco Trustportal](#) で入手できるプライバシーデータシートに従ってのみ顧客情報を収集、使用、処理します。

Webex はプライバシーを考慮して構築されており、EU 一般データ保護規則 (GDPR)、カリフォルニア消費者プライバシー法 (CCPA) / カリフォルニアプライバシー権利法 (CPR) など、国際的なプライバシー要件と一致した方法で使用できるように設計されています。カナダ個人情報保護および電子文書法 (PIPEDA)、個人医療情報保護法 (PHIPA)、医療保険の相互運用性と説明責任に関する法律 (HIPAA)、および家庭教育の権利およびプライバシー法 (FERPA) に準拠しています。

17. 透明度

Webex ユーザーと顧客は、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、ユーザー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、[CiscoTrustportal](#) 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

18. 業界標準と認証

Webex は、厳格な社内基準に準拠するだけでなく、情報セキュリティへの取り組みを示すために、サードパーティによる検証も継続的に維持しています。Webex は次の認証を取得しています:

- ISO 27001、27017、27018、および 27701
- Service Organization Controls (SOC) 2 Type II
- SOC 3
- SCOPE Europe による EU クラウド行動規範の遵守
- CAS CSTAR 2
- クラウド コンピューティング コンプライアンス コントロール カタログ (C5) 証明
- FedRAMP (詳細は <https://cisco.com/go/fedramp> を参照してください)

メモ: FedRAMP 認定の Webex サービスは、米国政府および教育機関の顧客のみが利用できます。

19. 結論

Cisco Collaboration ビデオデバイスを使えば、共同作業を行い、より多くのことをより早く行うことができます。Webex はウェブおよびビデオ会議、メッセージング、通話の分野で信頼される業界リーダーです。Webex は、スケーラブルなアーキテクチャ、一貫した可用性、および社内およびサードパーティの厳格な業界標準に準拠するために検証および継続的に監視されているマルチレイヤー セキュリティを提供します。Cisco はすべてをより安全に接続し、あらゆることを可能にします。

20. 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るには、[「Cisco 製品の購入のご案内」](#)をご覧ください。

21. 詳細情報

[Cisco Collaboration ビデオデバイス](#)