ホワイトペーパー

Webex Meetings のセキュリティ

webex by CISCO

目次

はじめに

Webex Meetings は、世界中の従業員と仮想チームが同じ部屋で作業を行っているかのような、リアルタイムのコラボレーションを実現します。各国の企業、組織、政府機関が Webex Meetings を活用しています。ビジネス プロセスを簡素化し、営業、マーケティング、トレーニング、プロジェクト管理、およびサポート チームの成果を向上させるために役立ってきました。

このような企業や組織のすべてにおいて、セキュリティは基本的な関心事項となっています。オンライン コラボレーションでは、ミーティングのスケジュール設定から参加者の認証、ドキュメントの共有にいたる多様なタスクに対して、複数のレベルのセキュリティを備える必要があります。

シスコは、セキュリティをネットワーク、プラットフォーム、およびアプリケーションの設計、開発、導入、メンテナンスにおける最優先事項に位置付け、最も厳しいセキュリティ要件が設けられている場合でも、Webex Meetings ソリューションなら自信を持ってビジネスプロセスに組み込むことができます。

本書では、重要な投資決定を行う際に役立つ、Webex Meetings およびその基盤となるインフラストラクチャのセキュリティ対策の詳細について説明します。

このドキュメントの内容

本書では、Webex Meetings スイートのセキュリティ機能について説明します。また、お客様が安心して Webex でコラボレーションできるように支援するツール、プロセス、エンジニアリングについても説明します。

Webex Meetings には、以下が含まれています。

- Webex Meetings
- Webex Webinars[1]
- Webex Training
- Webex Support
- Webex Edge
- Webex Cloud Connected Audio
- Webex Assistant
- Slido（投票機能）[2]

Webex セキュリティモデル

シスコはクラウド セキュリティにおけるリーダーシップを維持すべく取り組んでいます。シスコの Security and Trust 部門は社内全体のチームと連携し、コア インフラストラクチャの設計、開発、運用をサポートするフレームワークにセキュリティ、信頼性、および透過性を提供します。これにより、すべての業務で最高レベルのセキュリティを実現しています。

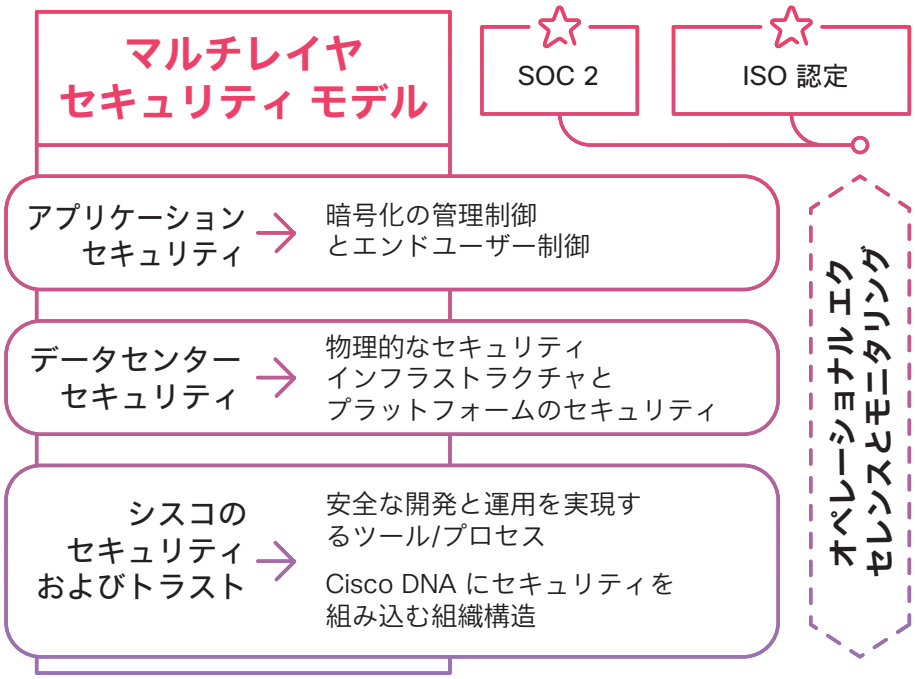
また、サイバーセキュリティのリスクを軽減し、管理するために必要な情報をお客様に提供することにも取り組んでいます。

Webex のセキュリティモデル（図 1）は、このようにシスコのプロセスに深く刻み込まれたセキュリティ基盤を土台としています。

Webex 部門は、一貫してこの基盤に基づき、Webex サービスを安全に開発、運用、モニタリングします。本書ではこれらの要素の一部について説明します。

[1] 旧 Webex Events

[2] Slido のセキュリティの情報については、Webex の Slido（投票機能）のセキュリティに関するホワイトペーパー（cisco.com/content/dam/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/esp/Slido-in-Webex-Security-Paper_1-0.pdf）を参照してください。



「セキュリティと信頼性がシスコをトップの IT 企業として差別化」

図 1. Webex セキュリティモデル

シスコのセキュリティおよびトラスト

シスコのセキュリティ ツールおよびプロセス

シスコのセキュアな開発ライフサイクル

シスコでは、セキュリティを補完的なものではなく、世界クラスの製品やサービスをゼロから構築して提供するための統制のとれたアプローチとして採用しています。すべての Cisco® 製品開発チームは、Cisco Secure Development Lifecycle に従う必要があります。これはシスコ製品の復元力と信頼性を向上させるための、反復可能で測定可能なプロセスです。開発ライフサイクルのすべての段階に導入されたツール、プロセス、認識トレーニングの組み合わせにより、徹底的な防御が保証されます。また、製品の復元力に対する包括的なアプローチが実現します。Webex 製品開発チームは、製品開発のあらゆる側面でこのライフサイクルに積極的に従います。

セキュアな開発ライフサイクルの詳細については、以下を参照してください。

シスコの基盤となるセキュリティ ツール

Cisco Security and Trust 部門は、セキュリティに関してすべての開発者が一貫した判断を下すために必要なプロセスとツールを提供します。

このようなツールを構築して提供する専門チームがいると、製品開発プロセスにおける不安定性が解消されます。

以下に、ツールの例を示します。

- 製品が準拠する必要がある製品セキュリティベースライン（PSB）の要件
- 脅威モデリングで使用される脅威ビルダーツール
- コーディングのガイドライン
- 開発者が独自のセキュリティコードを作成する代わりに使用できる検証済みまたは認定済みライブラリ
- セキュリティの欠陥をテストするために開発後に使用できるセキュリティ脆弱性テストツール（静的および動的解析用）
- シスコおよびサードパーティのライブラリをモニタリングし、脆弱性が検出されると製品チームに通知するソフトウェアトラッキング

シスコのプロセスにセキュリティを組み込む組織構造

シスコには、企業全体にセキュリティプロセスを組み込み、管理する専門の部門があります。セキュリティに対する脅威や課題の最新情報を常に把握するために、シスコは以下を活用しています。

- シスコ情報セキュリティ（InfoSec）クラウドチーム
- Cisco Product Security Incident Response Team（PSIRT; プロダクト セキュリティ インシデント レスポンス チーム）
- セキュリティに関する責任の共有

Cisco InfoSec Cloud

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、お客様に安全な Webex 環境を提供する責任を担っています。InfoSec では、セキュリティのプロセスおよびツールを定義し、Webex のお客様への提供に関与するすべての部門にそれを適用することで、安全な Webex 環境を提供しています。

さらに、Cisco InfoSec Cloud はシスコの他のチームと連携し、Webex サービスに対するあらゆるセキュリティ上の脅威に対応します。

また、Cisco InfoSec は、Webex のセキュリティ態勢における継続的な改善に対しても責任を負っています。

Cisco Product Security Incident Response Team (PSIRT)

Cisco PSIRT は、シスコの製品とサービスに関係するセキュリティの問題の流入、調査、およびレポートを管理する専門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、さまざまなメディアを使用して情報を公開します。 レポートのタイプは、 次の条件によって異なります。

- 脆弱性に対処するためのソフトウェアのパッチまたは回避策があるか、重大度の高い脆弱性に対応するためにコード修正の公開がその後予定されている。
- お客様に大きなリスクをもたらす可能性がある脆弱性のアクティブな不正利用を PSIRT が確認した。 この場合、PSIRT は、 パッチを完全には公開せずに、脆弱性について説明するセキュリティ情報の公開を早急に行う可能性があります。
- シスコ製品に影響を与える脆弱性が一般的に認識されると、お客様に大きなリスクをもたらす可能性がある。 この場合も、PSIRT はパッチを完全には公開せずに、お客様にアラートを通知する可能性があります。

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の対策を講じるために必要となる最低限の情報を公開します。PSIRT は共通脆弱性評価システム（CVSS）のスケールを使用し、発見された問題の重大度をランク付けします。PSIRT は、エクスプロイトの作成に役立つような脆弱性の詳細情報は提供しません。

PSIRT の詳細については、 こちらをご覧ください。

セキュリティに関する責任

Webex グループの全員にセキュリティに対する責任がありますが、その主な役割は次のとおりです。

- 最高セキュリティ責任者 : クラウド
- バイスプレジデントおよびゼネラルマネージャ : シスコ クラウド コラボレーション 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、シスコ クラウド コラボレーション アプリケーション
- バイスプレジデント : 製品管理、シスコ クラウド コラボレーション 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 グループは、内部の評価者による厳格なペネトレーションテストを定期的に行います。独自に設けた厳しい社内手順だけでなく、Cisco InfoSec では、独立した複数のサードパーティに、シスコの社内ポリシー、手順、およびアプリケーションに対する厳格な監査の実施を依頼しています。これらの監査は、商用および政府機関向けのアプリケーションの両方について、ミッションクリティカルなセキュリティ要件を確認することを目的としています。また、シスコはサードパーティベンダーを通じて、継続的かつ詳細な、コードによるペネトレーションテストとサービス評価を実施しています。この取り組みの一環として、サードパーティは次のようなセキュリティ評価を行っています。

- 重要なアプリケーションとサービスの脆弱性の特定、およびソリューションの提案
- アーキテクチャの改善に関する一般的な分野の推奨
- コーディングのエラーの特定、およびコーディングのプラクティスの改善に関するアドバイスの提供

サードパーティの評価者は Webex のエンジニアリングスタッフと直接連携して、評価結果について説明し、改善策を検証します。必要に応じて、Cisco InfoSec はこれらのベンダーからの証明書を提供できます。

Webex データセンターのセキュリティ

Webex は、業界をリードするパフォーマンス、統合性、柔軟性、拡張性、および可用性を備えた非常に安全なサービス配信プラットフォームである Webex クラウドを通じて配信される Software as a Service（SaaS）ソリューションです。Webex クラウドは、リアルタイムの Web 通信専用の通信インフラストラクチャです。

Webex ミーティングセッションは、世界中の複数のデータセンターにあるスイッチング機器を使用します。Webex クラウドサービスの大半にはシスコのデータセンターが使用されていますが、プライベート クラウド インスタンスに追加のサービスを提供するために、SOC2 や ISO に準拠している Amazon Web Services（AWS）と Microsoft Azure データセンターも使用されています。これらのデータセンターは、主要なインターネット アクセス ポイントの近くに戦略的に配置され、専用の高帯域幅ファイバを使用して世界中のトラフィックをルーティングします。

さらに、シスコはバックボーン接続、インターネットピアリング、グローバルサイトのバックアップ、およびエンドユーザのパフォーマンスと可用性を向上させるためのキャッシング技術を支える、ネットワークのポイントオブプレゼンス（PoP）ロケーションを運用しています。

物理的セキュリティ

データセンターの物理セキュリティには、施設や建物のビデオ監視や、入室の際の二要素認証の実施などが含まれます。シスコ データセンターでは、アクセスはバッジ リーダーと生体認証制御を組み合わせることによって制御されます。さらに、環境制御(温度センサーや消火システムなど)およびサービス継続インフラストラクチャ(電源バックアップなど)は、システムが中断することなく動作するために役立ちます。

データセンターサーバーは、インフラストラクチャの機密度に基づいて「信頼ゾーン」にセグメント化されます。たとえば、データベースは「厳重に保護」されていて、ネットワーク インフラストラクチャには専用の部屋があり、すべての装置ラックはロックされています。シスコのセキュリティ担当者、およびシスコの担当者が同伴する承認済みの訪問者だけがデータセンターに入ることができます。

シスコの実稼働ネットワークは信頼性の高いネットワークであり、信頼レベルの高い少数の人物だけがネットワークにアクセスできます。

インフラストラクチャとプラットフォームのセキュリティ

プラットフォームのセキュリティには、ネットワーク、システム、および Webex データセンター全体のセキュリティが含まれています。すべてのシステムに対して、本番環境への導入前に、徹底したセキュリティの確認と受け入れ検証が行われます。さらに、定期的かつ継続的なハードニング、セキュリティパッチング、および脆弱性のスキャンと評価も実施されています。

サーバは、国立標準技術研究所(NIST)によって発行されたセキュリティ技術の実装に関するガイドライン(STIG)を使用してハードニングされます。ファイアウォールはネットワーク周辺を保護します。Access Control List(ACL; アクセス コントロール リスト)は、異なるセキュリティ ゾーンを分離します。侵入検知システム(IDS)が配置されており、アクティビティが継続的に署名され、モニタリングされます。Webex によって、日単位で内外のセキュリティスキャンが行われます。すべてのシステムに対して、定期メンテナンスの一環としてハードニングおよびパッチングが行われます。さらに、脆弱性のスキャンと評価が継続的に行われます。

サービスの継続性とディザスタ リカバリは、セキュリティ計画の重要な要素です。シスコデータセンターのグローバル サイト バックアップと可用性に優れた設計により、Webex サービスの地理的なフェールオーバーが可能になります。シングルポイント障害は発生しません。

Webex アプリケーションのセキュリティ

暗号化

送信中データの暗号化

クラウドに登録されている Webex アプリ、Webex デバイス、および Webex サービス間の通信はすべて、暗号化されたチャネルで行われます。Webex はバージョン 1.2 以降の TLS プロトコルと強力な暗号スイートをシグナリングに使用します。

TLS を通じてセッションが確立されると、すべてのメディアストリーム（音声 VoIP、ビデオ、画面共有、およびドキュメントの共有）が暗号化されます [3]。

暗号化されたメディアは、UDP、TCP、または TLS で転送できます。シスコでは、Webex 用の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には UDP の使用を推奨しています。これは、TCP と TLS が接続指向のトランスポートプロトコルであり、正しく並べられたデータを確実に上位層のプロトコルに渡すように設計されているためです。TCP や TLS を使用すると、送信側は確認応答がとれるまで欠損パケットを送り直し、受信側は欠損パケットが元の状態に戻るまでパケットストリームをバッファリングすることになります。この挙動により TCP や TLS を介したメディアストリームでは遅延やジッターが増加し、コールの参加者が体感するメディア品質に影響します。

メディアパケットは、AES 256 または AES 128 ベースの暗号を使用して暗号化されます。Webex アプリと Webex Room デバイスは、AES-256-GCM を使用してメディアを暗号化します。これらのメディア暗号化キーは、TLS で保護されているシグナリングチャネルを介して交換されます。SRTP によるメディア暗号化に対応している SIP および H323 デバイスは、AES-256-GCM、AES-128-GCM、AES-CM-128-HMAC-SHA1 を使用できます（AES-256-GCM は Webex がメディアを暗号化するための優先暗号です）。

Webex Meetings のゼロトラストセキュリティに基づくエンドツーエンド暗号化

デバイスとサービスが SRTP を使用してホップバイホップでメディアを暗号化する標準的な会議の場合、Webex メディアサーバは SRTP の各コールレッグのメディアを復号するために、メディア暗号化キーにアクセスする必要があります。このことは SIP、H323、PSTN、録音サービス、SRTP を使用するその他のサービスをサポートする、すべての会議プロバイダーに当てはまります。

[3] SIP および H323 ベースのエンドポイントで Webex 会議に接続する場合は、暗号化されていないトラフィックがインターネットを通るのを避けるため、エンタープライズ ネットワーク エッジのエンドポイントである Expressway または SBC から発信されるすべてのメディアおよびシグナリングストリームを暗号化することを強く推奨しています。

ただし、より高いレベルのセキュリティを必要とする企業に対して、Webex は Meetings のエンドツーエンド暗号化も提供します。このオプションを使用すると、Webex クラウドは会議参加者が使用する暗号キーにアクセスできず、メディアストリームを復号できません。Webex のゼロトラストセキュリティに基づくエンドツーエンド暗号化では、標準的な追跡プロトコルを使用して共有会議暗号化キー（Messaging Layer Security（MLS））が生成され、そのキーによって会議コンテンツが暗号化されます（Secure Frame（S-Frame））。MLS では、会議暗号化キーは各参加者の Webex アプリまたはデバイスで生成されます。その際には、すべての参加者が共有する公開キーと参加者の（非共有の）秘密キーの組み合わせが使用されます。会議暗号化キーはクラウドに送信されず、参加者が会議に参加して退席するたびにローテーションされます。ゼロトラストセキュリティに基づくエンドツーエンド暗号化の詳細については、Webex のゼロトラストセキュリティに関するホワイトペーパーを参照してください。

エンドツーエンド暗号化により、Webex アプリと Webex デバイスで生成されるすべての会議データ（音声、ビデオ、チャットなど）は、ローカルで取得された会議暗号化キーで暗号化されます。このようにして暗号化されたデータは、Webex サービスで復号できません。

Webex Meetings では、エンドツーエンド暗号化が適用された会議タイプを使用できます。エンドツーエンド暗号化を有効にすると、コンテンツの復号に会議キーを必要とする Webex サービスやエンドポイント（暗号化がホップごとに行われる SRTP を使用したデバイスなど）はサポートされません。したがって、会議に参加できるのは、Webex アプリまたはクラウドに登録済みの Webex デバイスを使用している参加者のみとなります。ネットワークベースの録音、音声認識などのサービスは利用できません。

サポート対象の機能とサポート対象外の機能の詳細については、Webex Meetings の本人確認によるエンドツーエンド暗号化を参照してください。

Webex のプライベート会議

組織のネットワークにビデオメッシュがある場合、管理者はアカウント担当者に連絡してプライベート会議を有効にできます。この機能は、お客様の構内でメディアを終端させることで会議のセキュリティを強化します。プライベート会議のスケジュールを設定すると、メディアは常にクラウドカスケードを使用しない企業のネットワーク内のビデオメッシュノードで終端します。

Webex のプライベート会議と Webex Edge Video Mesh の設計ガイダンスの詳細については、こちらをクリックしてください。

暗号化された Webex シグナリング

Webex サービスは TLS バージョン 1.2 以降をサポートしています。通信のセキュリティを確保する TLS バージョン 1.2 の暗号スイートの優先順位は、以下のとおりです。Webex サービスでは、お客様の環境に最適な暗号が選択されます。

一般的な暗号スイートと各スイートのビット長の概要を表 1 に示します。

表 1. 暗号スイートとビット長

暗号スイート	ビット長
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	128
TLS_RSA_WITH_AES_256_GCM_SHA384	256
TLS_RSA_WITH_AES_128_GCM_SHA256	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	128

Webex Cloud に保存されている会議コンテンツの保護

Webex サービスを使用すると、会議の記録とトランスクリプトを Webex クラウドに安全に保存できます。これらのファイルは個別に暗号化され、お客様のリージョンで保管されます。

会議の記録とトランスクリプトは、AES-256-GCM 暗号化方式で暗号化されます。これらのファイルは、Webex Spaces で共有されるファイルやメッセージと同じように保護されます。

- Webex 会議ごとに一意の AES-256-GCM 暗号化キーを持つ（Webex スペースのような）会議コンテナが作成されます。
- 会議の記録が暗号化されて Webex クラウドに保存されると、ファイルの暗号化に使用されたキーと暗号化されたファイルの保管場所の URL を含むメッセージが会議コンテナに追加されます。このメッセージは、会議コンテナの暗号化キーを使用して暗号化されます。
- 会議コンテナにアクセスする権限のあるユーザーは、ファイルの保管場所とファイル暗号化キーを含む暗号化されたメッセージを取得し、会議コンテナの暗号化キーを使用してこのメッセージを復号することにより、記録とトランスクリプトを取得できます。

会議コンテナは、Webex Messagings と同じキー管理システム（KMS）を使用します。これにより、Webex Meetings サービスを使用する組織は、ハイブリッド データ セキュリティ（オンプレミス KMS）サービスと Bring Your Own Key（BYOK）サービスを展開し、さらにセキュアな暗号化キーの保存と保護を実現できます。

会議の記録とトランスクリプトの保存、アクセス、削除

管理者は、Control Hub に保存された会議コンテンツの保持期間を定義できます。保持期間に達すると、保存されたコンテンツは Webex クラウドから削除されます。記録は、Webex Recordings API を使用して一覧表示、エクスポート、削除することもできます。詳細はこちらをご覧ください。

Webex クラウドに保存される記録とトランスクリプトには、次のような特徴があります。

- パスワードで保護される（パスワードは SHA-2（一方向のハッシュアルゴリズム）とソルトを使用して保存される）。
- サインインユーザーのみに制限される。
- ダウンロードできない。
- コンテンツオーナーによって Webex ページや Webex アプリから管理される。

管理者は、ユーザーが各自のコンピュータで会議を記録できるようにすることも可能です。

Webex Meetings – ロビー制御と検証済みアイデンティティ

Webex Meetings のロビーでは、会議の主催者（と共同主催者）は、会議への参加を許可する前にユーザーの審査と管理を行うことができます。会議ロビーのユーザーは、次の 3 つのカテゴリにグループ化されて管理されます（図 2）。

1. 組織内のサインイン（認証済み）ユーザー
2. 組織外のサインイン（認証済み）ユーザー
3. 未認証ユーザー – 本人確認されていない未認証のゲストユーザー

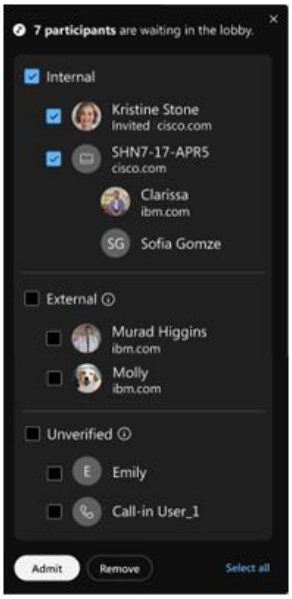


図 2. Webex Meetings のロビー

会議の進行中、Webex アプリまたは Webex デバイスを使用している会議の主催者（と共同主催者）には、ロビーの新規ユーザーについて通知するメッセージが表示されます。主催者（と共同主催者）は、それらのユーザーを会議に参加させるのか、会議とロビーから退出させるのかを選択します（図 3）。

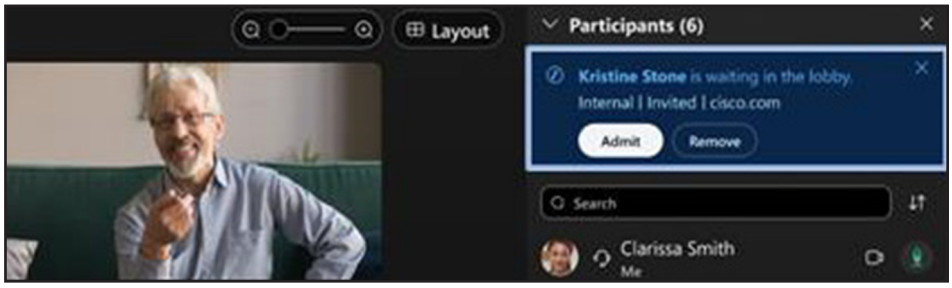


図 3. ロビーの通知

Webex のロールベースのアクセス

Webex アプリケーションの動作は、それぞれが異なる権限を付与されている 5 つのロールを中心にゼロから構築されます。以下に概要を説明します。

主催者

Webex ミーティングのスケジュールを設定し、ミーティングを開始します。会議のエクスペリエンスをすべての人に合わせて制御し、会議のスケジュール中または会議中に、関連する意思決定を行います。

サイト管理者(ロールについては後ほど説明)は、これらの制御の多くを強制できます。これらが強制されていない場合、主催者は会議をセキュリティ保護する方法を選択できます。

共同主催者 (Webex Meetings および Webex Webinars のみ)

会議主催者は、スケジューリングや会議の際に、主催者と同様の権限を付与した共同主催者を割り当てることができます。共同主催者は会議の生産性向上に効果的な役割です。主催者が開始時間に遅れていたり、出席できなかったりした場合に、共同主催者が会議を開始して管理を代行できます。主催者の補助役として会議の管理に関与できるため、大規模な会議の場合にも有効です。

プレゼンタ

プレゼンタは、プレゼンテーション、特定のアプリケーション、またはデスクトップ全体を共有でき、注釈ツールを制御します。セキュリティ面については、プレゼンタは各参加者に共有アプリケーションおよびデスクトップのリモート制御を許可したり、許可を取り消したりできます。

パネリスト (Webex Training および Webex Webinars のみ)

パネリストは主に、主催者とプレゼンタによるスムーズなイベント実行を支援する責任を持ちます。パネリストは、主催者がスケジュールの設定中に割り当てるか、イベント中に出席者リストから昇格させることができます。主催者はパネリストに対して、各分野の専門家として Q&A セッションで参加者の質問を確認して回答したり、パブリックとプライベートのチャットメッセージに応答したり、共有コンテンツに注釈を付けたり、投票のコーディネータとして Webex ネイティブの投票機能を管理したりするように求めることができます。

参加者

参加者には、プレゼンタまたは主催者のロールを割り当てられていない限り、セキュリティに関する責任や権限はありません。

最終的に、サイト管理者と主催者は、会議中いつでも参加者に Webex のボール (プレゼンタのロール) を渡すことができます。この設定はデフォルトでオフになっています。

通訳者（Webex Meetings および Webex Webinars のみ）

通訳者は、発言者の言語を同時通訳機能用の別の音声チャネルで主催者が割り当てた言語に通訳する責任を負います。主催者は、スケジュールの設定中か会議中に通訳を割り当てることができます。

サイト管理者

このロールには、アカウントの管理だけでなく、サイト単位またはユーザ単位でのポリシーの管理と適用の権限が付与されます。管理者は他のすべてのロールおよびユーザが使用できる Webex の機能を選択できます。

シングルサインオン

Webex は、セキュリティ アサーション マークアップ言語(SAML)2.0 プロトコルベースのシングルサインオン（SSO）を使用した、アイデンティティ プロバイダーによるユーザー認証をサポートしています。SSO により、ユーザーは組織内の Webex アプリをはじめとするアプリケーションで単一の共通のログイン情報セットを使用できます。Webex アプリは、Webex サービスを使用して Webex アイデンティティサービスと通信します。Webex アイデンティティサービスは IdP との契約を作成し、Webex アプリが IdP で認証を行えるようにします。IdP の例としては、Microsoft Active Directory フェデレーションサービス、PingFederate、CA SiteMinder シングルサインオン、OpenAM、Oracle Access Manager などがあります。

SSO を有効にするには、組織の証明書を生成する必要があります。こうした証明書は、Webex によって署名された自己署名証明書の場合もあれば、公的認証局(CA)によって署名された証明書の場合もあります。次に、IdP と Webex 間でメタデータを交換する必要があります。

ユーザーが Webex アプリを介して認証を行うと、Webex アイデンティティサービスから Webex アプリ経由で IdP にリクエストが送信され、Webex アプリ経由で IdP から Webex アイデンティティサービスに SAML アサーションが返されます。

Webex でシングルサインオンを導入することで、企業ポリシーに合わせてユーザとアクセス管理を完全に制御できます。お使いの IdP で SSO を使用することには次のような利点があります。

- IdP はユーザーのログイン情報（証明書やフィンガープリントなど）を検証するための機関として機能する。
- Webex はユーザーのログイン情報を保存しない。
- 誰が Webex サービスにアクセスするのかをお客様が制御できる。

詳細については、こちらの Control Hub でのシングルサインオン統合に関する Webex のヘルプ記事を参照してください。

ディレクトリ内のユーザーの場合、Webex は、Active Directory を備えた Directory Connector、または Azure AD か Okta を備えた System for Cross-domain Identity Management（SCIM）API を使用して、サポート対象のディレクトリからユーザーを Webex アイデンティティに同期できます。これにより、ユーザーはディレクトリと Webex 組織間で常に同期されます。ユーザーがディレクトリで作成、更新、または削除されるたびに変更が同期され、Control Hub に反映されます。

Cisco Directory Connector を使用した Active Directory と Webex 間のユーザー同期の詳細については、Cisco Directory Connector の導入ガイドを参照してください。

SCIM API を使用した Azure AD と Webex 間のユーザー同期の詳細については、ヘルプ記事『Azure Active Directory ユーザーを Control Hub に同期させる』を参照してください。

SCIM API を使用した Okta と Webex 間のユーザー同期の詳細については、ヘルプ記事『Okta ユーザーを Cisco Webex Control Hub に同期する』を参照してください。

ミーティングでの設定

Webex Meetings の詳細な設定を使用して、会議前、会議中、および会議後のユーザとシステムの動作を管理できます。一般的には、これらの設定をサイトレベルで適用することで会議を個別に動作させ、すべてのユーザーが必要とするユースケースに整合させることができます。Webex 管理者は、すべての会議のセキュリティを確保し、対象のユーザーとデバイスだけがそれらの会議にアクセスできるようにする必要があります。また、管理者はセキュリティポリシーを適用し、承認済みのユーザーだけが会議コンテンツにアクセスできるようにする必要もあります。管理者がセキュアな会議を実現するためのベストプラクティスについては、ヘルプ記事『Webex で安全なミーティングを行うためのベストプラクティス : サイト管理』と『Webex で安全なミーティングを行うためのベストプラクティス : Control Hub』を参照してください。

会議の主催者は、会議の設定方法を完全に制御し、対象の招待者だけが会議に参加できるようにする必要があります。また、主催者は組織のセキュリティポリシーに従って会議のスケジュールを設定する必要もあります。主催者として Webex Meetings を安全に保つ方法については、ヘルプ記事『ミーティングをセキュアにするための Webex ベストプラクティス : 主催者』を参照してください。

セキュリティポリシーによっては、組織が外部の会議に一切参加させないようにユーザーをブロックしたり、承認済みの外部サイトのリストに記載されている会議への参加だけをユーザーに許可したりする場合があります。さらに、ユーザーが外部の会議に参加するときに、組織がチャット、ファイル転送、注釈、Q&A、投票といった特定の会議内機能の使用を制限することもあります。これらの機能は、Webex のコラボレーションを制限することで使用できます。詳細については、ヘルプ記事『Control Hub 内の Webex Meetings のコラボレーション制限』を参照してください。

その他の Webex の機能とセキュリティ

ユーザーは、各種のクライアントとデバイスを柔軟に使用して Webex 会議に参加したり、Webex 会議を開始したりできます。ビデオデバイスを使用して会議に参加するか会議を開始すると、会議の参加者は、会議のビデオアドレスにダイヤルして、Webex デバイス（Cisco Unified CM 登録（SIP）デバイスか Webex クラウド登録（HTTP）デバイス）やサードパーティの標準ベース（SIP か H.323）のビデオデバイスまたはアプリケーションを使用できます。Unified CM に登録されたデバイスを使用して Expressway 経由で Webex に接続した場合、Expressway-E と Webex 間の SIP シグナリングは、暗号化されない場合もあれば（TCP）、暗号化される場合もあります（TLS または MTLS）。Webex クラウドと Expressway-E 間で交換される証明書は、接続を続行する前に検証できるため、MTLS で暗号化された SIP シグナリングが優先されます。SIP か TLS を使用すると、Webex クラウドのメディアストリームは SRTP によって暗号化されます。

Webex デバイスがあれば、Webex アプリユーザーはプロキシミティ機能を使用して Webex Room デバイスを会議とペアリングしたり、Webex Room デバイスで会議に参加したりすることもできます。詳細については、こちらをクリックしてください。

また、ビデオデバイスを使用して会議に参加するときに数字のパスコード（音声 PIN）を要求するようにサイトを設定できます。

ユーザーは、Webex デバイスから Microsoft Teams 会議に参加することもできます。Webex Video Integration with Microsoft Teams（VIMT）により、クラウドかオンプレミスのいずれかに登録されているシスコと SIP 対応のビデオデバイスから Microsoft Teams 会議に参加できます。この統合により、サードパーティとの相互運用性を必要としない、リッチでシームレスな会議のエクスペリエンスが実現します。ビデオ統合通話のメディアパスは、Webex クラウドの専用のメディアクラスタで処理されます。Webex Video Integration with Microsoft Teams（VIMT）の詳細については、こちらの記事を参照してください。

もう 1 つのビデオエンドポイント統合は、Microsoft の B2B 会議に参加できる Webex Web エンジン対応デバイスとの統合です。この統合は、外部の組織が VIMT を使用していない場合などに利用できます。この統合により、シグナリングとメディアは WebRTC ストリームを介して送信されます。

またユーザーは、Webex デバイスから Google Meet 会議に参加することもできます。Webex と Google Meet の統合により、メディアとシグナリングが Google のクラウドから Webex デバイスに直接送信されて WebRTC テクノロジーが活用されるようになり、Webex デバイスから Google Meet への参加が可能になります。その逆もまた同じにように、Google Meet デバイスでは、使い慣れた Google Meet の UI と通話コントロールを使用して、Webex 会議のエクスペリエンスで Webex Meetings に参加できます。

Webex Meetings の音声プラン

Webex は、お客様の既存の通話ソリューションを活用する構内ベースのシステムから、承認済みの Cloud Connected Calling プロバイダー（CCPP）、Cloud Connected Audio Service プロバイダー（CCA-SP）、BYoPSTN、Cisco PSTN までの通話プランを統合しました。

Cisco PSTN は、Webex Meetings、Webinars、および Training の参加者が利用できる、公衆電話交換網（PSTN）を介した非常に広範な世界規模のダイヤルインサービスとコールミーサービスを提供します。Webex 製品で利用できる音声オプションは、完全統合型のエクスペリエンスによって参加者間のやり取りを効率化します。クラウドベースの PSTN 音声オプションである Webex Meetings Audio は、有料ダイヤルイン、無料ダイヤルイン、およびコールミー機能をローカル接続とグローバル接続の両方で広範囲に提供します。また、携帯電話、IP フォン、ソフトフォンなどのさまざまなデバイスに対応します。つまりテレフォニーからだけでなく、Voice over IP（VoIP）からも同じセッションに参加できます。Cisco PSTN は、Webex が販売されているすべての場所で利用できます。

Webex Cloud Connected PSTN（CCP）は、Webex のエンタープライズグレードの通話機能を提供するクラウドサービスです。このプラットフォームは、100 以上のユーザー市場セグメントで必要とされている、通話、メッセージング、会議、およびコンタクトセンターのワークロードに対応する包括的な Webex Suite に含まれています。Webex は「Bring Your Own Carrier」モデルをサポートしており、お客様はローカルゲートウェイを展開することで PSTN サービスに任意のキャリアを使用できます。CCP により、お客様は PSTN アクセスに認定 CCP プロバイダーを使用できます。シスコは認定 PSTN プロバイダーと相互接続することにより、Webex ユーザーがクラウドで経済的かつ信頼性の高い PSTN を使用できるようにします。構内ベースのゲートウェイは必要ありません。Cloud Connected PSTN プロバイダーは、Webex ユーザーが高い品質で安全に世界とつながり合えるようにする、一連の包括的なサービスパッケージを設計しました。Cloud Connected PSTN は、ローカル カスタマー ゲートウェイが展開されている場合、SIP ダイジェスト認証と TLS/SRTP を介して、お客様が使用する SBC と Webex Edge 間のローカルゲートウェイ（お客様構内）のエントリポイントにセキュリティを提供します。お客様が Webex Cloud Connected PSTN のクラウド通話コンポーネントのみを使用している場合、「Webex のセキュリティ」セクションで説明されているように、Webex クラウドに直接接続されている Webex アプリおよびデバイス間でセキュリティが確保されます。

Webex for BroadWorks を利用するお客様には、BYoPSTN と呼ばれるオプションも提供されます。Bring Your Own PSTN（BYoPSTN）ソリューションを使用することで、Webex for BroadWorks サービスプロバイダーは、ユーザーが Webex Meetings に参加するときに使用する電話番号を用意できます。このソリューションにより、パートナーは独自の PSTN ネットワークを活用し、シスコが用意した番号を使用するのではなく、PSTN プロバイダーとの既存の関係を利用できます。

リファレンスアーキテクチャは、BYoPSTN オプションのエンドツーエンドの設計を提供します。このアーキテクチャはシスコによって検証されており、BroadWorks と Webex Meetings 間のコールトラフィックのセッション ボーダー コントローラ（SBC）として Cisco Unified Border Element（CUBE）を使用します。詳細については、BYoPSTN ソリューションガイドを参照してください。

パートナー インフラストラクチャ内で BroadWorks から CUBE にルーティングされるコールでは、コールシグナリングとメディアのそれぞれに SIP TCP と RTP を使用します。CUBE から Webex へのコールでは、シグナリングとメディアのそれぞれに SIP MTLS と SRTP を使用します。CUBE から Webex へのコールルーティングはインターネットを介して行われ、SIP トランクを使用しません。BYoPSTN は、SBC の認証と SRTP を介して伝送されるすべての音声メディアの暗号化を組み込んだ Webex Edge Audio アーキテクチャを活用します。

Cloud Connected Audio（CCA）の接続は、Webex とのポイントツーポイントのプライベート接続を介して確立されます。CCA 回線は専用のカスタマー ポートで終端処理されます。お客様とシスコの両方のデータセンターにあるエッジ ルータとファイアウォールのアクセス コントロール リストによって、回線が保護されます。CCA サービスの IP サブネットはセグメント化されており、Cisco Unified Border Element（CUBE）の IP セグメントのみがお客様にアドバタイズされます。お客様には他のお客様の IP または CUBE に対する可視性がありません。

結論として、Webex CCA は、トラフィックに不要なオーバーヘッドを発生させたり設計を妨げたりすることなく、強力なセキュリティを提供します。詳細については、Webex CCA を参照してください。

Webex のプライバシー

Webex は顧客データの保護に積極的に取り組んでいます。シスコは、シスコのプライバシーポリシーと Cisco Webex Meetings プライバシーデータシートに従ってお客様の情報を収集、使用、処理します。

本サービスはプライバシーを念頭に置いて構築されており、EU の一般データ保護規制（GDPR）、カリフォルニア州消費者プライバシー法（CCPA）、カナダの個人情報保護および電子文書法（PIPEDA）、個人の医療情報保護法（PHIPA）、医療保険の相互運用性と説明責任に関する法令（HIPAA）、家族教育権とプライバシー法（FERPA）を含め、グローバルなプライバシー要件に合致した方法で使用できるように設計されています。

管理データ

シスコによる製品やサービスの提供を運用または管理するため、またはシスコ自身のビジネス上の目的でお客様またはサードパーティのアカウントを運営または管理するためにシスコが収集して使用する、お客様またはサードパーティの従業員や担当者に関する情報。

管理データには、名前、住所、電話番号、電子メール アドレス、およびシスコとサードパーティの間の契約責任に関する情報が含まれます。これには最初の登録の時点で収集されたデータおよび、シスコの製品またはサービスの管理または運用に関連してその後収集されたデータも含まれます。

また、管理データには、お客様の従業員または担当者が Webex で行った会議のタイトル、時刻、およびその他の属性も含まれています。管理データの他の例としては、Webex で開催された会議の議題、時刻、およびその他の属性があります。

お客様のデータ

これには、お客様によるシスコ製品またはサービスの使用に関連してお客様がシスコに提供したデータ、または作業明細書や契約に従い、お客様の特定の要求によってシスコが開発したすべてのデータ（テキスト、音声、ビデオ、画像ファイル、および記録を含む）が含まれます。

顧客データには、ログ、構成またはファームウェアのファイル、およびコアダンプも含まれます。

これらのデータは、製品またはサービスから取得され、サポート要求に対応して問題をトラブルシューティングするためにシスコに提供されます。顧客データには、管理データ、サポートデータ、テレメトリデータは含まれません。

サポートデータ

サポートサービスまたはその他のトラブルシューティングの依頼をお客様が送信したときにシスコが収集する情報(ハードウェアまたはソフトウェアに関する情報を含む)。これには、製品の状態に関する情報、ソフトウェアのインストールやハードウェアの構成に関するシステムおよびレジストリのデータ、およびエラー トラッキング ファイルなど、サポート インシデントに関する詳細が含まれます。サポートデータには、製品から取得され、サポート要求に対応して問題をトラブルシューティングするためにシスコに提供されるログ、構成またはファームウェアのファイル、コアダンプは含まれません。これらはすべて顧客データの例です。

テレメトリデータ

製品またはサービスの利用と運用によってもたらされる情報であり、計測およびロギングシステムによって生成されます。

Webex クラウドで収集されるすべてのデータは、堅牢なセキュリティテクノロジーおよびプロセスから成る複数の層によって保護されます。顧客データを保護するために Webex 運用の各層に配置される制御の例を次に示します。

- **物理アクセス制御:**物理アクセスは、生体認証、バッジ、およびビデオ監視によって制御されます。データセンターへのアクセスには承認が必要で、アクセスは電子チケットシステムで管理されます。
- **ネットワーク アクセス コントロール :** Webex ネットワークの境界は、ファイアウォールによって保護されています。Webex データセンターを出入りするネットワークトラフィックは、侵入検知システム（IDS）によって継続的にモニタリングされます。また、Webex のネットワークは、個別のセキュリティゾーンにセグメント化されます。ゾーン間のトラフィックは、ファイアウォールと Access Control List（ACL; アクセス コントロール リスト）によって制御されます。
- **インフラストラクチャのモニタリングと管理制御 :** ネットワークデバイス、アプリケーションサーバー、およびデータベースを含むインフラストラクチャのすべてのコンポーネントは、厳しいガイドラインに沿って強化されています。また、セキュリティ上の問題を検出して対処するために、定期的にスキャンされます。
- **暗号化制御 :** 前述のように、Webex データセンターとクラウドに登録された Webex アプリおよび Webex デバイス間で送受信されるデータは、PSTN トラフィックとクラウド対応会議での非暗号化 SIP/H323 ビデオデバイスを除いて、すべて暗号化されます。また、Webex に保存された重要なデータ（パスワードなど）は暗号化されます。

シスコの従業員は、サポート上の理由でお客様からアクセスを依頼された場合を除いて、顧客データにアクセスしません。この場合のシステムへのアクセスは、「職務の分離」の原則に従って、マネージャによってのみ許可されます。アクセス権は職務遂行の必要性に基づいて、必要なアクセス レベルでのみ与えられます。また、これらのシステムに対する従業員のアクセスについても、コンプライアンス維持のために定期的に確認されています。このようなアクセス権を持つ従業員は、国際標準化機構（ISO）27001 の情報セキュリティ認識トレーニングを毎年受講する必要があります。

これらの専門的な管理に加え、シスコの従業員は身元調査を受けて守秘義務契約（NDA）に署名し、企業倫理規定（COBC）のトレーニングを完了しています。

医療保険の相互運用性と説明責任に関する法令（HIPAA）

シスコは Webex の機能、テクノロジー、およびセキュリティに関する情報を提供します。HIPAA の対象となるエンティティは、自社の法律顧問と相談し、Webex の機能がビジネスプロセスに準拠し、GDPR に対応しているかどうかを判断する必要があります。

- GDPR コンプライアンス
- Webex Meetings プライバシーシート

業界標準と認定

シスコの厳しい社内標準に従うことに加えて、Webex は、情報セキュリティに対するシスコ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行っています。Webex は以下の認定に対応しています。

- ISO 27001、27017、27018、および 27701 認定
- Service Organization Controls（SOC）2 タイプ II 監査済み
- SOC 3 認定
- クラウド行動規範
- CSTAR
- クラウド コンピューティング コンプライアンス制御カタログ（C5）の構成証明
- FedRAMP 認定（詳細、範囲、および可用性については、cisco.com/jp/go/fedramp を参照）

注：FedRAMP 認定 Webex サービスは、米国政府および教育機関のお客様のみが利用できます。

まとめ

信頼のウェブ会議やビデオ会議をリードする Webex ソリューションを利用すれば、コラボレーションや業務スピードを向上させることができます。Webex は、スケーラブルなアーキテクチャ、一貫した可用性、およびマルチレイヤセキュリティを提供します。これらは、社内およびサードパーティの定める厳しい業界標準に準拠しているかどうかが検証され、継続的にモニタリングされています。シスコはあらゆるものを安全に接続し、あらゆることを可能にします。

購入のご相談

購入オプションの詳しい情報やシスコのセールス担当者への問い合わせをご希望の場合は、cisco.com/c/en/us/buy をご覧ください。

関連情報
Webex Meetings | Webex Events | Webex Training Webex Support | Cloud Connected Audio

2022 年 2 月