Cisco Webex Meetings セキュリティ

目次

はじめに 3

このドキュメントの内容 3

Webex セキュリティモデル 4

シスコのセキュリティおよびトラスト 5

- シスコのセキュリティツールおよびプロセス 5
- 内部および外部ペネトレーションテスト 7

Webex データセンターのセキュリティ 7

- 物理的セキュリティ 7
- 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 8

Webex アプリケーションのセキュリティ 8

- 暗号化 8
- Webex のロールベースのアクセス 11
- 管理機能 12
- その他の Webex の機能とセキュリティ 15
- Webex のプライバシー 16
- 業界標準と認定 18

まとめ 18

詳細情報 19

購入案内

はじめに

Cisco 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。

注： 「Webex Meetings」や「Webex Meetings セッション」という用語は、すべての Webex Meetings オンライン製品で使用される統合音声会議、インターネット音声会議、およびビデオ会議を指します。特に記載がない限り、ここでのセキュリティ機能は、本書で説明する Webex Meetings アプリケーションのすべてに等しく備えられています。

このドキュメントの内容

本書では、Webex アプリケーションのセキュリティ機能および関連サービスについて説明します。また、お客様が安心して Webex Meetings プラットフォーム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 のアプリケーションは、次のとおりです。

- Webex Meetings
- Webex Events
- Webex Training
- Webex Support（Webex Remote Access を含む）
- Webex Edge
- Webex Cloud Connected Audio

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。

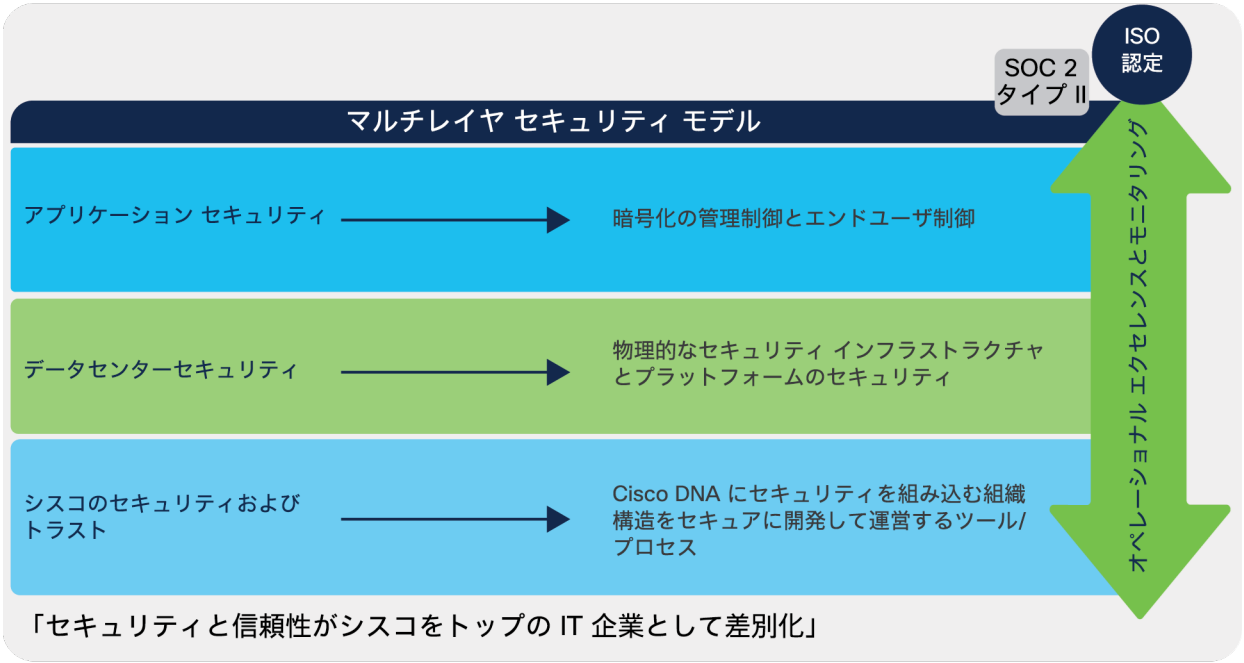

図 1.
シスコのセキュリティモデル

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意思決定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）
- 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、cisco.com/go/psirt を参照してください。

セキュリティに関する責任

シスコの 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、Webex クラウド内のネットワーク、システム、および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やファイアウォールを保護します。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 クラウドによって、日単位で内部および外部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

実行時の暗号化

クラウドに登録されている Webex アプリ、Webex Room デバイス、Webex クラウドとの間のすべての通信は、暗号化されたチャネルで行われます。Webex は TLS 1.2 の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）は暗号化されます。[1]

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 が接続指向であり、正しく並べられたデータを確実に上位層プロトコルに渡すため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 128 または AES 256 ベースの暗号を使用して暗号化されます。SRTP によるメディア暗号化をサポートする Webex ビデオデバイスやサードパーティ製のビデオデバイスでは、AES-CM-128-HMAC-SHA1 を使用します。Webex アプリは AES-256-GCM でメディアを暗号化します。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。

[1] 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とシグナリングストリームを暗号化することを推奨しています。

エンドツーエンドの暗号化

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。

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。

エンドツーエンドでの暗号化では、主催者が会議の暗号キーを生成し、他の参加者全員に安全に配布されます。会議の暗号キーを保護するため、キーは会議の主催者によって暗号化されてから Webex クラウドを介して各参加者に送信されます。

これを実現するために、各参加者の Webex アプリは 2048 ビットの RSA 公開キーと秘密キーのペアを生成し、公開キーを主催者の Webex アプリに送信します。ホストのアプリは、参加者の公開キーを使用して会議キーを暗号化し、暗号化された会議用の暗号キーを参加者のアプリに返します。Webex アプリは、RSA 秘密キーを使用して会議キーを復号できます。

エンドツーエンドの暗号化を利用することで、Webex アプリ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）は共有の会議暗号キーで暗号化され、Webex サービスは会議データを復号できなくなります。

このエンドツーエンドの暗号化オプションは、Webex Meetings および Webex Support サービスで使用できます。エンドツーエンドの暗号化を有効にすると、次の機能がサポートされなくなるのでご注意ください。

- パーソナル会議室でのミーティング
- 主催者より先に参加
- ロビーへの移動
- ビデオデバイス対応の会議
- ブレイクアウトセッション
- Webex Meetings Web アプリ
- Linux クライアント
- ネットワークベースの録画（NBR）
- Webex Assistant
- リモートコンピュータの共有
- セッションデータのトランスクリプト、議事録の保存
- PSTN コールイン/コールバック [2]

[2] エンドツーエンドの暗号化が有効な状態で Pro-E2E-Unencrypted Audio セッションタイプを使用すると、Webex アプリだけがエンドツーエンドの暗号化を使用します。つまり PSTN ユーザから送信されるメディアは、エンドツーエンドでは暗号化されません。

さまざまな暗号方式

Webex サービスは TLS 暗号スイートを次の優先順位でサポートし、セキュアな通信を実現します。表 1 は、Webex サービスで使用される一般的な暗号スイートとその優先順位を表したものです。

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_128_GCM_SHA256	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	256
TLS_RSA_WITH_AES_128_GCM_SHA256	128
TLS_RSA_WITH_AES_256_GCM_SHA384	256
TLS_RSA_WITH_AES_128_CBC_SHA256	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	256
TLS_RSA_WITH_AES_128_CBC_SHA	128
TLS_RSA_WITH_AES_256_CBC_SHA	256

保管中のデータの保護

お客様が保管中のデータを保護するように設定している場合、Webex Meetings はビジネスにとって重要になる可能性がある会議やユーザデータを保存します。Webex Meetings は次の安全対策を使用して保管中のデータを保護します。

- 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、すべてのユーザパスワードを保存する。
- 会議や録画データなどに設定された他のパスワードを暗号化する。
- 保存されたネットワークベースの録画データを暗号化する。Webex 録画は、ファイルレベルと論理ボリュームレベルの両方で暗号化されます。ファイルの暗号化には AES-256-GCM が使用されます。このファイル暗号キーは、256 ビットのマスターキーをベースに暗号化され、ポリシーに基づいてローテーションされてキー管理サーバ（KMS）に保存されます。暗号化された録画ファイルは、再生時やダウンロードフロー時の動作前または動作中に復号されます。シスコは、お客様のためにこれらのキーを保持します。

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

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（トレーニングとイベントのみ）

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。参加者は何人でもパネリストになれます。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、パブリックおよび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投票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。

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。

管理機能

Webex には、Webex のサイトをビジネスニーズに効果的に合わせることができる、きめ細かなサイト管理機能があります。ここではセキュリティ関連の主な管理機能について説明します。

アカウント管理

ID 管理技術を Webex と統合してお使いの IdP によるシングルサインオン（SSO）を可能にし、アカウント管理とアクセスポリシーを完全に制御できるようにします。Webex でアカウントが保持されると、必要に応じて多数のサイト管理機能で管理できるようになります。

サイト管理者は次の操作を実行できます。

- 制限回数を超えてログインに失敗すると、アカウントをロックする（制限回数は設定により変更可能）
- 指定された時間が経過した後、アカウントのロックを自動的に解除する
- 定義した期間使用されなかったアカウントを非アクティブ化する
- 次回ログイン時にユーザにパスワードの変更を要求する
- ユーザアカウントをロックまたはロック解除する
- ユーザアカウントをアクティブ化または非アクティブ化する
- 新規アカウントの要求時にセキュリティテキストを求める
- 電子メールによる新規アカウントの確認を要求する
- 新規アカウントの自己登録（サインアップ）を許可する
- 新規アカウントの自己登録の規則を設定する
- セキュリティオプションを設定して、参加者が 1 人しかいない場合は会議を自動的に終了する
- ダイヤルインユーザの発信者 ID を可能な場合に表示する
- 主催者が個人のアバターをアップロードできるようにする
- 主催者がカスタム仮想バックグラウンドを追加できるようにする
- 参加者に会議での共有を許可する（会議のみ）
- 参加者に主催者より前の参加を許可する（デフォルトではオフ）
- 参加者に主催者より前の音声での参加を許可する（デフォルトではオフ）
- 会議をリストから外す（デフォルトではオフ）
- メールアドレスの更新でユーザによる確認を求める

SSO を使用せず、Webex Control Hub を使用していない Webex サイトの管理者は、次の設定オプションでパスワード条件設定を管理できます。

- 大文字と小文字の両方を含む
- 最小長
- 数字、英文字、または特殊文字の必要最低文字数
- 同じ文字を連続して 3 回以上繰り返すことは不可

- 以前使用したパスワードは再使用不可（使用不可とする直近のパスワード数は指定可能）
- ダイナミックテキスト（サイト名、ホスト名、ユーザ名）は使用不可
- 使用できないパスワード（「password」など）のリストを設定可能
- パスワード変更の最小間隔
- 主催者によるアカウントパスワードの変更（間隔は設定可能）
- 次回ログイン時にすべてのユーザにアカウントパスワードの変更を要求
- サイト設定の監査ログをダウンロード（このログは、[共通サイト設定（Common Site Settings）] の [オプション（Options）] で行われた設定の変更内容を示します）
- 会議が予定されているサイトからホストキーを取得するための認証を要求
- 主催者が個人をアップロードする機能を無効化
- 同じ文字の 3 回以上の繰り返し使用を許可しない
- ユーザのアカウントパスワードの Cookie への保存を許可する

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。ほとんどの場合、これらの設定をサイトレベルで適用し、Webex Meetings、Webex Events、および Webex Training が別々に動作するようにすることで、すべてのユーザが必要とする使用例に合わせることができます。また、ファイル転送、デスクトップ共有、記録などの多くの会議内機能は、カスタマイズしたセッション タイプを使用して、特定のユーザグループに対して有効または無効にすることができます。

Webex Meetings では次のような設定が可能です。

- ユーザが名前と電子メールアドレスを保存することで、簡単に今後の会議を主催したり会議に参加したりできるようにする
- 主催者が共同主催者を指名できるようにする
- 主催者が他の主催者に代わってスケジュールすることを許可する
- 主催者が他の主催者に記録を再譲渡できるようにする
- サイトへのアクセスの際に、すべての主催者と出席者に認証を要求する
- 現在公開されているすべての会議を非表示にする
- すべての会議でパスワードを義務付ける
- 電話で参加するときに会議パスワードを適用する
- ビデオでの参加者に数字のパスワードを適用する
- 会議に参加するすべての参加者（主催者を含む）に免責事項を適用する
- 参加者に主催者より前の参加を許可する
- ロック解除された会議にゲストユーザが参加する方法を制御する（参加可、ロビーで待機、参加不可）
- 音声のみユーザ用のロビーを有効にする

- 残りの参加者が 1 名のみになった場合、設定可能な時間が経過した後に会議を自動的に終了する
- 記録の閲覧をサインインしたユーザに制限する
- 録画および録音のダウンロードを禁止する
- ネットワーク上にあるすべての録画および録音にパスワードを適用する
- 録画および録音を表示またはダウンロードする前に、すべての参加者に免責事項を適用する
- 「パスワードを忘れた場合」の更新リクエストの承認を管理者に要求する
- Dropbox や Box などの外部アプリとコンテンツを共有できるようにする
- リモートアクセスサービスに強力なパスワードを適用する
- 人工知能によるロボットの Webex 会議への参加を禁止する

管理者は、サイト全体でこれらの設定のセキュリティレベルを低く設定することで、主催者が必要に応じて特定の会議のセキュリティを設定できるようにすることができます。

たとえばサイト管理者が、会議参加にあたってのサインインをユーザに要求せず、サインインした参加者のみを個々の主催者が許可することによって、特定の会議をセキュリティで保護することができます。

パーソナルルームのセキュリティ設定

すべての Webex Meetings 主催者に、会議に使用できるパーソナルルームの専用 URL を与えることができます。パーソナルルームの URL は次のように構造化されています。https://sitename.webex.com/meet/username 主催者または Webex 管理者は、ユーザ名を変更できます。パーソナルルームを使用すると、参加者は会議に参加するために電子メールまたはカレンダーを探す必要がないため、簡単にコラボレーションを行うことができます。パーソナルルームは、主催者がログインしている場合に有効になる、パーソナライズされた仮想ルームと考えてください。

パーソナルルームのセキュリティ保護に関しては、Webex 管理者は次のことが可能です。

- パーソナルルームを自動的にロックする
- 主催者のパーソナルルーム（Webex アプリおよびビデオエンドポイント）に入室する前に、参加者の認証を要求する
- 会議がロックされているかロック解除されているかに応じて、認証済みの出席者とゲストをロビーに移動させるためのポリシーを適用する
- 参加者がロビーにいるときに主催者に通知することを許可する（または許可しない）
- ロビーからのタイムアウト値（最長待機時間）を設定する
- ホスト PIN の長さ（ビデオエンドポイントからパーソナルルームに入るために使用する）を適用する

パーソナルルームの主催者は次のことができます。

- パーソナル会議室を手動でロックする、または指定した期間の経過後に自動的にロックするようにルームを設定する
- 会議がロックされているかロック解除されているかに応じて、認証済みの出席者とゲストをロビーに移動させるためのポリシーを適用する。たとえば、実際の会議室と同様に、権限が付与された従業員はどの部屋にも入室できるが、権限のない訪問者は同伴が必要

- 主催者が電話からパーソナルルームを開始できるようにする
- （i）Webex サイトの主催者アカウントを持つユーザ、または（ii）認証済みのシスコビデオデバイスから参加する参加者に、パーソナルルームでの会議開催を許可する
- パーソナルルームへの共同主催者の割り当てを許可する
- 参加者自身によるミュート解除を許可する
- 会議に参加する際に参加者をミュート設定にする
- 不在中にパーソナルルームのロビーへの入室があった場合、電子メール通知を送信する

シングルサインオン（SSO）

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 プロトコルを使用したシングルサインオン（SSO）のユーザ認証をサポートしています。

SSO を有効にするには、サイト管理者が X.509 証明書を Webex サイトにアップロードする必要があります。

アップロードすると、ユーザ属性を含む SAML アサーションを生成して、X.509 証明書の秘密キーでアサーションのデジタル署名が行えます。Webex では、ユーザ認証の前に、プリロードされた証明書の公開キーと照らし合わせて SAML の署名を検証します。

SAML アサーションは、Webex サイトとお客様の ID プロバイダー（IdP）（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 アクセスマネージャなど）との間で交換されます。Webex サイトは、サービスプロバイダーとして機能します。Webex は、サービスプロバイダーが開始した SSO フローと IdP が開始した SSO フローの両方をサポートします。

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 はユーザクレデンシャル（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
- お客様は、SaaS ベースの各サービスで異なるソリューションを使用させるのではなく、ユーザの二要素認証を一元的に実行できる
- Webex はユーザクレデンシャルを保存しない
- 誰が Webex にアクセスするかをお客様が制御できる
- ユーザが企業の IdP に参加または退席するときのオンボーディングとオフボーディングの透過性が高まる

その他の Webex の機能とセキュリティ

ビデオデバイスによる会議への参加

ユーザは、ビデオデバイスを使用して Webex での会議に参加または開始できます。会議の参加者は、Webex Room デバイス（Cisco UCM 登録（SIP）デバイスまたは 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のビデオデバイスまたはアプリケーションから会議のビデオアドレスにダイヤルして会議に参加できます。Webex Room デバイスがあれば、Webex アプリユーザ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、会議に参加したりできます。

お客様の施設では、ビデオデバイスを稼動するためにビデオ ブリッジング デバイスを追加する必要はありません。ビデオブリッジング機能は、Webex Meetings と同様に安全性の高い Webex クラウドに導入されており、同じ業界クラスのセキュリティ制御（物理、ネットワーク、インフラストラクチャ、および管理）を使用しています。ビデオエンドポイントは、シグナリングおよび Real-Time Transport Protocol/Secure Real-Time Protocol（RTP/SRTP）メディア向けの Session Initiation Protocol（SIP）と H.323 を使用して、会議に参加できます。Webex Meetings では、SIP 向けに TLS トランスポートがサポートされ、メディア向けに SRTP がサポートされています。ビデオエンドポイントが SIP/TLS を利用して会議に参加すると、Webex クラウドメディアストリームは SRTP によって暗号化されます。

H.235 は H.323 接続をセキュリティ保護するために使用されます。

また、サイトは、ビデオ デバイスを使用して会議に参加する際に、パスコードを要求するように設定できます。

Cloud Connected Audio

Webex Cloud Connected Audio（CCA）は、エンドツーエンドの音声ソリューションです。オンプレミスの IP テレフォニーネットワークを利用して、統合された音声エクスペリエンスを Webex 会議に提供します。Webex CCA は、従来の PSTN 接続を使用する代わりに、Session Initiation Protocol（SIP）トランクを使用して、構内から Webex データセンターに接続します。このソリューションは、他のすべての Webex 音声オプションと同様に、統合された直感的なユーザエクスペリエンスを提供します。ただし、IP テレフォニーネットワークを直接使用するため、Webex CCA は魅力的な価格で購入できます。

CCA は完全にカプセル化された環境です。インターネットからこの環境に到達することや、あらゆる種類の攻撃を実行することは非常に困難です。インフラストラクチャは共有されていますが、テナント間のルーティングがないため、他のテナントからの悪意のあるトラフィックがブロックされます。さらに、トランクを通じたトラフィックは、目的の Webex インフラストラクチャポートに送信されるルーティングプロトコルと User Datagram Protocol（UDP）パケットに制限されます。Webex インフラストラクチャは、事前設定されたダイヤルピアからのみトラフィックを受信するように設定されています。

CCA の接続は、Webex プラットフォーム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。

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。

Webex サービス利用条件では、追加情報を提供しています。

Webex は、適切な正規の転送メカニズムに従って、管理データ、サポートデータ、およびテレメトリデータを EU から米国に（必要に応じて、他の許可されたロケーションにも）転送します。これらのデータのカテゴリの定義を次に示します。

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、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。

顧客データ：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、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、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 Room デバイスの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て、シスコの従業員は身元調査を受け、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 への対応状況
- 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、および 27018 認定
- Service Organization Controls（SOC）2 タイプ II 監査済み
- SOC 3 認定
- 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/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、https://www.cisco.com/c/en/us/buy をご覧ください。

詳細情報

Webex ソリューションの詳細については、次のサイトを参照してください。

- Cisco Webex Meetings
- Cisco Webex Events
- Cisco Webex Training
- Cisco Webex Support
- Cisco Webex Cloud Connected Audio

お問い合せ先

シスコシステムズ合同会社

〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp

C11-737588-04JA 21.11