ホワイトペーパー

Webex Calling セキュリティ

webex by CISCO

目次

1. 概要

Webex® Calling は、あらゆる規模の企業向けに最適化されたクラウドベースの電話システムです。デスクトップ、モバイル、リモートワーカーに不可欠なビジネスコール機能を、グローバルな Webex コラボレーション プラットフォームから提供します。Webex Calling はクラウドベースなので、柔軟性に優れ、新機能をすばやく提供でき、運用コストが予測可能です。また、世界規模で瞬時にキャパシティを拡張でき、Webex コラボレーション プラットフォームに接続することでオンプレミスの投資も保護できます。

このドキュメント全体を通じて使用される Webex および Webex コラボレーション プラットフォームという用語は、Webex Calling、Webex Meetings、Webex アプリサービスを含む Webex 製品ライン全体と、それらが運用されるインフラストラクチャを指しています。Webex Calling は Webex 製品ラインのコアサービスであり、Webex コラボレーション プラットフォーム上で運用されています。

Webex セキュリティとプライバシーの違い

Webex の製品設計と提供のアプローチには、セキュリティとプライバシーが組み込まれています。Webex はセキュリティの文化を確立し、チェックとバランスを徹底するために多額の投資を続けてきました。Webex Calling を含むすべての Webex サービスのデフォルト設定はセキュリティを考慮して決定されているため、設定を気にせず安心してコラボレーションを開始できます。同時に、Webex はセキュリティを損なうことなく快適なユーザー体験を提供します。

Webex と Webex Calling は、ネットワークからエンドポイント、データセンター、クラウドサービスに至るまで、セキュリティ分野におけるシスコの豊富な実績と専門知識に支えられています。Webex のすべての製品とサービスは、シスコのセキュアな開発ライフサイクル（CSDL）を通じて開発され、厳格なセキュリティ基準に沿って構築されています。シスコ製品のセキュリティは、複数の部門にまたがる何百人ものセキュリティアドバイザによって個別に検証されています。Webex は、組織内のコラボレーションにも企業間のコラボレーションにも利用できるエンタープライズクラスの強力なコラボレーションプラットフォームです。デフォルト設定のまま安全に利用でき、プラットフォーム上でやり取りされるデータも確実に保護できます。

プライバシー、セキュリティ、透明性：シスコが掲げる 3 つのセキュリティ原則

シスコはお客様のデータの**プライバシー**を尊重することに注力しています。

- Webex がユーザーデータをサードパーティに貸与、販売することは一切ありません。
- Webex ではセキュリティとプライバシーを重視してすべての機能を実装しています。
- Webex におけるプライバシーへの取り組みはすべて公開されています。

Webex は、追加で機能を加えることなく**安全性を確保**します。

- Webex にはセキュリティが重要な基本要素として最初から組み込まれているため、デフォルト設定のままでも安全です。データ共有からのオプトアウトやプライバシー設定をユーザー任せにすることは決してありません。
- Webex ではすべてのサービスで強力なパスワードがデフォルトで有効になっています。
- Webex は、**セキュリティ サイバー ガバナンス**を導入しており、セキュリティ上の問題が見つかった場合の**透明性**を維持します。
- シスコの Security and Trust 部門がWebex のセキュリティとプライバシーを統括し、セキュリティの脆弱性についても公開しています。

シスコにとってセキュリティは最優先事項です。シスコは、セキュリティとプライバシーに多大な投資を行ってきました。Webex Calling は、エンドツーエンドでセキュリティを確保するためにゼロから構築されました。シスコのプロセスとガバナンスは、お客様のプライバシーを保護し、信頼できるセキュリティを提供する上で十分に成熟しているものと自負しています。シスコのミッションは、妥協のないコラボレーションを実現することです。

Webex Calling と Webex コラボレーション プラットフォームは、管理機能からエンドユーザーとのやり取りまで、幅広いタスクに対応する複数レベルのセキュリティを備えています。このホワイトペーパーでは、Webex Calling を支える主要なセキュリティ対策と、Cisco Webex Calling が稼働する Webex コラボレーション プラットフォーム インフラストラクチャについて詳細に解説し、投資の判断に必要な情報を提供します。

1.1 本書の内容

本書では、Webex Calling と Webex コラボレーション プラットフォームの保護に役立つシスコのツール、プロセス、認定、エンジニアリング手法について説明します。

2. シスコの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、すべてのシスコ製品およびソリューションと同じセキュリティ基盤に基づいて構築されています。

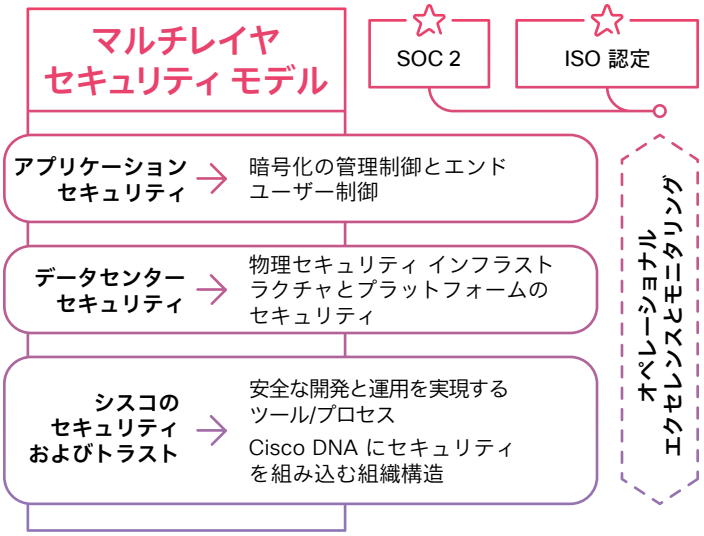


図 1. Webex セキュリティモデル

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。

2.1 シスコのセキュリティおよびトラスト

すべてのシスコ製品開発チームは、シスコのセキュアな開発ライフサイクル（図 2）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、Webex Calling 製品開発のあらゆる側面でこのライフサイクルに従います。

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。

2.2 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。

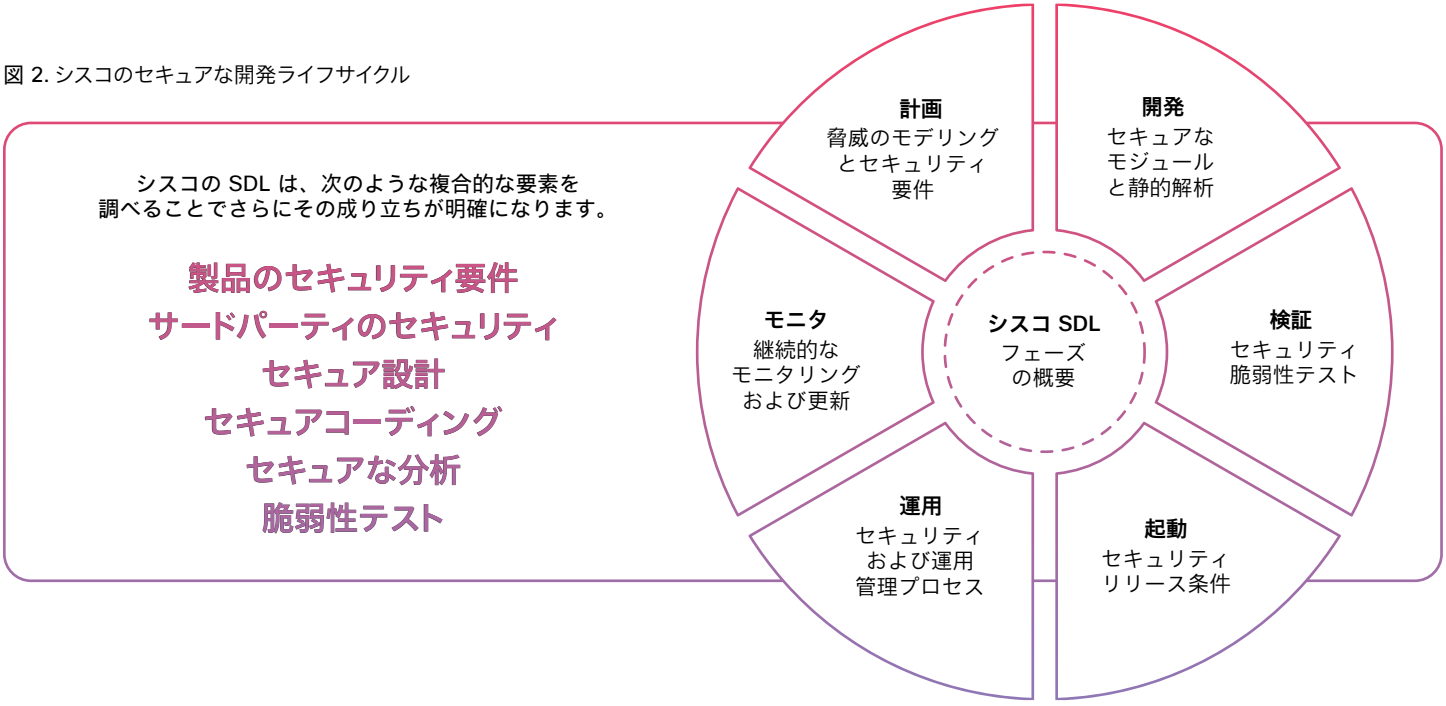
- 製品が準拠する必要がある製品セキュリティベースライン（PSB）の要件
- 脅威モデリングで使用される脅威ビルダーツール
- コーディングのガイドライン
- 開発者が独自のセキュリティコードを作成する代わりに使用できる検証済みまたは認定済みライブラリ
- セキュリティの欠陥をテストするために開発後に使用できるセキュリティ脆弱性テストツール（静的および動的解析用）
- シスコおよびサードパーティのライブラリをモニタリングし、脆弱性が検出されると製品チームに通知するソフトウェアトラッキング

2.3 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

図 2. シスコのセキュアな開発ライフサイクル



2.4 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 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の継続的な改善に対しても責任を負っています。

2.5 Cisco Security and Trust 部門 : インシデント指揮官

Cisco Security and Trust 部門のインシデント指揮官は、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。インシデント指揮官はセキュリティ問題のシビラティ（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、シビラティ（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今後予定されている。
- 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インシデント指揮官が確認した。この場合、インシデント指揮官は、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、インシデント指揮官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、インシデント指揮官は、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。インシデント指揮官は共通脆弱性評価システム（CVSS）のスケールを使用し、発見された問題のシビラティ（重大度）をランク付けします。インシデント指揮官は、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。

インシデント指揮官の詳細については、tools.cisco.com/security/center/publicationListing.x をご覧ください。

Cisco Talos によって支えられる比類のない可視性と脅威からの保護

Cisco Talos は、300 名を超える研究者が所属する、世界最大規模の民間脅威インテリジェンスチームであり、攻撃に利用されるさまざまな悪意のあるドメイン、IP、URL、ファイルを検出してブロックします。また、世界中から集められる膨大な量のインターネット アクティビティ データを、統計処理と機械学習を組み合わせたモデルに投入することで、インターネットに出現する新たな脅威を特定します。Cisco Talos は、アンチウイルスエンジン、Cisco Advanced Malware Protection（AMP）、Cisco Threat Grid サンドボックスを使用し、毎日分析される何百万もの新しいマルウェア サンプルから得られたインテリジェンスを活用して、悪意のあるファイルに対する最も効果的な防御を実現します。

2.6 セキュリティに関する責任の共有

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。

- シニアバイスプレジデント / ゼネラルマネージャ:セキュリティおよびアプリケーション担当
- シニアバイスプレジデント / ゼネラルマネージャ : コラボレーション担当
- バイスプレジデント : Webex プラットフォームおよびインフラストラクチャ エンジニアリング担当
- 最高情報セキュリティ責任者 : コラボレーション担当

3. Webex Calling データセンターのセキュリティ

Webex Calling 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 Cloud を通じて配信されるクラウドソリューションです。Webex Cloud は、 リアルタイムのオーディオ、ビデオ、コンテンツ共有を目的とした通信インフラストラクチャです。

Webex Calling では、 世界中の複数のデータセンターに存在するコンピューティング機器が使用されます。 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。

データセンターは SSAE-16 および SOC-2 に準拠しており、物理的なセキュリティ境界、物理的な入場管理、 オフィス、部屋、施設の保護、外部および環境の脅威からの保護、安全なエリアでの作業、補助的公共設備、ケーブル配線のセキュリティ、配送および荷積みゾーンなどの分野で SOC2 に遵守していることを証明するために毎年評価を受けています。Webex Calling アプリケーションとサービスは、シスコおよびサード パーティ データ センター内の複数のサーバで運用されています。Webex Calling は、物理的なアクセスと保護、ネットワーク接続、 リモート / ローカルアクセス、アプリケーションとサーバの管理、 可用性、 およびお客様の機密データの保護に対応するセキュリティおよび可用性確保の手法と手順に基づいて設計および構築されています。シスコは、大規模なデータセンターの設計、実装、運用に関する長年の経験を持つデータセンター運用事業者と提携しています。 これらの施設は、Webex Calling の物理アプリケーションおよび仮想アプリケーション環境を保護できるように、物理面、環境面、アクセス面でのセキュリティを備えています。 次に例を挙げます。

- 24 時間常駐のオンサイトセキュリティ担当者
- 自然境界で保護され、 名称などを表示していない施設
- 現地の法執行機関への通報を自動的に行うサイレントアラームシステム
- 現地政府の基準に準拠したコード開発
- 環境保護
- 完全冗長 HVAC 施設
- 自動火災抑制システム、 デュアルアラーム (熱 / 煙)、 クロスリンクイベント管理によるデュアルインターロック
- データセンター全体のキャパシティをサポートする N+1 冗長無停電電源 (UPS) システムと冗長バックアップ発電装置
- 施設ごとのディザスタリカバリ計画 (震災、洪水対策)
- 生体認証スキャンおよび / または二要素認証によるアクセス
- 入口での入退出管理 (マントラップ)
- 施設への入場には政府発行の有効な写真付き身分証明書が必要 (すべての入場履歴を監査用の記録として保存)
- 施設への入場には事前の許可が必要 (業務上正当な理由がある場合にのみ入場を許可)
- 出荷と受け取りの場所を他のエリアから隔離
- すべての資材の入退出時にオンサイトのセキュリティスタッフが検査を実施

管理者が Webex Calling コンピューティングアセットにアクセスする際には、 二要素認証 (2FA) を使用します。 また、 すべてのユーザーと管理者のアクティビティがログに記録されます。24 時間 365 日体制の Webex Calling Security Operations Center (SOC) が、システムログ、侵入検知システム (IDS)、ファイアウォールアラートを監視し、 攻撃や誤用を検出して防止します。

4. 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

シスコのセキュリティに対するアプローチは、Webex コラボレーション プラットフォームを構成するネットワーク、システム、データセンター全体のセキュリティにも反映されています。ネットワーク サービス エンジニアがオペレーティングシステムとインフラストラクチャを強化して常時パッチを適用し、 さまざまなセキュリティ脆弱性からシステムを保護します。 サーバは、安全かつ確実にデータを配信できるよう管理されています。

オペレーティングシステム、ミドルウェア、アプリケーションの強化には、以下の対策が含まれます。

- セキュリティ重視の継続的な強化
- 本番環境導入前の徹底したセキュリティチェックと受け入れ検査
- 脆弱性スキャニングとアセスメント
- セキュリティパッチの適用
- マルウェア対策
- 堅牢なロギングの実装と構成
- 強力な認証
- アクセス制御、「最小権限」、「必要最小限の情報提供」による慎重な設定
- 情報のバックアップ

適切なアクセス制御と管理体制により強化されたシステムでは、システム機能へのアクセスが必要かつ許容範囲内のものだけに制限されます。システム、ソフトウェアのバージョン、およびアップグレードは、実稼働環境に導入して使用を開始する前に、ステージング環境で適切にテストされ、クロスチェックされます。情報システムの技術的な脆弱性は常に監視され、ログに記録されます。運用チームは、脆弱性の影響度を評価し、関連するリスクに対処するための適切なパッチ管理ライフサイクル対策を実施します。情報処理施設の利用状況を監視するためのプロセスも用意されていて、運用チームが定期的に施設の利用状況を確認します。

5. ネットワーク通信セキュリティ

ネットワークで相互接続された情報とシステムは、重要なビジネス資産です。したがって、すべてのレベルでネットワークセキュリティを維持および確保することが不可欠です。運用チームは、技術的な手段と管理手順の両方を通じてネットワークセキュリティを実現します。

ネットワークセキュリティには次のものが含まれます。

- Demilitarized Zone (DMZ; 緩衝地帯)
- ファイアウォール
- 侵入検知
- システム認証
- データ暗号化

セキュリティ管理チームが、すべてのネットワークサービスのセキュリティ機能、サービスレベル、管理要件を決定します。また、脅威からネットワークを保護するとともに、ネットワークを使用するシステムやアプリケーションに加え、転送中の情報のセキュリティを維持できるようにネットワークを管理します。脅威の検出、防止、修復のための対策と、適切なユーザー意識向上手順を通じて、悪意のあるコードからネットワークを保護します。監査ログには、すべてのユーザーアクティビティ、例外、情報セキュリティイベントが記録されます。運用チームとセキュリティチームは、これらのログを保存して、将来の調査やアクセス制御のモニタリングに役立てます。情報セキュリティプロセスが適切かつ完全で、目的に適合し、実際に適用されていることを確認するために、独立機関によるレビューが定期的に実施されます。

6. Webex Calling アプリケーションのセキュリティ

6.1 暗号化

6.1.1 転送中のデータの保護

Webex Calling は、アクセス側のネットワーク通信アクセスにデータ暗号化を適用します。Webex Calling は、アクセス側のネットワーク通信アクセスにデータ暗号化を適用します。管理者によるシステムへのアクセスは、次の Transport Layer Security(TLS) バージョンと強力な暗号スイートを使用して暗号化されます。

TLS 1.3 暗号スイート :

- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_AES_128_GCM_SHA256

TLS 1.2 暗号スイート :

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

6.1 暗号（続き）

- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA

SIP エンドポイントとサービスの間の SIP コール制御シグナルは、次の Transport Layer Security（TLS）バージョンと強力な暗号スイートを使用して暗号化されます。

TLS 1.2 暗号スイート：

- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- 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

SIP エンドポイントとサービスの間のメディアストリームは、RFC 3711 に記載されている Secure Real-Time Transport Protocol（SRTP）を使用して保護されます。

6.1.2 保管中のデータの保護

Webex Calling には、ビジネスに不可欠な組織とユーザーのデータが保存されます。Webex Meetings では、次の安全対策を通じて保管中のデータが保護されます。

- AES 256 を使用して保存データを暗号化
- 一方向のハッシュアルゴリズムとソルトを使用して、すべてのユーザーパスワードを保存
- 他のパスワードを暗号化（SIP 認証など）
- すべてのバックアップファイルとアーカイブを暗号化

6.2 アクセス制御

Webex サービスでは、適切なレベルのアクセス制御が定義され、運用環境に実装されています。このポリシーに準拠したアクセス制御が各システム、アプリケーション、データベース、ネットワークに適用され、各種のデータ分類とデータにアクセスするユーザーの管理に使用されます。これらの制御は、ユーザーアクセスの要求、承認、付与、取り消し、変更と、ユーザーロールの定義に関する標準化されたプロセスで構成されています。制御には、職務分掌分析、最小特権アクセス、ユーザーパスワード、ユーザー識別ポリシーと標準、ユーザーアクセス監査に対する期待、ネットワークアクセス制御リストに加え、ネットワークアクティビティとアクセスアクティビティの監査も含まれます。

アクセス制御ポリシーでは、設定および情報へのアクセスを必要とするシステムとアプリケーションのユーザーアカウントとアクセス制御を実装する必要があります。ポリシーと制御の範囲は、シスコ カスタマーエクスペリエンス（シスコサービス）組織が所有および運用または管理するインフラストラクチャとアプリケーションへのアクセスのみに限定されます。

ユーザーアカウントとアクセス制御は、次のセキュリティ要件を満たしている必要があります。

- すべてのユーザーに一意の ID が割り当てられ、割り当てられた特権コンポーネントにアクセスするには認証が必要となる
- ID と認証ログイン情報が複数のユーザーに配布されることはなく、グループ / 共有ログイン情報は共有および配布されない
- ユーザー ID、ログイン情報、その他の識別子オブジェクトの追加、削除、および変更は、システムによって制御される
- 特権ユーザー ID へのアクセスは、職務の遂行に必要な最小限の権限のみに制限される
- 特権ユーザーの識別はアクセスのたびに行う必要がある
- 雇用期間を終了したユーザーのアクセス権はただちに取り消される
- 非アクティブなユーザーアカウントは削除または無効化される
- システムコンポーネントにアクセスしてサポートや保守を行うサードパーティが利用する ID を管理できること

6.2 アクセス制御（続き）

これらの制御は、管理者または指定されたセキュリティ担当者によって定義、承認、実施、および監視されます。これらの制御の正確性と有効性は、内部および独立監査機関によって、少なくとも年に 1 回レビューされます。

6.3 ユーザー認証

サブスクライバは、Webex アイデンティティに登録されます。Webex アイデンティティは、スタンドアロンの ID 管理機能またはオンプレミスハイブリッド ID 統合を提供するクラウド規模の ID プラットフォームです。統合には、Active Directory ユーザーアカウントのレプリケーション、主要プロバイダー（Okta、Ping Identity など）によるシングルサインオン（SSO）、お客様が利用可能な API が含まれます。最新のテクノロジーと標準（SAML 2.0、OAuth2、REST など）に基づいて構築された CI は、シスコのクラウド コラボレーション ポートフォリオの基盤であり、成長と適応を見据え、クラウド規模のアプリケーション向けに構築されています。

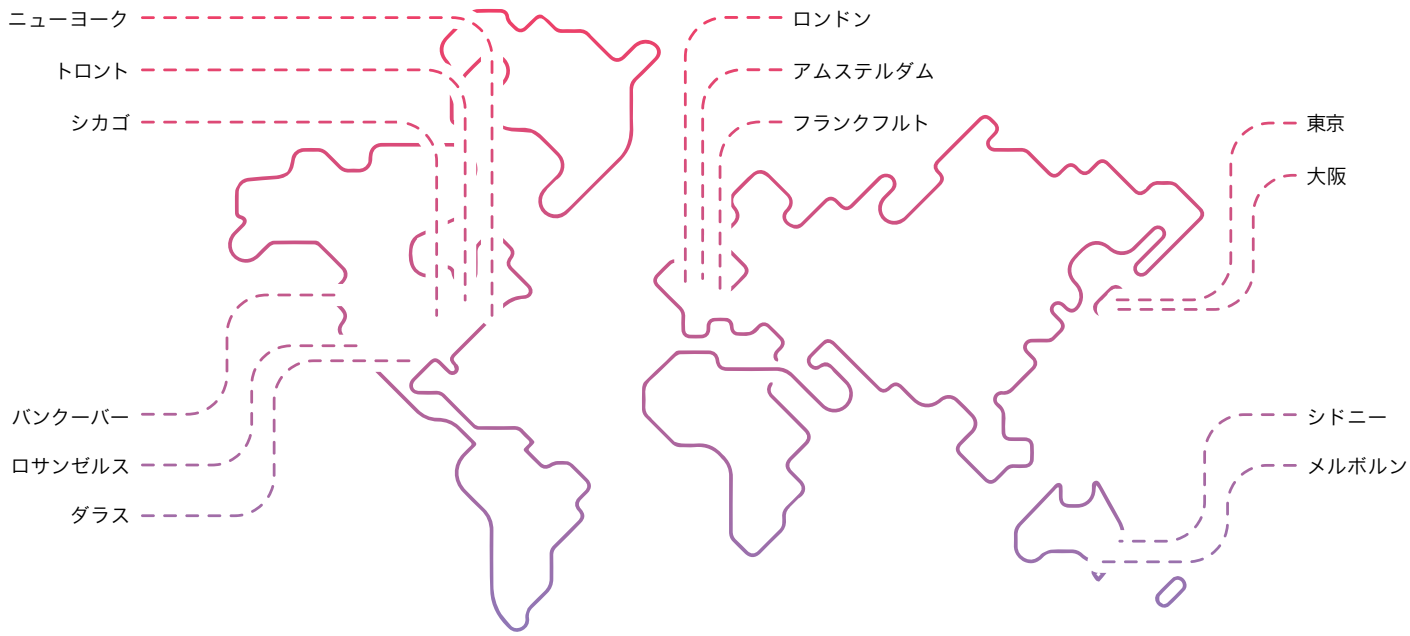
7. 販売地域

Webex Calling は、キャリアクラスの可用性（99.99% の可用性）を実現するように設計されています。キャリアクラスの可用性は、次の手法によって実現されます。

- N+1 サーバクラスタリング
- 地理的な冗長性（3 つの大陸に 10 ヵ所のデータセンターを設置、図 3 を参照）
- データセンター内およびデータセンター間での自動データレプリケーション
- 分散型サービス妨害（DDoS）の検出と防止

Webex Calling ディザスタリカバリプランは、Webex Calling エンジニアリングチームと運用チームが運用するネットワークおよびサービス要素の冗長設計の概要を定義し、災害発生時にネットワーク機能とサービス機能を迅速に復旧することに重点を置いています。シスコは、地理的冗長性が確保されたデータセンターを通じて Webex Calling サービスを提供しています。

図 3. データセンターの場所



これらのデータセンターには、お客様にサービスを提供するために必要なすべてのデータネットワーク機器とサーバ機器が設置されています。シスコの従業員が勤務するオフィスは、これらのデータセンターから物理的に独立しています。そのため、いずれかのシスコ従業員オフィスが利用不可能になる事態が発生しても、データセンターを通じてお客様に提供されるサービスには影響しません。いずれかのシスコ オフィスに影響を与える事態が発生した場合でも、Webex Calling 運用チームは、世界中どこからでもセキュアな VPN アクセスを介してネットワーク要素とサービス要素をリモートで管理できます。

また、Webex Calling ソリューションは、いずれかのデータセンターが利用できなくなった場合でも、別のデータセンターがトラフィックをリダイレクトして処理できるように設計されています。シスコは、ワールドクラスのデータセンターベンダーを活用して、ネットワークとサービスの運用に必要なスペースと電力を確保しています。すべてのベンダーが SSAE 16 Type 2 に準拠し、99.99% を超える稼働時間と 24 時間のデータセンターモニタリングを実現しています。音声コール制御と音声サービスの要素はすべて、いずれかのデータセンターが利用できなくなった場合に、別のデータセンターへ自動的に移行（フェールオーバー）するように設計されています。フェールオーバープロセスはすべて自動的に実行され、ほぼリアルタイムで開始されます。プロビジョニングおよび設定用の Web インターフェイスを含むすべての運用サービス要素がアクティブ / スタンバイアーキテクチャで設計されているため、いずれかのデータセンターが利用できなくなった場合でも、別のデータセンターに手動で移行（フェールオーバー）できます。

8. Webex Calling の運用セキュリティ

8.1 セキュリティポリシー

情報、情報システム、およびすべての関連資産は、Webex Calling のビジネスプロセスにとって必須であり、極めて重要です。Webex Calling は、機密性、価値、重要性に応じて各情報資産を保護します。セキュリティ対策は、情報が保存されているメディア、情報を処理するシステム、または情報の転送に使用される方法に関係なく適用されます。

シスコは、セキュリティライフサイクル管理プロセスを使用して情報セキュリティポリシーを管理しています。このプロセスには、ポリシーに焦点を当てた次の要素が含まれます。

- 認定、承認、実施
- 年次レビュー、更新（必要に応じて）、再認定
- 年次通達および意識向上トレーニング
- 例外管理

8.2 不正行為の検出

シスコは不正検出の重要性を認識しています。そのため、プラットフォーム全体の通話トラフィックを監視するシスコの運用チームやサポートチームを支援するために、Calling Detail Records（CDR）を使用して不正なアクティビティの発信パターンを分析する複雑で大規模なアプリケーションを開発しました。

8.3 情報の分類

情報の分類は、各資産に適切なレベルのセキュリティを適用するのに役立ちます。

管理機能とリソースにより、あらゆる種類のメディアの内部または外部への配信が厳密に制御されます。制御には以下の処理が含まれます。

- データの機密性を判別できるようにメディアを分類
- ビジネスまたは法律上の理由で不要になったメディアの破棄
- データを再構築できないようにするために複写資料の細断処理、焼却処理、またはパルプ化処理を行うかどうかの決定
- 廃棄資料の保管用コンテナの安全確保

8.4 資産管理

インフラストラクチャ資産管理とは、必要なレベルのサービスを最もコスト効率の高い方法で提供することを目的として、管理、財務、経済、エンジニアリング、その他の面で物理資産に適用される措置の総称です。

Webex Calling には、システムとコンポーネントのインフラストラクチャ資産管理インベントリが実装されています。このインベントリを使用することで、資産の所有者、連絡先情報、目的を正確かつ容易に判断できます。資産管理には、物理ホストと仮想マシンのインベントリが含まれる場合があります。

運用管理チームは、サービスプラットフォーム環境内に展開されているすべての資産に対して責任を負います。環境内に管理対象外の資産や不要な資産を展開することは許可されません。適切に管理されていない環境内で資産が発見された場合は、運用管理チームの責任下に置くか、環境から撤去ないし持ち込み禁止にする必要があります。

お客様に対しては、すべてのメディアのインベントリログを保持し、少なくとも年 1 回、または資産の移動、追加、変更、廃棄時にメディアインベントリの確認と更新を行うことが推奨されます。

8.5 職務分掌

職務分掌は、偶発的または意図的なシステム誤用のリスクを軽減する方法として実施されます。一人の人物が許可なく、または記録に残らない形で資産にアクセスしたり、変更を加えたり、使用したりすることは、ポリシー、プロセス、手順に関するデューデリジェンスにより防止されます。

イベントの開始とイベントの承認は別々に行われます。これらの制御の設計は、共謀の可能性に対する監視とガバナンスに可能することを目的としています。

IT インフラストラクチャとアプリケーションの開発環境、テスト環境、実稼働環境は、運用システムへの不正アクセスや変更のリスクを軽減するために分離されています。運用チームは、アクセスに関するビジネス要件とセキュリティ要件に基づいてアクセス制御手順を確立し、文書化して、レビューします。設定およびアプリケーションコードは、暗号化された安全なデータベースに保存されます。

8.6 ロギングとモニタリング

運用チームは、高可用性をサポートするための広範な運用プロセスに基づいて活動します。これらのプロセスには、主要な担当者、サポートおよび連絡プロセス、システムロギング、モニタリング、システムテストプロセス、ネットワークパフォーマンスの選択が含まれます。アラーム発生の原因になった異常は、シビラティ（重大度）に基づいて対処されます。

運用チームは、サーバネットワークのパフォーマンスを維持するために、すべてのサーバ、インターネット接続、遅延、可用性、帯域幅、シビラティ（重大度）を継続的に監視します。すべての運用ログとセキュリティログは、可用性を確保するために長期間保持されます。ネットワーク運用チームは、キャパシティプランニングの一環として、これらのログを定期的にレビューします。

8.7 ベンダー管理 – サプライヤとの関係

シスコは、Webex Calling に対して提供されるすべてのサードパーティサービスにおいてセキュリティリスク要件とコンプライアンス要件に準拠したセキュリティ態勢が確保されるように、ベンダー向けのセキュリティ評価プログラムを管理しています。このプログラムの一環として、主要ベンダーは定期的に再評価され、セキュリティ態勢に変更がないことが確認されます。

8.8 変更管理

変更管理はサービス管理の重要な要素であり、サービス提供ネットワークに変更を導入する際の標準的なプロセスになります。変更を適切に実装するには、変更管理が不可欠です。変更は、エンジニアリング、システムエンジニアリング、サービス管理、サポート、プロフェッショナルサービスなどのさまざまなグループ、さらにはお客様によって開始されます。

変更を適用するプロセスは、すべての組織の間で設計、レビュー、情報共有を行い、適切に告示された時間枠内に実施することが重要です。これにより、変更に関する情報をすべての関係者に提供し、あらゆる観点から問題を予測して、変更の発生を認識し、導入された変更に起因する異常な動作を特定することが可能になります。シスコは、Webex Calling の定期メンテナンスに関するリアルタイム情報を提供する公開 Web ページを管理しています。

8.9 人事

8.9.1 管理者と開発者の身辺調査

シスコは、特定の個人および団体の身辺調査に関連するプロセスと手順を定めた身辺調査ポリシーを制定しています。

8.9.2 雇用条件 - 許容される使用方法

シスコの資産を使用するか、シスコの資産にアクセスする従業員および外部の関係者に対しては、シスコのポリシーおよび IT ハンドブックで定められている許容可能な使用方法に関するポリシーが通達されます。すべての従業員と契約社員は、シスコのポリシーおよび IT ハンドブックを読み、理解した上で署名する必要があります。このポリシーに違反したことが判明した従業員には、解雇を含む懲戒処分が科せられることがあります。

8.10 トレーニング

すべての従業員はオリエンテーションプロセスの一環として広範なセキュリティトレーニングを受け、その後も毎年セキュリティトレーニングを受けます。職務によっては、追加のセキュリティ関連トレーニングが必要になる場合があります。

8.11 カスタマーサポート

カスタマー サポート エンジニアは、すべてのシステムコンポーネントの正常性を継続的に監視するツールを使用して、すべてのシステムとクライアント アプリケーションが稼働していることを確認します。これらのツールは、潜在的な問題がネットワークの運用に影響を与える前に解決できるよう、問題の兆候が発見されるとただちにアラートを発行します。これらのツールでは、問題解決手順（診断の実行など）を自動的に開始することもできます。

また、サポートエンジニアは、ネットワーク運用を監視してネットワークの緊急事態に対応するとともに、カスタマーサポートとお客様の間の重要な連絡窓口としても機能します。サポートエンジニアは、お客様から報告された問題を自動化された問題追跡システムに記録し、お客様が満足できるレベルで迅速に問題を解決するために必要な作業の調整を継続的に行います。

このポリシーと段階的サポート構造により、サポートインシデントを通じて個人データが第三者に漏洩することが防止されます。

8.12 情報セキュリティインシデント管理

シスコのインシデント対応計画管理マニュアルは、米国国立標準技術研究所（NIST）800-61 コンピュータセキュリティ処理ガイドに準拠しています。インシデント管理ポリシーは、ビジネスクリティカルなサービスを提供するサービス担当者、またはビジネスクリティカルなサービスをサポートするアプリケーション、ソフトウェア、ハードウェアを保守するサービス担当者に適用されます。

インシデント管理の目標は、通常のサービス運用をできるだけ迅速に回復し、ビジネス運用への影響を最小限に抑えることです。通常のサービス運用とは、合意されたサービスレベル契約（SLA）の制限内での運用と定義されます。

シスコは、セキュリティインシデント対応と評価を処理するためのポリシーと手順を文書化しています。セキュリティインシデントへの対応には、特定、文書化、情報共有、封じ込め、評価、修復、根絶という 7 つの段階があります。

8.13 ビジネスの継続性とディザスタリカバリ

Webex Calling 部門には、運用チーム向けの事業継続計画スクリプトが用意されています。Cisco Webex Calling 部門は、可用性を継続的に確保するために、複数のデータセンターの余剰キャパシティをはじめとする運用状況を管理しています。また、効果的な事業継続管理システムを確立して維持するための要件を定めた ISO 22301 のガイダンスに準拠して活動してます。

事業継続計画のテストは年に 1 回実施されます。実際にインシデントが発生した際には、将来の運用を評価および改善するために、フォローアップアクションと事後分析が実施されます。ビジネスへの影響分析は組織の設計に反映されます。また、運用上のコミットメントが一貫して満たされるようにするために、ビジネスへの影響分析では、運用上のさまざまな障害シナリオに関して評価されたリスクのレベルに応じて、ビジネス継続性システムとディザスタリカバリシステムが評価されます。

バックアップ手順の実装は Cisco Webex Calling 部門が行います。増分バックアップは毎日行われ、オフサイトに少なくとも 3 週間保存されます。また、週次の完全バックアップもオフサイトに少なくとも 3 週間保存され、一部のバックアップは数年間保存されます。バックアップは、2 つの冗長データセンターのストレージノードと、サードパーティの暗号化されたクラウドストレージに保存されます。バックアップの整合性は実際上少なくとも月に 1 回テストされ、年 1 回の非常事態計画のテストと合わせて、バックアップのテストも必要になります。

9. 業界標準とコンプライアンス

Webex Calling は ISO 27001:2013 認定を取得しており、ISO 27017:2015 および ISO 27018:2019 の追加管理策に照らして評価を行っています。また、ISO の再認定を受けるためのレビューを毎年実施しています。このほか、Webex Calling は、適用される Trust サービス基準と、これに関連したセキュリティ、可用性、機密保持、プライバシーについての管理策に対する SOC 2 Type 2 認証を取得しています。SOC 2 の認証も毎年実施されます。

Webex Calling は、次の標準規格に認定されています。

- ISO 27001: 2013
- ISO/IEC 27017:2015
- ISO/IEC 27018:2019
- セキュリティ、可用性、機密保持に適したトラストサービス基準の SOC 2 Type II
- SOC 2 Type II Privacy
- SOC 3

これらの標準に準拠するには、高度な運用セキュリティの維持、脆弱性評価と侵入テストの実施、サードパーティの監査機関による毎年の監査実施、インシデント対応時間の SLA の達成が必要になります。

Webex Calling は、米国保健福祉省（HHS）のセキュリティリスク アセスメント ツールに基づく HIPAA 自己評価に加え、自己調査による PCI DSS（クレジットカードデータ保護基準）v3.2.1 準拠の証明も行っています。

10. 透明性

シスコは、世界各国の警察および国家安全保障機関から顧客データの提供を要求または命令された場合に、データの公開に協力いたします。シスコは毎年 2 回（1 月 ～ 6 月、または 7 月 ～ 12 月にかかるレポート期間について）、このデータを公開します。他のテクノロジー企業と同様に、このデータは報告の時期に関する制限に準拠して、各レポート期間の終了時から 6 ヵ月後に公開されます。

詳細については、次の URL にアクセスしてください。
cisco.com/web/about/doing_business/trust-center/transparency-report.html

シスコは、Webex Calling サービスによって収集されるデータ、データの保護方法、およびそのデータの保持期間を記載したプライバシーデータシートを管理しています。

まとめ

現在、世界中の企業、組織、政府機関が重要なビジネスコミュニケーションに Webex Calling を利用しています。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。クラウドベースのテレフォニーソリューションでは、コールの発信、モバイル参加者の認証、Webex アプリおよび Webex Meetings サービスを使用したコラボレーションなど、さまざまなレベルのセキュリティを確保する必要があります。

Webex は、スケーラブルなアーキテクチャ、キャリアクラスの可用性、およびマルチレイヤセキュリティを提供します。これらの要因が社内規定およびサードパーティによって定められた厳格な業界標準に準拠しているかどうかは継続的に検証および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。

Webex Calling の 90 日間無料トライアルを開始するには、シスコセールスまでご連絡ください。

Webex コラボレーション プラットフォームのセキュリティについて詳しくは、こちらをご覧ください。

Webex Meetings のセキュリティについて詳しくは、こちらをご覧ください。

Webex のシングルプラットフォームの利点については、こちらをご覧ください。

詳細情報
webex.com をご覧ください

2021 年 7 月