Cisco Webex

The bridge to possible

Control Hub

データセキュリティとプライバシー

目次

セキュリティとプライバシーの概要

企業がクラウド サービスを利用する主な利点の 1 つは、クラウド サービス プロバイダーが展開した付加価値の高い機能をすぐに活用できることです。しかし、多くのクラウド プロバイダーが意味する「付加価値」とは、ユーザのデータとコンテンツにすべてアクセスできるということです。コラボレーションのアプリケーションについて、ほとんどのクラウド事業者では、メッセージやコール、会議のコンテンツに直接アクセスすることで、メッセージ検索やコンテンツ変換、サードパーティ製アプリケーションとのインテグレーションを実現しています。一方、最新のコンシューマ コラボレーション サービスは、付加価値機能を犠牲にしてエンドツーエンドの暗号化を提供することで、利用者のプライバシーを保護することを目指す傾向にあります。

Webex はこの両者の長所を採り入れおり、エンドツーエンドで暗号化されたクラウド コラボレーション プラットフォームであると同時に、サードパーティとの連携により付加価値を提供することも可能です。Webex は、暗号キーを安全に配布するためのオープン アーキテクチャに基づいているため、企業は暗号キーの管理とデータの機密性をコントロールできます。つまり、コンテンツはユーザーの Webex アプリで暗号化され、受け取り相手に届くまで暗号化されたままになります。明示的にアクセスを許可することを選択しない限り、間に入ってコンテンツの暗号化解除キーにアクセスすることはできません。

セキュリティ侵害による影響は甚大になることがあるため、Webex ではインテグレーションと制御を導入することで、顧客がセキュリティポリシーの適用を管理できるようにしました。Control Hub は、Webex サービスのプロビジョニングと管理を直感的に行うことができる Web ベースの一元管理ポータルです。

Pro Pack for Control Hub は、さらに高度な機能や、既存のソフトウェア（コンプライアンス、セキュリティ、分析）との連携を必要とするお客様向けのプレミアム サービスです。

セキュリティの差別化要因

- Webex のゼロトラストセキュリティは、予約会議とパーソナル会議に対して、オープン標準に基づいたエンドツーエンド暗号化と強力な本人確認機能を提供しています。会議をエンドツーエンドで暗号化することで、お客様が会議の暗号鍵を独占制御できるため、シスコや他の誰も無断で会議の内容を知ることはできなくなります。本人確認と組み合わせた標準ベースのエンドツーエンドで暗号化された会議は、他のコラボレーション事業者では提供されていません。
- ユーザが生成したデータに対する Webex ベースライン セキュリティは、コラボレーション ソリューション市場で最も強力です。他のコラボレーション ベンダーが提供するセキュリティでは、伝送中のデータ、デバイス上にあるデータ、保管されているデータがさまざまなソリューションで段階的に暗号化されることがよくあります。
- お客様が暗号鍵をオンプレミスで（ハイブリッド データ セキュリティ（HDS）を使用して）保持できることも、Webex が競合製品とは異なる点です。お客様は暗号鍵の保管場所を管理できるだけでなく、暗号鍵のコンプライアンスおよび検索サービスをオンプレミス環境に構築することができます。HDS では、コンプライアンスおよび検索サービスのための暗号化されていないコンテンツは、Webex プラットフォーム上ではなくお客様の安全なデータセンターで処理します。

- Webex プラットフォームでは、暗号化されていないコンテンツを扱う鍵やサービスとはまったく別の領域に、暗号化されたコンテンツが保管されます。このレベルのデータ セキュリティを実現しても、Webex のコンテンツ検索、e-discovery、アーカイブ機能、データ損失防止（DLP）などのエンタープライズ グレードの機能に妥協はありません。

Webex Meetings のエンドツーエンドの暗号化と本人確認

Webex のゼロトラストセキュリティでは、予約会議とパーソナル会議に対して、オープン標準に基づいたエンドツーエンド暗号化と強力な本人確認機能を提供することで、あらゆる攻撃から会議を守ります。ミーティングの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のホワイトペーパー」を参照してください。

エンドツーエンドで暗号化された会議では、ゼロトラストセキュリティは以下をサポートします。

- 標準規格に準拠した暗号化
- エンドツーエンドの本人確認（E2EI）
- Webex Room デバイス （Room シリーズ、Desk シリーズ、Board シリーズ）
- パーソナル会議室のエンドツーエンド暗号化 (E2EE)
- 会議が安全であり、会議でエンドツーエンドの暗号化が有効になっていることが一目で参加者にわかるセキュリティ アイコン
- 新しいセキュリティ検証コードを使用したミーティング参加者の口頭による検証

クラウド鍵管理サービスを利用したデータセキュリティ

プラットフォーム ベースの鍵管理サービス（クラウド KMS）はすべてのお客様がデフォルトで利用できます。このサービスにより、コンテンツはユーザーの Webex アプリで暗号化されてから送信されます。 この基本機能によって、すべての顧客に対して KMS とエンドツーエンド暗号化を常に提供することができます。

クラウド KMS により、Webex ユーザーは次のことを実現できます。

- マスターキーは、クラウドのハードウェア セキュリティ モジュール（HSM）によって保護されています。
- 暗号化されたコンテンツの保存と伝送を担うサービスと、暗号化とセキュリティ キーの管理を担うサービスの明確な分離
- クラウド KMS と Webex アプリまたは Webex 登録デバイスの間でキーを交換するためにエンドツーエンドで暗号化されたチャネル
- クラウド KMS で管理される共通鍵を用いた業界標準の暗号化方式を用いたユーザーコンテンツの暗号化（Webex スペースごとに少なくとも 1 つのキー）
- ユーザのアクセス トークンを使用した、キーへのアクセス許可の管理
- 暗号化された検索機能
- e-discovery、DLP API、アーカイブ機能などのエンタープライズ機能（復号化は境界で実施、管理者によって認可）

ハイブリッド データ セキュリティによるデータセキュリティ

セキュリティを重視する企業のお客様は、KMS を含むセキュリティ レルム サービスを自社内に展開できます。これはクラウド KMS を使用する場合と変わりませんが、キーの取得とアクセスがサーバのオンプレミス展開で行われる点が異なります。

Hybrid Data Security（HDS）の特長は次のとおりです。

- Pro Pack for Control Hub を使用したオンプレミス展開とセキュリティレルムの管理
- KMS とストレージ
- 透過的プロキシと明示的プロキシの両方の検査と非検査の両方をサポートする展開（外部 DNS 解決がブロックされるモードを含む）
- 検索インデクサ：暗号化されたコンテンツを安全に検索する機能
- オンプレミスの e-discovery エンジン：e-discovery ユーザ インターフェイスはクラウドでホストされますが、独自のデータ センターに HDS を展開することを選択したお客様のために、エンジンはオンプレミスに留まります。
- HDS ノードとデータベースサーバー間での暗号化された接続
- プロキシのサポート: 透過的な非検査、透過的なトンネリング、明示的およびブロックされた外部 DNS 解決環境のサポート
- 自動のアップグレード、アラート、通知
- オンプレミスの「持ち込み」syslog を使用したキー アクセスのローカル ログと監査

データ セキュリティ機能

表 1 に Webex のデータ セキュリティ機能をまとめました。

表 1. データ セキュリティ機能

機能	標準オファーまたは Pro Pack が必要	説明
会議のエンドツーエンド暗号化	標準オファー	Webex は予約会議とパーソナル会議に対して、オープン標準に基づいたエンドツーエンド暗号化と強力な本人確認機能を提供しています。エンドツーエンドで暗号化された会議では、お客様は会議の暗号キーを独自に制御できるため、シスコだけでなく誰も会議コンテンツに無断でアクセスできなくなります。
コンテンツのエンドツーエンド暗号化 注：メッセージ、ファイル アップロード、スペース名、会議の議題、デバイスのニックネーム、Webex Board コンテンツなど、ユーザー生成コンテンツが含まれます。	標準オファー	業界最先端の暗号化により、Webex ではメッセージ、ファイル、ホワイトボードをいつでも安全に利用することができます。Webex はデータの送信前にデバイスにて暗号化します。その際は KMS で動的に生成された鍵を利用します。クラウドに送信中でも、処理中でも、保管中でも、データは常に暗号化されたままです。KMS は、Webex アプリでコンテンツの暗号化と

機能	標準オファーまたは Pro Pack が必要	説明
		復号化に使用される暗号キーの作成、管理、およびアクセス許可を担います。

機能	標準オファーまたは Pro Pack が必要	説明
伝送中の暗号化	標準オファー	すべての Webex Messaging の Web 通信には安全な HTTPS が利用されています。（Mac、Windows、iPhone、Android、web ブラウザ、Cisco クラウド） 同様に、Webex デバイスからのすべての Web トランザクション（たとえば、Webex Room デバイス、IP 電話、Webex Board）にも HTTPS が使用されます。クラウド上の Web API（developer.webex.com）は、HTTPS を使用します。HTTP はサポートされていません。つまり、クラウドでのすべての送受信データは暗号化されます。HTTPS は Control Hub の送受信データの保護にも使用されます。Webex のすべてのメディア（音声、ビデオ、デスクトップ共有、ホワイトボードなど）は Secure Real-Time Transport Protocol（SRTP、RFC 3711 で定義）で送信されます。現在はプラットフォームにて、ミキシングや分離、電話網との接続、配信といった用途のためにリアルタイムメディアは復号化されます。
暗号化されたコンテンツの検索	標準オファー	暗号化されたコンテンツを Cisco Collaboration Cloud が受信すると、すべてのユーザ生成メッセージの検索インデックスが作成されます。検索インデックスは、動的キーを使用して一方向にハッシュされてから格納されます。エンドユーザーが Webex で単語を検索すると、その単語はアプリで暗号化されてから送信されます。単語は適切にハッシュされ、以前に暗号化されて保存された検索語に照らして検索されます。一致する単語が取得され、アプリに送信され、復号化されてからエンド ユーザに表示されます。
ハイブリッド データ セキュリティ お客様管理のデータセキュリティ	Pro Pack が必要	企業は、コンテンツの暗号化に使用するキーを管理および保存するサービスと、検索インデックスのハッシュを生成するサービスの両方を展開できます。この展開では、外部 DNS 解決がブロックされるモードを含め、透過プロキシと明示的プロキシの両方についての検査と非検査の両方がサポートされます。これらの機能を利用することで、企業のお客様は、ユーザのキーが物理的に格納される場所を選択して、セキュリティをさらに確実なものにすることができます。サービスを円滑に開始できるように、この機能を展開した後には、選択したユーザを対象に当初は試用モードで機能を運用する必要があります。詳細については、『導入ガイド』を参照してください。

アプリケーションおよびモバイル デバイスのセキュリティ管理

概要

Webex アプリケーションはエンタープライズグレードで、Webex はお客様のセキュリティ ニーズに応えます。エンタープライズ IT は、ユーザに展開するアプリケーションのセキュリティの基本コントロールが必要です。Webex で使用可能なコントロールには、PIN ロックの適用、モバイルデバイスにキャッシュされた Webex コンテンツのトークンの取り消しとリモートワイプ、Webex Web アクセス時のアイドル セッション タイムアウトなどの機能が含まれます。

アクセスのリセット

ユーザ プロファイルで、管理者はユーザのアクセス権を取り消すことができます。これにより、すべてのアクセス権が削除され、そのユーザのトークンが更新されます。ユーザが認証されているモバイル デバイスにキャッシュされたすべてのコンテンツもリモートでワイプされます。この機能の一般的な使用例は、ユーザがモバイル デバイスを紛失した場合や、ユーザが退職してもまだ Webex へのプロビジョニングが解除されていない場合です。

モバイル デバイスのセキュリティ管理

iPhone および Android 用の Webex アプリは、次のエンタープライズ グレードのセキュリティ機能を利用できます。

- サポートされているすべての Webex 認証（パスワードベースまたはシングルサインオンベース）で認証用 OAuth トークンが生成されます。生成されたアクセス トークンはクライアントで更新されます。プロビジョニング解除やトークン失効などの特定のイベントが発生しない限り、再認証は必要ありません。
- 動的キーを使用したエンドツーエンド暗号化。
- Webex サービス、およびユーザ組織が定義した定義 KMS（Webex プラットフォームまたは HDS）へのセキュア な Transport Layer Security（TLS）接続。
- Pin ロックの有効化（ProPack が必要）。この機能が有効である場合は、ユーザーは PIN ロックまたはパスコードでデバイスを保護する必要があります。これにより、デバイスを置き忘れたり紛失したりした場合や、デバイスが不適切な人の手に渡ってしまった場合に、Webex アプリの企業コンテンツにアクセスできなくなります。
- ユーザーが Webex へのプロビジョニングを解除された場合や、ユーザーのアクセストークンが管理者によって取り消された場合に、モバイルデバイスにキャッシュされたコンテンツをリモートでワイプできます。
- モバイルデバイスのロック画面でメッセージ プレビューを無効にして、近くのユーザーが通知プレビュー経由で配信されたメッセージを覗き見できないようにします。また、デバイスがロックされたまま置き忘れられている場合でも、他のユーザーが、デバイスのロックされた画面に表示されているメッセージのプレビューを見続けることはできません。
- 管理されていないアプリの使用を無効にして、ユーザーが Webex アプリの企業管理バージョンのみを使用できるようにし、組織のセキュリティとコンプライアンスポリシーに準拠できるようにします。

- モバイルアプリ用 Webex で暗号化。
- 基本的なモバイル デバイス管理（MDM）サポートは、Mobile Iron、Cisco Meraki® Systems Manager、AirWatch、MaaS360 などのさまざまなベンダーに認定されています。

Webex アプリケーションとモバイル デバイスのセキュリティ機能

表 2 にアプリケーションとモバイル デバイスのセキュリティ管理をまとめました。

表 2. アプリケーションとモバイルデバイスのセキュリティ管理

機能	標準オファーまたは Pro Pack が必要	利点
PIN ロックの適用 注：iOS と Android スマートフォンのみ。Chromebook は含まれません。	Pro Pack が必要	企業の管理者が PIN ロックの適用を有効にすると、iPhone および Android 用の Webex ユーザーはモバイルアプリの特定の機能を使用する際にデバイスの PIN ロックを有効にしないとアプリを使用できなくなります。この機能は、Webex アプリのコンテンツのセキュリティ維持に役立ちます。
管理者によるリモート ワイプとアクセスのリセット	Pro Pack が必要	ユーザーがモバイルデバイスを紛失した場合や、離職した場合に、管理者はすべてのアクセス権を取り消し、Webex にキャッシュされたコンテンツをモバイルデバイス（iPhone と Android）からワイプすることで、企業コンテンツのセキュリティを維持できます。
モバイルデバイスのロック画面でメッセージのプレビューを無効にする	Pro Pack が必要	お客様は、モバイル通知のメッセージプレビューを常に無効にして、交換されるメッセージを近くのユーザーがのぞき込めないようにすることが可能です。また、デバイスがロックされたまま置き忘れられている場合でも、他のユーザーが、デバイスのロックされた画面に表示されているメッセージのプレビューを見続けることはできません。
管理対象外アプリの使用を無効化	Pro Pack が必要	管理者は、ユーザーを Webex アプリの企業管理バージョンに制限することを選択できます。Control Hub でこの設定を有効にすると、ユーザーは Apple App Store/Google Play ストアから、または他の方法でダウンロードした Webex アプリの管理対象外バージョンを使用できなくなります。
ファイル共有コントロール	Pro Pack が必要	ロックダウンされた環境を使用するお客様は、ユーザーが優先クライアントタイプ（モバイルではなくデスクトップなど）、指定 IP 範囲または Active Directory グループからのみ、ファイルのアップロードとダウンロードを実行できるようにすることが可能です。
基本的な MDM サポート	標準オファー	Webex モバイルアプリの管理には MDM プロバイダーを利用し、デバイスに対してセキュリティ管理を有効にすることで、データの漏洩や流出を防ぐことができます。 • コピー/ペースト、バックアップ、ドキュメント共有の無効化 • デバイスレベルでパスコードとリモートワイプを適用 注：このサポートは特に Meraki Systems Manager、VMware AirWatch、Mobile Iron、IBM MaaS360 で検証されていますが、基本コントロールはアプリ構成コミュニティ標準規格を確認したほとんどの MDM プロバイダーに対して機能するはずです。
MAM: Intune SDK の統合	標準オファー	Webex モバイルアプリケーションは、Microsoft Intune とソフトウェア開発キット（SDK）の統合をサポートしています。IT 管理者は、この SDK を利用することで、Webex Meetings および Messaging のアプリケーション機能と設定ポリシーにユーザーがアクセスするのを制御し、企業データを管理/保護できます。

機能	標準オファーまたは Pro Pack が必要	利点
MAM アプリのラッピング	標準オファー	BYOD 環境をサポートするお客様は、通常、エンタープライズ アプリケーションのコンテナ化が必要です。お客様が選択した MAM プロバイダから Webex モバイルアプリのラッピングを実行できるオプションを使用すると、管理せずにモバイルデバイス向けの企業コンプライアンス要件に準拠しながら、ユーザーに対してシームレスに Webex アプリを導入できます。
外部通信制御	Pro Pack が必要	企業は、情報セキュリティやデータ損失の懸念から、外部通信を許可しないことを選択できます。その結果、組織内のユーザは組織が所有するスペースに組織外のユーザを追加できず、組織内のユーザは外部スペースに参加できなくなります。 ゲストを招いた会議と通話は引き続き可能です。

エンドポイント接続

Webex では、すでに展開されているプロキシを使用して、クラウドへのシームレスな接続がサポートされます。サポートされている認証タイプには、NoAuth、Basic、および NTLM（モバイルとデスクトップ クライアント）、ダイジェスト ベースの認証（モバイル クライアント）、TLS インターセプト プロキシ（デスクトップ クライアント）などがあります。サポートされているプロキシ構成方法は、手動構成、プロキシ自動構成（PAC）、および Web プロキシの自動検出（WPAD）です。グループ ポリシー オブジェクト（GPO）は、Windows クライアントでのみサポートされます。

Webex でプロキシがサポートされるようになったため、プロキシの許可リスト登録は不要になりました。プロキシサポートを有効にするためのネットワーク要件については、次の 2 つの記事を参照してください。

- Webex Meetings のネットワーク要件
- Webex Services のネットワーク要件

認定、標準規格、および規制への遵守

Webex はいくつもの業界標準に準拠していると認定されており、多くの国際的内部統制フレームワークおよび規制への遵守を維持しているため、世界中で販売が可能です（図 1）。それらの認定と法規制は次のとおりです。

- ISO/IEC 27001:2013、27017:2015、27018:2019、27701:2019
- CSA STAR レベル 2 認定（CSA STAR 認証クラウドプロバイダバッジ込み）
- SOC 2 Type II
- 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）
- サードパーティによる検証済み HIPAA 構成証明（近日公開）を通じて HIPPA コンプライアンスを有効化
- スペイン ENS High
- FedRamp 認定 Meetings

- EU - 米国間のプライバシー シールド
- スイス - 米国間のプライバシーシールド
- APEC クロスボーダー プライバシー ルール
- 拘束力のある企業ルール
- EU モデル契約条項
- EU GDPR 行動規範

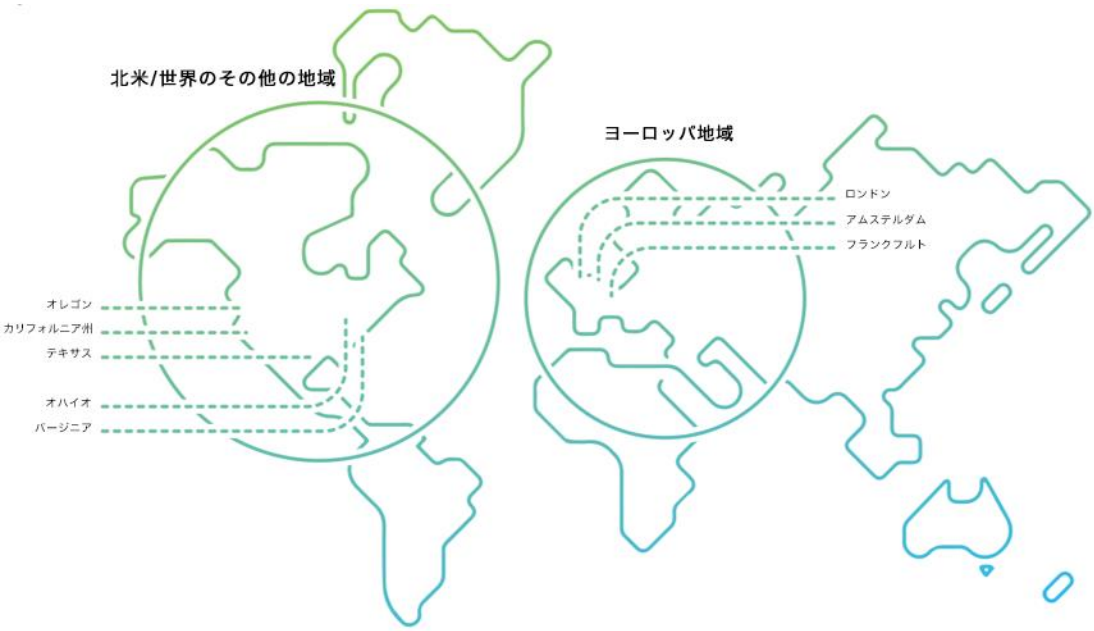

図 1.
地域

データの局所性

EU データ レジデンシーは、選択、信頼、革新でリードするという当社のコミットメントと戦略の一部です。データ レジデンシーを検討するお客様にとって重要な要素は、データの取り扱いが EU データ保護基準を満たしていること、および公的機関によるデータへのアクセスを確実に管理できるようにすることです。

Cisco は、ドイツのフランクフルトに Webex データセンターを置き、アムステルダム（オランダ）の 2 番目のデータセンターと組み合わせて、バックアップ、レジリエンシ、および可用性を提供します。EU のお客様は、EU 内でデータを保存して処理できるようになりました。これには、ユーザー ID、ミーティングの記録、共有ファイル、チャットなどで生成されたユーザー、暗号化キーなどが含まれ、すべてお客様の日常の Webex エクスペリエンスの一部となります。

Cisco Capital

目的達成に役立つ柔軟な支払いソリューション

Cisco Capital により、目標を達成するための適切なテクノロジーを簡単に取得し、ビジネス変革を実現し、競争力を維持できます。総所有コスト（TCO）の削減、資金の節約、成長の促進に役立ちます。シスコの柔軟な支払いソリューションは 100 か国以上で利用可能であり、ハードウェア、ソフトウェア、サービス、およびサードパーティ製の補完的な機器を、利用しやすい計画的な支払方法で購入できます。詳細はこちらをご覧ください。

米国本社
Cisco Systems, Inc.
サンノゼ(カリフォルニア州)

アジア太平洋本社
Cisco Systems (USA) Pte. Ltd.
シンガポール

ヨーロッパ本社
Cisco Systems International BV Amsterdam,
アムステルダム(オランダ)

シスコは世界各国 200 箇所にオフィスを開設しています。各オフィスの住所、電話番号、FAX 番号は当社の Web サイト(https://www.cisco.com/go/offices [英語])をご覧ください。

Printed in USA C78-740771-02 01/22