Cisco Webex Control Hub (データ セキュリティとプライバシー)

Contents

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 アプリケーションでは、ほとんどのクラウド プロバイダーは、メッセージ検索、コンテンツ トランスコーディング、サードパーティ アプリケーションとの統合などの機能を提供するために、メッセージ、コール、会議のコンテンツに直接アクセスします。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。

Cisco Webex® は両方の長所が生かされたクラウド コラボレーション プラットフォームであり、データはエンドツーエンドで暗号化されますが、付加価値を提供するシスコとサードパーティの統合を利用できる場合は、企業はそれを選択できます。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の Cisco Webex Teams アプリで暗号化され、受信者に到達するまで暗号化されたままになり、企業が明示的にそのようなアクセスを許可することを選択しない限り、コンテンツの暗号化解除キーにアクセスできる仲介者はいません。

侵害の影響は深刻になる可能性があるため、お客様がセキュリティ ポリシーの適用を管理できるように、シスコは Webex ポートフォリオに統合と制御の仕組みを導入しました。Cisco®Webex 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 Webex Control Hub は、高度な機能と、既存のコンプライアンス、セキュリティ、分析ソフトウェアとの統合を必要とするお客様向けのプレミアム サービスです。

Webex セキュリティの違い

- 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。Webex Teams での暗号化は本当のエンド ツー エンドですが、そのような暗号化を実現するエンタープライズ メッセージング システムは現在ほかにありません。
- Webex ではお客様が（Webex Hybrid Data Security（HDS）を使用して）オンプレミスでキーを保持できることも、競合他社とは異なる点です。お客様はキー ストレージを管理できるだけでなく、コンプライアンスと検索のサービスをオンプレミスでホストすることもできます。HDS では、コンプライアンスと検索のサービスのために暗号化されていないコンテンツは Webex プラットフォームではなくお客様の安全なデータセンターで処理されます。
- 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処理するキーやサービスのストレージとは別の領域に、暗号化されたコンテンツが常に格納されます。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。

クラウド キー管理サービスを利用した Webex データ セキュリティ

Webex プラットフォーム ベースのキー管理サービス（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の Webex Teams™ アプリで暗号化されてから送信されます。このベースラインにより、オンライン オファー コンシューマを含むすべてのお客様に KMS とエンドツーエンドの暗号化を提供できます。

クラウド KMS では、すべての Webex Teams ユーザを対象に次のことを実現できます。

- 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 Teams 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
- ユーザ生成コンテンツの暗号化にクラウド KMS で管理される対称キーを使用する業界標準の暗号化（Webex Teams 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
- 管理者が許可する e-discovery、DLP API、アーカイブ機能などのエンタープライズ機能（復号化は境界で行われる）

Hybrid Data Security による Webex 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 サービスを独自のオンプレミスに展開できます。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 Webex 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 Webex Teams 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。
- 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

Webex 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
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、Cisco Webex Board コンテンツなど、ユーザ生成コンテンツが含まれます。**	標準オファー	Webex Teams では業界の主要な暗号化が使用されますので、秘密を守りながら Webex のメッセージ、ファイル、ホワイトボードを安全に利用できます。Webex Teams アプリケーションでは、KMS からの動的キーを使用してデータがデバイスで暗号化されてから送信されます。データはクラウド サーバに送信されているときも、処理されているとき（使用中データ）も、保管されるとき（保管データ）も、暗号化されたままになります。KMS は、Webex Teams アプリでコンテンツの暗号化と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。
伝送中の暗号化	標準オファー	Mac、Windows、iPhone、Android 用の Webex Teams と Web とシスコのクラウドの間でのすべての Web トランザクションには、セキュアな HTTPS が使用されます。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。Cisco® Collaboration Cloud（developer.webex.com）の Web API でも HTTPS が使用されます。HTTP はサポートされていません。つまり、Cisco Collaboration Cloud の送受信データはすべて暗号化されます。HTTPS は Webex 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 Webex プラットフォームでは、混合、配信、PSTN トランキング、および分界のためにリアルタイム メディアが復号化されます。
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 ユーザが Webex Teams 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。

機能	標準オファーまたは Pro Pack が必要	説明
Hybrid Data Security（お客様が管理する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。

よくある質問

Q. コンテンツの暗号化にはどのような暗号化アルゴリズムが使用されますか。

A. Webex Teams のコンテンツの暗号化に使用される対称暗号は AES-256 GCM です。

Q. KMS に対して定義されたインターネット技術特別調査委員会（IETF）プロトコルはありますか。

A. Webex はデータ保護のオープン スタンダードとプロトコルに基づいており、シスコが設計してインターネット標準として公に提案したキー管理仕様が含まれています。

Q. HDS はどうやって入手できますか。

A. HDS は Pro Pack for Webex Control Hub の一部として購入可能な多くの機能の 1 つです。

Q. HDS の詳細な導入ガイドはありますか。

A. https://www.cisco.com/go/hybrid-data-security を参照してください。

Q. HDS によってどのような追加のセキュリティが保証されますか。

A. 組織が生成および所有するキーを HDS で物理的に管理できます。特定のクラウド サービスがこれらのキーにアクセスできますが、セキュリティを重視する組織がクラウド内の暗号化されたコンテンツからキーを分離すると、攻撃者は暗号化されたコンテンツとキーの両方にアクセスできなければ、外部からの攻撃でコンテンツを侵害することができなくなります。

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

Cisco Webex Teams アプリケーションはエンタープライズ グレードです。シスコは Webex プラットフォームで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 Teams 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 Teams コンテンツのトークンの取り消しとリモート ワイプ、Web アイドル セッション タイムアウトの Webex Teams 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 アプリ用の Cisco Webex Teams では、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。
- Cisco Webex サービス、およびユーザ組織が定義した定義 KMS（Cisco 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 ロックが有効な場合の要件（Pro Pack が必要）。この機能が有効である場合は、ユーザは 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 Teams アプリのエンタープライズ コンテンツにアクセスできなくなります。
- ユーザが Webex へのプロビジョニングを解除された場合や、ユーザのアクセス 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 アプリ用 Webex Teams での保存データの暗号化。
- 基本的なモバイル デバイス管理（MDM）サポートは、Cisco Meraki®Systems Manager と AirWatch に対しては認定されていますが、これらのプロバイダーに限定されません。

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.　アプリケーションおよびモバイル デバイスのセキュリティ管理機能

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 Cisco Webex Teams ユーザはモバイル 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 Teams 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 Teams 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、企業のコンテンツ セキュリティを維持できます。

機能	標準オファーまたは Pro Pack が必要	利点
ファイル共有コントロール	Pro Pack が必要	企業は、データ漏洩の懸念がある場合や、コンプライアンスまたは規制上の理由から他のファイル管理ベンダーが存在する場合に、Webex ファイル共有を使用しないことを選択できます。
基本的な MDM サポート	標準オファー	Webex Teams のモバイル 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、ドキュメント共有を無効にする。 • デバイス レベルでパスコードとリモート ワイプを適用する。 注：このサポートは特に Meraki Systems Manager と VMware AirWatch で検証されていますが、基本コントロールはほとんどの MDM プロバイダーに対して機能するはずです。
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。

よくある質問

Q. Cisco Webex は特定の MDM プロバイダーに対して認定されていますか。

A. はい。

Q. 管理者はどのように PIN ロック適用機能にアクセスできますか。

A. これはプレミアム機能であり、Pro Pack for Webex Control Hub で有効になります。アドオン オファーを購入すると、[設定（Settings）] で利用できるようになります。

Q. セキュリティ管理は追加されますか。

A. はい。Webex はクラウド サービスであり、継続的な管理と可視性のために新機能は継続して追加されます。

エンドポイント接続

Cisco 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、プロキシのホワイトリスト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。

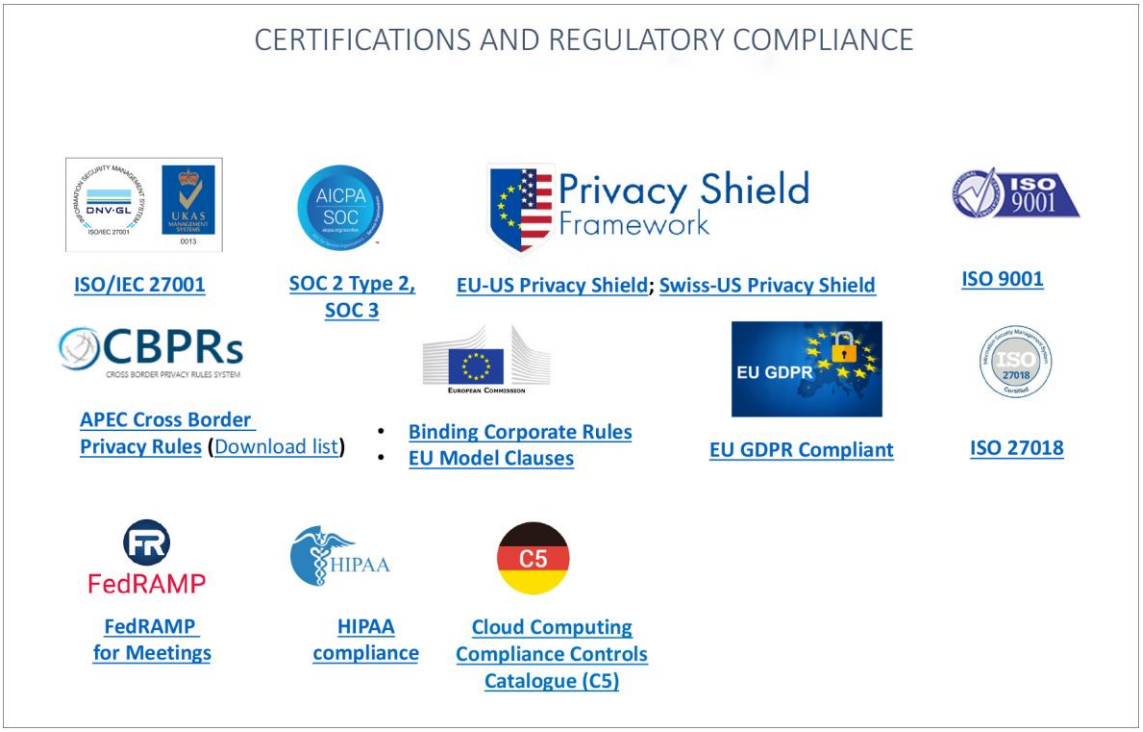
Cisco Webex のネットワーク要件：https://collaborationhelp.cisco.com/article/en-us/WBX264

Cisco Webex Teams Services のネットワーク要件：https://collaborationhelp.cisco.com/article/en-us/WBX000028782

認定と法規制の遵守

Cisco Webex はいくつもの標準に準拠していると認定されており、多くの国際的な法規制を遵守しているため、世界中で販売可能です（図 1）。それらの認定と法規制は次のとおりです。

- ISO/IEC 27001, 27017
- ISO 27018
- SOC 2 タイプ 1 およびタイプ 2
- 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）
- 医療機関のお客様が使用するための HIPAA 自己評価による HIPAA 準拠
- 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



データの局所性

Cisco Webex を欧州でご利用のお客様は、欧州のデータ センターでのユーザ ID と暗号キーのプロビジョニングを選択できます。詳細については、データの局所性の概要を参照してください。Cisco Webex の認定と法規制の遵守

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。100 ヵ国あまりの国々では、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の補助機器を購入するのに、シスコの柔軟な支払いソリューションを利用して、簡単かつ計画的に支払うことができます。 詳細はこちらをご覧ください。

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

米国で印刷

C78-740771-01 09/19