Cisco Webex Control Hub

(データ セキュリティとプライバシー)

データ セキュリティとプライバシーの概要

クラウドサービスを利用する事によって企業が獲得できる大きな利点の一つは、付加価値のある機能やサービスを、サービスが導入された時点ですぐに活用できる事です。しかし多くのクラウドサービスプロバイダでは、「付加価値」の実現のために、ユーザのデータやコンテンツに完全にアクセス可能である事を意味しており、ほとんどのクラウドサービスプロバイダが提供するコラボレーション アプリケーションでは、メッセージ検索、コンテンツのトランスコード、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実現するために、メッセージ、コール、会議コンテンツに直接アクセスできるようになっています。一方で、新たなコンシューマ コラボレーション サービスでは、付加価値機能を制限してでもエンドツーエンドの暗号化を可能にして、コンシューマのプライバシーを保護する傾向にあります。

Cisco Webex® はこの両者の長所を採り入れており、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 では、暗号化キーをセキュアに配布できるオープン アーキテクチャが採用されているため、企業は暗号化キーとデータの機密性を管理する事が可能です。それにより、コンテンツはユーザの Cisco Webex Teams アプリケーションで暗号化され、受信者に到達するまで暗号化が保持されます。企業が明示的に許可しない限り、このコンテンツの暗号化キーにはアクセスできません。

セキュリティ問題の影響は深刻である可能性があるため、シスコは Webex ポートフォリオにサードパーティ連携とコントロールを導入し、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しています。Cisco Webex Control Hub は、Webex® サービスのプロビジョニングと管理を可能にする、Web ベースの直感的で使いやすい一括管理ポータルです。

Pro Pack for Webex 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。

Webex セキュリティの差別化要因

- ユーザ生成データの 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な差別化要因の 1 つです。多くの場合、セキュリティは、さまざまなソリューションを使用して、送信中、デバイスに保管中、ストレージ内のデータを段階的に暗号化することにより提供されます。現在、他のエンタープライズ メッセージング サービスには、Webex Teams によって提供されるようなエンドツーエンドの暗号化を提供しているものはありません。
- また、お客様がキーをオンプレミスで（Webex 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 を競合製品と差別化する要因です。なぜなら、お客様はキーの保管を管理できるだけでなく、キー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できるからです。HDS 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、コンプライアンスおよび検索サービスに関する暗号化されていないコンテンツを処理します。
- Webex プラットフォームは常に、暗号化されていないコンテンツを処理するキーおよび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を保管します。このレベルのデータ セキュリティを実現している一方で、Webex は、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関して妥協していません。

クラウド キー管理サービスを使用した 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）はデフォルトで使用可能です。すべてのお客様は、自身のコンテンツがユーザの Webex Teams アプリケーションを離れる前に、それを暗号化することができます。オンライン オファーの利用者を含む、すべてのお客様に対するこのベースラインは、シスコが常に KMS およびエンドツーエンドの暗号化を提供することを保証します。

クラウド KMS では、すべての Webex Teams のユーザは以下を実現できます。

- 暗号化されたコンテンツのストレージとトランスポートを処理するサービスと、暗号化およびセキュリティ キー管理を処理するサービスを明確に分離
- クラウド KMS と Webex Teams アプリケーションまたはキーを交換するための Webex 登録デバイスの間のエンドツーエンドの暗号化チャネル
- クラウド KMS によって管理される対称キーを使用した、ユーザ生成コンテンツの業界標準の暗号化（Webex Teams スペースごとに最低 1 つのキー）
- ユーザのアクセス トークンを使用してキーにアクセスするための制御された認証
- 暗号化された検索機能
- 管理者によって承認された、e-discovery、DLP API、アーカイブ機能などのエンタープライズ機能（境界で復号化が実行される）

ハイブリッド データ セキュリティによる Webex データ セキュリティ

セキュリティへの関心が高い企業のお客様は自社で、セキュリティ レルム サービス（KMS を含む）の導入を選択できます。これは、キーがサーバのオンプレミスの導入によって取得およびアクセスすることを除いて、クラウド KMS を使用した場合と変わりません。

ハイブリッド データ セキュリティ（HDS）には次のものが含まれます。

- Pro Pack for Webex Control Hub によるセキュリティ レルムのオンプレミス導入と管理
- KMS とストレージ
- 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
- e-discovery オンプレミス 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ているが、自社データセンターに HDS を導入することを選ぶお客様向けに、エンジンをオンプレミスでホスト可能
- 自動アップデート、アラート、および通知
- ローカル ログおよびオンプレミスの「持ち込み」の syslog を使用するキーへのアクセスの監査

Webex データ セキュリティ機能

表 1 に、Webex データ セキュリティ機能の概要を示します。

表 1. データ セキュリティ機能

機能	標準オファー/ Pro Pack が必要	説明
コンテンツのエンドツーエンドの暗号化 **注：メッセージ、ファイルのアップロード、スペース名、会議の件名、デバイスのニックネーム、Cisco Webex Board のコンテンツなどのユーザ生成コンテンツが含まれます。**	標準オファー	Webex Teams は業界トップクラスの暗号化を使用して、Webex メッセージ、ファイル、およびホワイトボードの機密性、可用性、およびセキュリティを常に確保します。Webex Teams アプリケーションは、KMS からの動的キーを使用して、データがデバイスを離れる前に暗号化します。データは、クラウド サーバへの送信中、データの処理中（使用中のデータ）、データの保管時（保管中のデータ）のいずれにおいても、暗号化された状態を維持します。KMS は、Webex Teams アプリケーションがコンテンツの暗号化と復号に使用する暗号化キーの作成、維持、およびアクセス許可を行います。
送信中の暗号化	標準オファー	Mac、Windows、iPhone、Android、Web、およびクラウド用の Webex Teams 間のすべての Web トランザクションに対して、セキュアな HTTPS を使用します。同様に、HTTPS は Webex デバイス（Webex Room デバイス、IP 電話、Webex Board など）からのすべての Web トランザクションに使用されます。Cisco® コラボレーション クラウド（developer.webex.com）上の Web API は HTTPS を使用します。HTTP はサポートされていません。そのため、Cisco Collaboration Cloud との間のすべてのトランスポートは暗号化されます。また、HTTPS は、Webex Control Hub との間で転送中のデータを保護するためにも使用されます。音声、ビデオ、デスクトップ共有、ホワイトボード機能など、Webex のすべてのメディアは、Secure Real-Time Transport Protocol（SRTP。RFC 3711 で定義）を使用して送信されます。現在、Webex プラットフォームでは、ミキシング、分配、および PSTN のトランキングと境界設定の目的で、リアルタイム メディアの復号を行っています。
暗号化されたコンテンツでの検索	標準オファー	Cisco Collaboration Cloud で暗号化されたコンテンツを受信すると、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、保存される前に動的キーを使用して一方向にハッシュされます。エンドユーザが Webex Teams で単語を検索すると、その単語はアプリケーションを終了する前に暗号化されます。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対して検索されます。一致が取得されると、アプリケーションに送信されて復号化が行われ、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（お客様が制御するデータ 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されるキーを管理および保管するサービスと、検索インデックス ハッシュを生成するサービスの両方の導入を選択できます。これらの機能により、企業のお客様はユーザのキーの物理的な保管場所を選択できることがさらに保証されます。サービスを円滑に展開するために、この機能は導入されたら、選択した一連のユーザに対して最初にトライアル モードで実行する必要があります。詳細については、こちらの導入ガイドを参照してください。 **注意：** • **特定のクラウド サービスは、お客様のキー、特に API サーバと Webex プラットフォームのプレビュー機能にアクセスすることが可能です。** • **アクセス キーに対するエンドユーザの権限は、Cisco Collaboration Cloud で生成および保管されている OAuth トークンを通じて提供されます。トークンが侵害された場合は、認証されたトークンによってアクセス可能なキーとコンテンツに対するアクセスを許可するという脆弱性が生じます。**

よくある質問（FAQ）

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 で使用される対称暗号は、AES-256 GCM です。

Q. KMS 用に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、シスコが設計したキー管理の仕様や、インターネット標準として検討するために公開されている、データを保護するためのオープンな標準およびプロトコルに基づいて構築されています。

Q. HDS はどのように入手できますか。

A. HDS は、Pro Pack for Webex Control Hub の一部として購入できる多くの機能のうちの 1 つです。

Q. HDS の詳細な導入ガイドは使用できますか。

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

Q. HDS が保証する追加のセキュリティ機能は何ですか。

A. HDS は、生成されたキーをお客様がお客様環境で物理的に制御することが可能です。特定のクラウド サービスはこれらのキーにアクセスすることが可能ですが、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ことで、攻撃者が暗号化されたコンテンツとキーの両方にアクセスできる場合を除き、高いセキュリティが外部の攻撃によって侵害されないことを保証します。

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制御

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あり、シスコは Webex プラットフォームを使用してお客様のセキュリティ ニーズを満たすことに取り組んでいます。企業 IT 部門は、ユーザに導入するアプリケーションのセキュリティに関する基本的な管理/制御を必要としています。Webex Teams を使用する場合、使用可能な制御には、PIN ロックの適用、トークンの失効、モバイル デバイスにキャッシュされた Webex Teams コンテンツのリモート ワイプ、Web アイドル セッション タイムアウトなどの機能があります。

アクセスのリセット

ユーザ プロファイルでは、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、すべてのアクセスが削除され、そのユーザのトークンを更新し、ユーザが認証されているモバイル デバイス上の、キャッシュされたすべてのコンテンツをリモートから消去します。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、ユーザが組織を離れてもまだ Webex からプロビジョニング解除されない場合です。

モバイル デバイスのセキュリティ制御

iPhone および Android 向け Cisco Webex Teams アプリケーションは、次のエンタープライズグレードのセキュリティ機能を活用しています。

- サポートされるすべての 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）は、認可用の OAuth トークンを確立します。確立されると、クライアントはアクセス トークンを更新します。このとき、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、再認証を必要としません。
- 動的キーを使用したエンドツーエンドの暗号化。
- Cisco Webex サービスおよびユーザの組織定義型 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 ロック有効化の要求（Pro Pack が必要）。この機能を設定すると、ユーザは PIN ロックまたはパスコードを使用してデバイスを保護する必要があります。これにより、デバイスが置き忘れや紛失、または不適切な相手に渡った場合に、Webex Teams アプリケーションのコンテンツにアクセスできないようにすることができます。
- ユーザが Webex から削除されるか、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 ワイプします。
- iPhone 用の Webex Teams での保存データの暗号化。
- Cisco Meraki® Systems Manager および AirWatch（ただしこれらのプロバイダーに限定されるものではない）で認定された、基本的なモバイル デバイス管理（MDM）サポート。

ファイル共有の制御

通常、企業は、ビジネス プロセス管理で使用するファイル管理のためにベンダーを選択する必要があります。このような状況では、内部プロセスに準拠していないか、または情報セキュリティ要件を満たしていない可能性があるため、お客様は Cisco Webex をメッセージング、会議、コール、および Webex Board には使用しても、ファイル ストレージには使用しません。また、Webex Teams を介したファイル共有によって発生する可能性があるマルウェアやデータ漏洩についても、お客様は警戒しています。お客様のこうした使用例をサポートするために、Webex Control Hub はファイル共有制御のポリシーを提供します。

企業の管理者は、クライアント タイプ（Web、デスクトップ、モバイル、ボット）ごとに、ファイルのアップロードまたはファイルのアップロードとダウンロードの両方を無効にすることができます。また、これらの制御により、ソフト クライアントでのホワイトボード機能も無効になります。

Webex 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機能

表 2 に、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制御の概要を示します。

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制御機能

機能	標準オファー/ Pro Pack が必要	利点
PIN ロックの強制化 **注：iOS および Android スマートフォンの場合のみ。Chromebook は含まれていません**	Pro Pack が必要	企業の管理者が PIN ロックの強制化を有効にした場合、iPhone および Android 上の Webex Teams のユーザは、モバイル アプリケーションの特定の機能を使用するためにデバイスの PIN ロックを有効にする必要があります。この機能により、Webex Teams アプリケーションにおいてコンテンツのセキュリティを確保できます。
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 デバイスをなくした場合や組織を辞めた場合、管理者はすべてのアクセスを取り消して、モバイル デバイス（iPhone および Android）にキャッシュされた Webex Teams コンテンツを消去できるため、企業のコンテンツ セキュリティが確保されます。
ファイル共有の制御	Pro Pack が必要	お客様は、データ漏洩への懸念やコンプライアンス、または規制上の理由により他のファイル管理ベンダーを使用している場合、Webex 上でのファイル共有機能を利用しないという選択も可能です。
基本的な MDM のサポート	標準オファー	Webex Teams モバイル アプリケーションは、MDM プロバイダーとセキュリティ管理によって、デバイスのデータを流出または漏洩から保護することができます。 • コピー/貼り付け、バックアップ、ドキュメント共有を無効にします。 • デバイスレベルのパスコードとリモート ワイプを適用します。 注：このサポートは、Meraki Systems Manager および VMware AirWatch では具体的に検証されていますが、基本の制御はほとんどの MDM プロバイダーとの連携を予定しています。
外部通信制御	Pro Pack が必要	お客様は、情報セキュリティとデータ損失の懸念といった理由により、外部組織とのコミュニケーションや通信を許可しないという選択も可能です。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、同時に組織内のユーザが外部のスペースに参加することもできなくなります。 ゲスト ミーティングとコールは引き続き許可されます。

よくある質問（FAQ）

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

A. はい。

Q. 管理者が PIN ロックの適用機能にアクセスするにはどうすればよいですか。

A. これは、Pro Pack によって有効になるプレミアム機能です。アドオン オファーを購入すると、[設定（Settings）] で使用可能になります。

Q. セキュリティ制御が追加される予定はありますか。

A. はい。Webex はクラウド サービスであり、継続的な制御と可視性を確保するために、常に新しい機能を追加します。

エンドポイント接続

Cisco Webex は、すでに導入されたプロキシを介してクラウドへのシームレスな接続をサポートします。サポートされる認証タイプには、モバイル クライアントおよびデスクトップ クライアント用の NoAuth、Basic、および NTLM、モバイル クライアント用のダイジェストベース認証、およびデスクトップ クライアント用の TLS インターセプト プロキシがあります。サポートされるプロキシ設定方法は、手動設定、プロキシ自動設定（PAC）、Web プロキシ自動検出（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。

プロキシ サポートが Webex で利用できるようになったので、プロキシのホワイト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。

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

Cisco Webex Teams サービスのネットワーク要件：https://collaborationhelp.cisco.com/article/ja-jp/WBX000028782

認定および規制準拠

Cisco Webex は、一連の標準認定に準拠し、国際規制の多くを遵守しているため、世界中で Webex を販売できます（図 1）。これらの認定および規制は次のとおりです。

- ISO/IEC 27001
- SOC 2 Type 1 および Type 2
- 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
- EU-US Privacy Shield（EU-米国間のプライバシー シールド）
- Swiss-US Privacy Shield（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

図 1. Cisco Webex 認定および規制準拠

Cisco Capital

目標の達成を支援する ファイナンス

Cisco Capital® では、目標を達成し、競争力を維持するために必要なテクノロジーの取得を支援します。CapEx の削減をサポートし、成功を加速させ、投資金額と ROI を最適化します。Cisco Capital ファイナンス プログラムは、お客様がハードウェア、ソフトウェア、サービス、および補完的なサードパーティ製機器を柔軟に取得できるようにします。また、支払に関しては予測可能な支払方法をご用意しています。Cisco Capital は 100 ヵ国以上で利用できます。Cisco Capital についての詳細はこちらをご覧ください。

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

C78-740771-00JA 19.06