ホワイト ペーパー

Cisco Webex Teams セキュリティ ホワイト ペーパー

バージョン 2.0（2018 年 6 月）

Cisco Webex は、メッセージング、コール、および会議機能を備えたクラウド コラボレーション プラットフォームです。Cisco Webex Teams アプリケーションは、Webex プラットフォームに接続するクライアント アプリケーションであり、チームワークを促進する包括的なツールとして機能します。ユーザはメッセージの送信、ファイルの共有、各チームとの会議などを 1 箇所で行うことができます。このホワイト ペーパーでは、Cisco Webex Teams のセキュリティ機能の概要を説明します*。

* 本書に記載されるシスコの製品、サービス、機能の一部は、現在開発中または将来公開予定です。将来公開予定の機能には、記載後に「🔨」アイコンを追加しています。シスコは、このアイコンで示されている製品、サービス、または機能の提供の遅延、または中止について一切の責任を負いません。

Cisco Webex Teams で、クラウド コラボレーションのセキュリティとプライバシーの課題に対応

クラウド サービスによって企業が得られる大きな利点の 1 つは、クラウド サービス プロバイダーによってサービスが導入された時点で、付加価値のある特長や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 プロバイダーでは、「付加価値」とは、ユーザのデータやコンテンツに完全にアクセスできることを意味しています。ほとんどのクラウド プロバイダー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ります。これとは反対に、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 Teams は両者の長所を採り入れています。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、企業はシスコとサードパーティの統合による付加価値を選択して利用できます。Cisco Webex Teams では、暗号化キーを管理できるオープン アーキテクチャが採用されているため、お客様は暗号化キーとデータの機密性を排他的に制御できます。それにより、コンテンツはユーザ クライアントで暗号化され、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、コンテンツの復号キーにはアクセスできません。

暗号化キーに対するアクセスを明示的に許可することで追加機能が得られますが、Webex Teams のファブリックにエンドツーエンドの暗号化が最初から組み込まれているため多くの付加価値的特長や機能は暗号化されたデータに対して動作します。Webex Teams では、革新的なメッセージ インデックス、許可モデル、認証フロー、暗号化、導入モデルを使用することで、クラウドでの復号を一切必要としない暗号化コンテンツのグローバル検索などの機能がサポートされます。

ほとんどのクラウド サービス プロバイダーでは、ユーザのデバイスとサーバ間、またはデータセンター間での「送信中」およびサーバでの「保管中」にデータが暗号化されるため、セキュリティが確保されていると主張しています。一部のプロバイダーでは、この暗号化のキーをお客様に用意させることもあります。しかし、送信中および保管中のデータが暗号化される場合でも、クラウドのサーバはお客様のコンテンツにアクセスできます。そのため、お客様は、クラウド プロバイダー自体が侵害された場合は被害を受ける可能性があります。Webex Teams に組み込まれるエンドツーエンド アーキテクチャでは、お客様が信頼することを選択した場合のみ、お客様のコンテンツに対してサーバが信頼されます。

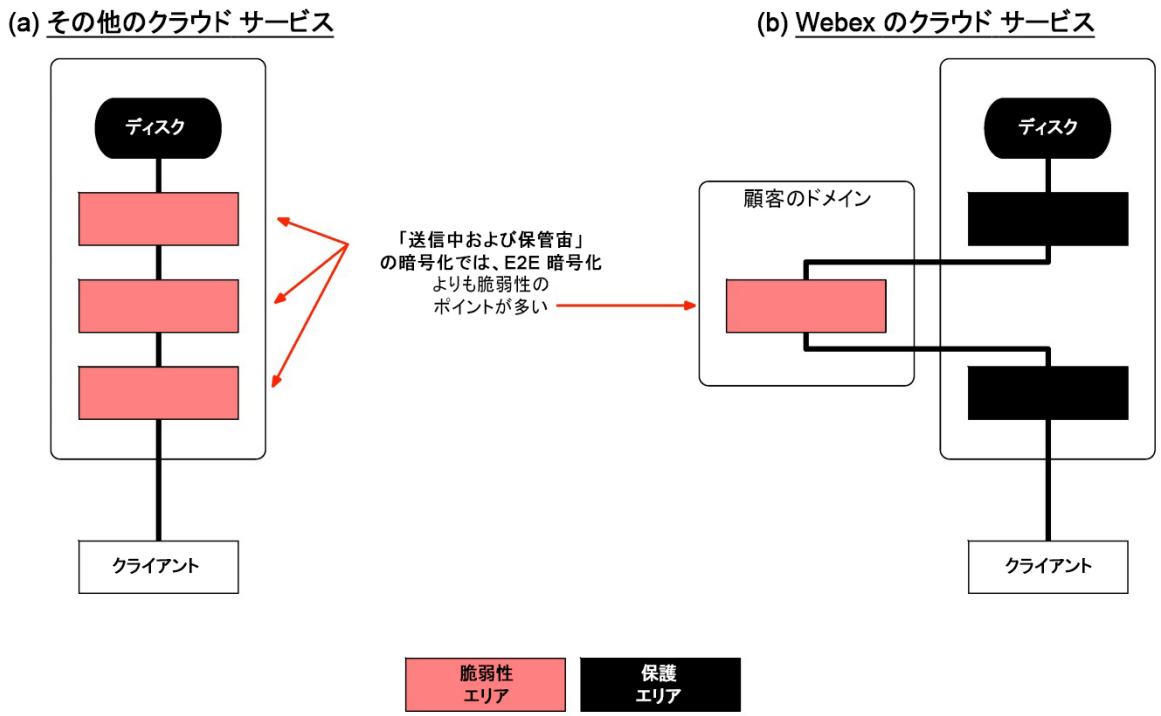

図 1. その他のクラウド アプリケーション (A) と Webex Teams (B) のセキュリティ アーキテクチャ

シスコが約束する信頼性の高いサービスでは、ユーザ コンテンツが保護されるだけではありません。Webex Teams では、難読化アイデンティティ、選択、透過性を含む、プライバシーのためのツールと機能を組み合わせることで、ユーザと使用状況に関するすべてのデータが保護されます。エンドツーエンドの暗号化と同様に、これらの保護機能は最初からサービスに組み込まれています。

このホワイト ペーパーでは、シスコおよび外部の攻撃者からお客様のデータを保護するために Webex Teams で提供されるツール スイートについて説明します。

- **Webex Teams のエンドツーエンドのセキュリティ**:シスコは、お客様が明示的に許可した場合のみお客様のデータにアクセスできます。
- **Webex Teams の使用状況の保護**:お客様によるコラボレーションに向けた Webex Teams の使用によって新たなセキュリティ リスクが発生することを防ぎます。
- **プラットフォームの保護**:Cisco Webex Cloud と Webex Teams アプリケーションを外部攻撃から保護します。

エンドツーエンドのセキュリティ

エンドツーエンドのセキュリティは、Webex Teams の中心となるセキュリティ機能であり、標準的なクラウド セキュリティを超えた追加の保護を提供します。Webex クラウドを通じて転送されるすべてのお客様のデータは、送信前に暗号化されます。そのため、クラウド コンポーネントによって処理されるお客様のデータは、常に安全に暗号化されています。その結果、**クラウド コンポーネントの 1 つが完全に侵害された場合(「保管中の暗号化」および「送信中の暗号化」では保護できない状況)でも、データはエンドツーエンドで暗号化されているため、攻撃者はお客様のデータにアクセスできません。**このルールの例外は、お客様が明示的に許可した場合のみです。

お客様のデータと Cisco Webex の分離は、Webex Teams の構築と運用における土台です。これは非常に重要なため、シスコでは Webex Teams の機能全体が 2 つの信頼ドメインに分割されていると考えています。その 2 つとは「お客様ドメイン」と「Webex Teams コア」です。お客様ドメインには、企業内で使用される一連のクライアントおよびハードウェア エンドポイントなどの直接お客様によって制御される要素や、クライアントがセキュアに通信できるようにクライアントで運用される Webex Teams のインフラストラクチャが含まれます。Webex Teams コアには、これらのクライアントが他のクライアントと、またお客様ドメインのインフラストラクチャとコラボレーションすることを可能にするためにシスコによって運用される Webex サービスが含まれます。

E2E クリティカル パス

お客様ドメインと Webex Teams コアの分割は、究極的には暗号化によって実現します。お客様のデータを暗号化することで、Webex Teams コアの信頼されていない要素によるアクセスを防ぎます。つまり、分割の利点は、暗号化のキーがどの程度安全に保護されているかに左右されます。キーへのアクセスの管理には、「エンドツーエンド クリティカル パス」として連携する以下のキーコンポーネントが使用されます。

ブートストラップ	- どの KMS および認証サービスを信頼するかをクライアントに伝える
認証サービス	- どの ID プロバイダーを信頼するかをクライアントに伝える - ID プロバイダーによって信頼される SAML リクエストを発行する - KMS によって信頼されるトークンを発行する
ID/SSO プロバイダー（IDP）	- ユーザのパスワードを受け取る - 認証サービスによって信頼される SAML 応答を発行する
キー管理サーバ（KMS）	- 認証サービスからのトークンに依存する - キーへのアクセスを生成および制御する
プレーン テキスト サービス	- 例：検索インデックス、ドキュメントのトランスコーディング - プレーン テキスト コンテンツにアクセスするには、お客様の認証を受ける

図 2. Webex Teams のエンドツーエンド クリティカル パス

クリティカル パスの要素は互いに連携して、お客様が認証済みのエンティティのみがお客様のコンテンツを復号するキーにアクセスできるようにします。すべての未認証のパーティはロックアウトされます。クリティカル パスの要素が連携してこの分離を達成する仕組みを理解するために、図 3 に記載される、クライアントによる Webex Teams へのログイン方法を確認してみましょう。

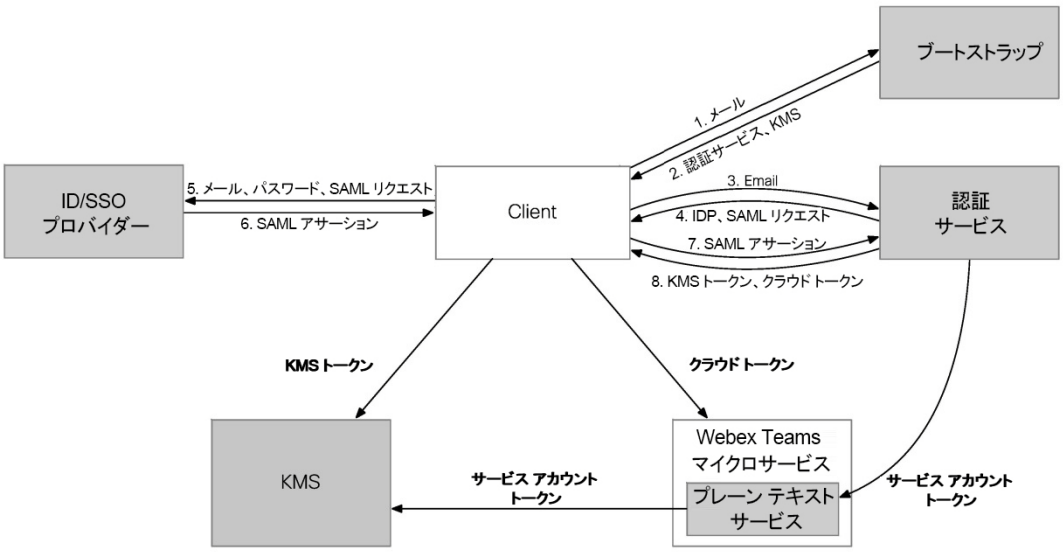

図 3. Webex Teams のログイン フロー

ユーザは Webex Teams にログインしたら、まずメールアドレスを入力します。そのメールアドレスに基づいて、クライアントは、信頼するべき認証サービスとキー管理サービス(KMS)を Webex Teams によって提供されるブートストラップ サービスから確認します(1、2)。次に、クライアントはその認証サービスを使用した標準の SAML ログインを開始します。クライアントはメールアドレスに基づいて適切な ID プロバイダーにリダイレクトされ(3、4)、ID プロバイダーを使用してログインして SAML アサーションを取得し(5、6)、認証サービスに SAML アサーションを戻します(7)。次に、認証サービスによって 2 つの Oauth2 トークンがクライアントに提供されます(8)。これらは、クライアントが自身の KMS のみに対して証明するために使用する KMS トークンと、クライアントが Webex クラウドのマイクロサービスに対して証明するために使用するクラウド トークンです。

KMS は、お客様のデータの暗号化に使用されるキーを保護し、お客様によって認証されたエンティティのみがこれらのキーにアクセスできるようにします。クライアントは、組織のユーザに代わってキーをダウンロードします。クライアントからの要求は、上述の KMS トークンで認証されます。KMS トークンとクラウド トークンが分離されているため、クライアントは KMS トークンを KMS のみに送信します。**Webex Teams のコンポーネントは、ユーザを偽装できません。**Webex Teams のマイクロサービスが一部のコンテンツにアクセスできるようにお客様が認証すると(詳しく後述する「プレーン テキスト サービス」)、そのサービスは認証サービスから特別なトークンを取得し、認証されたタイプのサービスであることが KMS に対して証明されます(「サービス アカウント トークン」)。**お客様は、特定のプレーン テキスト サービスを選択できます。Webex クラウド全体にデータへのアクセス権を付与する必要はありません** 🔨。

Webex Teams の E2E 暗号化によって、このクリティカル パスを分離して保護を強化できます。E2E 暗号化によってその他のコンポーネントの侵害のリスクを大幅に軽減できるため、クリティカル パスの保護に集中できます。KMS や検索インデクサ (プレーン テキスト サービス) など、クリティカル パスのいくつかの要素については、お客様はシスコのハイブリッド データ セキュリティ アーキテクチャを使用して、オンプレミスで直接インスタンスを運用できます。これらのコンポーネントをシスコがホストする場合、アクセス制御と運用は、Webex Teams の他の部分から分離されます 🔨。

結果として、攻撃者がクラウド プロバイダーを侵害することにより得られる情報は大幅に減少します。この違いは図 1 で示しています。左は、転送中および保管中の暗号化を使用する一般的なクラウド サービス プロバイダーです。暗号化さ

れたストレージとクラウド コンポーネント間の接続のみが暗号化されます。そのため、クラウド サービスが侵害された場合はお客様のデータの漏洩につながります。これに対し、Webex Teams が使用する E2E 暗号化アプローチではお客様の情報がデフォルトで暗号化され、必要な時のみ復号されます。プレーン テキストでお客様の情報を処理する一般的なクラウド サービスでは、クラウドで提供されるサービスが増えるほどお客様の情報が侵害されるリスクが高まります。Webex Teams は E2E 暗号化により、攻撃対象領域を最小限に抑えながら豊富なクラウド サービスを提供できます。

エンドツーエンドのコンテンツ暗号化

Webex Teams では、クライアント アプリケーションはエンドツーエンドの暗号化を使用するため、Cisco Webex を使用してコンテンツを配信してもクラウドではそのコンテンツにアクセスできません。この暗号化のキーは、キー管理サービス（KMS）によって管理されます。お客様の KMS は、コンテンツの暗号化キーにアクセスできるユーザ（つまり、お客様のコンテンツにアクセスできるユーザ）を制御するための効果的なエージェントです。シスコでは、お客様の制御によって実行されるコンポーネント（お客様の KMS およびクライアント）はお客様ドメインに含まれると考えています。これらのコンポーネントの一部がシスコによって運用される場合でも、その他の Webex Teams のコンポーネントからは分離されます。

ただし、コンテンツの実際の暗号化はクライアントによって実行されます。クライアントは KMS からキーを取得する必要があるため、クライアントを管理するお客様から実質的に「暗号化キーを借り出す」ことになります。これを安全に実行するために、各クライアントは Cisco Webex から組織の KMS への暗号化トンネルを確立します。このトンネルは、認証済みのエフェメラルな楕円曲線 Diffie-Hellman（ECDH）交換を使用して、HTTPS や VPN などに使用される TLS および IPsec プロトコルとほとんど同じように機能します。クライアントは、まず RSA 公開キーを KMS ドメイン名に関連付ける証明書を受け取ります（1）。クライアントは EC キー ペアを生成し、KMS の RSA 公開キーを使用してそのペアの公開コンポーネントを暗号化し、Webex Teams を使用して結果を KMS に送信します（2）。KMS はこのメッセージを復号し、独自のエフェメラルな EC キー ペアを生成し、証明書に対応する RSA 秘密キーで公開コンポーネントに署名し、クライアントにメッセージで結果を戻します（3）。この時点で、クライアントとサーバは今後のメッセージに向けて暗号化キーを取得するために使用できる共有秘密を有しており、KMS はクライアントに対して ID を証明しています。クライアントのアイデンティティを証明するために、クライアントは今後のリクエストで KMS トークンを KMS に送信します（4）。

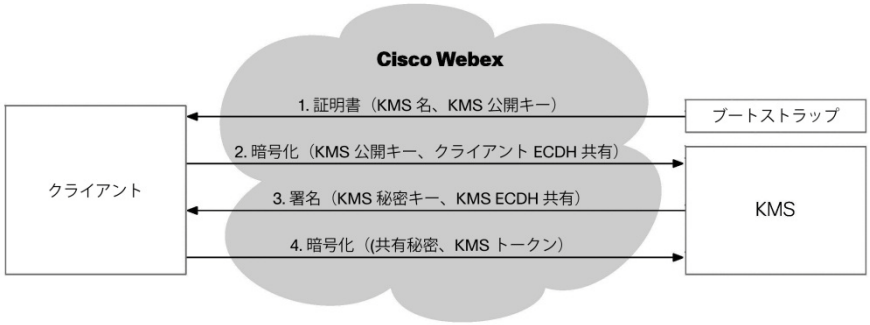

図 4. KMS によるセキュア通信

メッセージやファイルのような Webex Teams の暗号化された各アイテムは、復号するために使用できるキーを示すキー URL でタグ付けされます。クライアントがキーを必要とする場合、自身の KMS からリクエストします。キーが別の KMS に保管されていることをキーの URL が示している場合、クライアントに代わってクライアントの KMS がその KMS からキーを取得します。各キーにはアクセス コントロール リスト（ACL）が関連付けられており、そのキーへのアクセスを許可されたユーザが示されています。キーへのアクセスを許可する前に、キーを保管する KMS は、リクエストしているユーザが ACL に記載されていることを検証します。また、別の KMS からリクエストを受けた場合、リクエストしている KMS がユーザに代わってアクションを実行することを許可されていることを検証します。

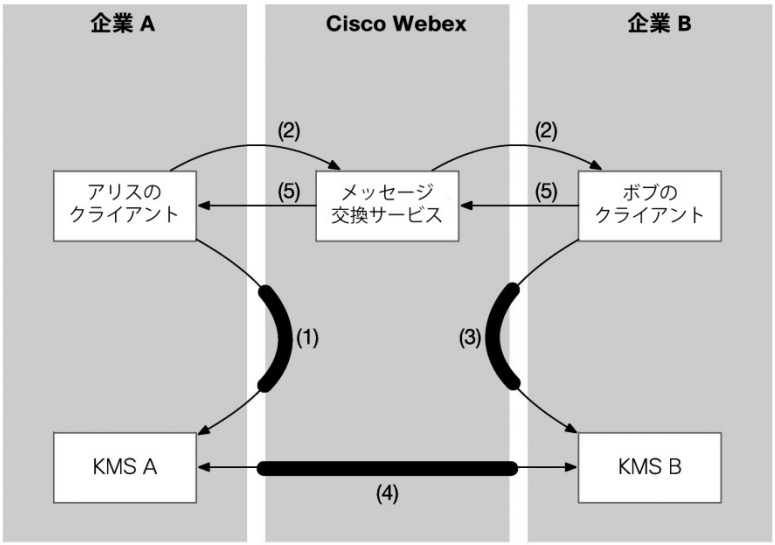

図 5. Webex Teams のセキュアなメッセージング

これらすべてがどのように相互作用するかを確認するために、異なる組織の 2 人のユーザ（ボブとアリス）が互いにメッセージを送信する様子を見てみましょう。アリスがボブとのメッセージ交換を作成する場合、アリスのクライアントは KMS A から（クラウドを通る ECDH トンネルを使用して）そのためのキーを取得し、ボブが認証済みであることを KMS A に伝えます（1）。アリスがメッセージ交換を作成するように Webex Teams に指示する際、メッセージ交換のためのキー URL も同時に伝えます。メッセージ交換サービスはその URL をボブにリレーします（2）。ボブのクライアントがメッセージ交換に参加すると、そのクライアントはボブの企業の KMS （KMS B）からキーをリクエストします（3）。ボブの KMS はキーが KMS A に保管されていることを確認し、リクエストを転送します（4）。KMS A は、ボブがリクエストされているキーを受け取ることを許可されており、KMS B がボブの代理となることを許可されていることをチェックします。これらのチェックに合格すると、KMS A は KMS B にキーを渡し、KMS B はボブにキーを渡します。次に、ボブはそのキーを使用してアリスへのメッセージを暗号化し、Cisco Webex のメッセージ交換サービスに安全にメッセージを送信します（4）。メッセージ交換サービスはメッセージを保存し、アリスがオンラインになるとメッセージを転送します（スペース内のその他の参加者の場合も同様です）。アリスのクライアントは同じキーを持っているため、メッセージを復号してアリスに表示できます。

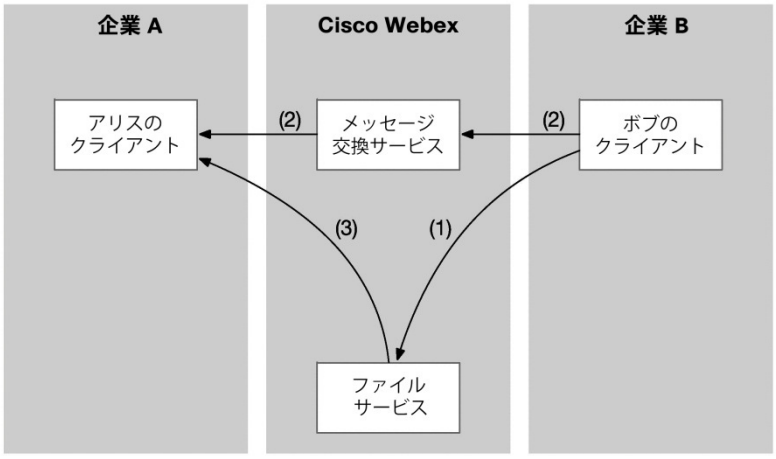

図 6. Webex Teams でのセキュアなファイル共有

Webex Teams 内のファイルも同様の方法で保護されています。ボブがファイルをスペースにアップロードする場合、ボブのクライアントは新しいキーを生成してファイルの暗号化に使用します。次に、クライアントは暗号化したファイルを Cisco Webex 内のファイル ストレージ サービスに送信します(1)。スペースの他のクライアントがファイルをダウンロードできるようにするために、ボブのクライアントは、ファイルの暗号化に使用したキーと暗号化ファイルの URL を含むメッセージを作成します。このメッセージはスペース内の他のユーザに送信され、スペースの他のメッセージと同じキーで暗号化されます(2)。アリスのクライアントがこの特別なメッセージを受け取ると、URL を使用して暗号化ファイルを取得し、キーを使用してファイルを復号してアリスに表示します。

クライアントとクラウド コンポーネントが KMS と対話するために使用する完全なプロトコルは、IETF インターネットドラフトとして公開されています。

キーへのアクセスの管理

認証されていないパーティがエンドツーエンドの暗号化に使用されるキーにアクセスできないようにするために、組織の KMS は各キーへのアクセスが許可されるユーザを記録します。スペースが作成されると、KMS によって KMS リソース オブジェクト(KRO)がプロビジョニングされます。KMS は、KRO を使用してスペースのキーとキーの受け取りを許可されたユーザを追跡します。

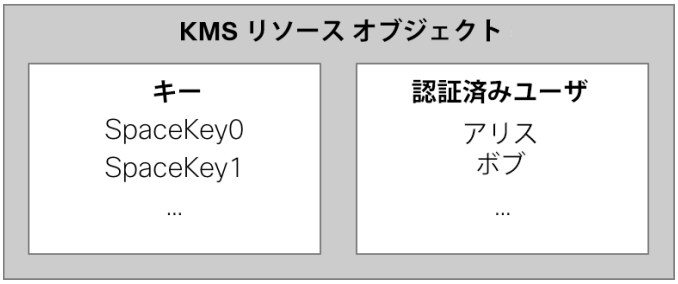

図 7. KMS リソース オブジェクトの構造

各スペースには常に 1 つのキーがあります。スペースのすべての参加者が、そのキーを使用してメッセージを暗号化します。ユーザが新しい参加者をスペースに追加すると、対応する KRO にも追加することになるため、新しい参加者はキーを取得できます。ユーザがスペースから抜ける(または削除される)と、そのユーザは KRO から削除されます。次に、KMS から新しいキーを取得し、スペースの KRO に「バインド」することでスペースのキーが更新されます。そのため、他の参加者はキーをダウンロードできますが、スペースから抜けた参加者はダウンロードできません 🔨。

ファイルも同様の方法で処理されます。前述したように、各ファイルは 異なるキーで暗号化され、ファイル自体の URL と併せて暗号化されたメッセージで送信されます。スペースに向けた暗号化されたメッセージによってファイルが共有されるため、スペースのキーにアクセスできる場合のみ、クライアントがファイルを復号できます。

これらのメカニズムの結果として、スペースの現在の参加者はスペースに送信されたすべてのメッセージまたはファイルをダウンロードおよび復号できます。これには、その参加者がスペースに参加する前に送信されたものも含まれます。ただし、参加者がスペースから抜けると、その後に送信されたメッセージやファイルに使用されたキーにはアクセスできません。さらに、スペースから抜けた参加者は KRO から削除されているため、スペースに参加していたときに使用していたキーもダウンロードできなくなります。

キーに対する機能アクセス

特定の Webex Teams 機能では、通常は暗号化されているコンテンツのプレーン テキストにクラウド サービスがアクセスする必要があります。以下は、現在のプレーン テキスト機能の一覧です。

- 音声およびビデオ コール：トランスコーディング、メディア ミキシング、PSTN 相互運用性、会議録画などのサービスを提供するために、メディア ノードが音声およびビデオ パケットを復号できるようにする必要があります。
- ドキュメントのトランスコーディング：スペースにアップロードされたドキュメントのプレビュー画像を作成します。
- API アクセス：E2E システムと統合しなくても、ボットと統合がスペースのコンテンツにアクセスできるようにします。
- (*) 検索インデックス：クラウドで安全に保存および検索できる暗号化されたインデックスを作成します。
- (*) eDiscovery：コンプライアンスの目的で、暗号化されたメッセージの検索を可能にします。
- (*) カレンダー コネクタ：Webex Teams によって会議のスケジュールを立て、お客様のカレンダー システムに自動的に反映されるようにします（スペースのタイトルを復号するためにキーが必要）。
- IM & プレゼンスの相互運用性：Webex Teams とその他のメッセージング システム（Cisco Jabber など）の相互運用を可能にします。これらのシステムでは E2E 暗号化がサポートされていないため、相互運用性を提供するコンポーネントによって暗号化されたコンテンツを復号する必要があります。
- Webex Teams アシスタント：自動的な会議の開始などを可能にする、AI によるスマート アシスタントを提供します。ユーザに向けたアクションを実行するために、アシスタントはユーザの Webex Teams データにアクセスする必要があります。

(*) でマークされたサービスは、お客様がコンポーネントをオンプレミスで実行できます。暗号化された検索とボットおよび統合機能については以下で詳しく説明します。

プレーン テキスト機能は、コンテンツがクラウドに公開されることに組織が同意した場合のみ有効です。この同意を得るには、機能は、組織の KMS から復号キーへのアクセス権を取得する必要があります。KMS は、どの機能にアクセスを許可するかに関する組織のポリシーを適用できます 🔨。

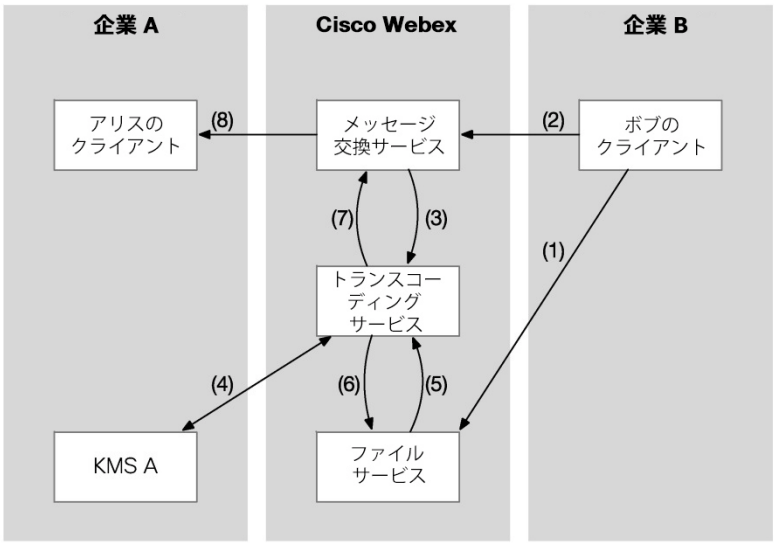

図 8. プレーン テキスト サービスのキー アクセス

企業 A が、企業が所有するスペースでドキュメント プレビューを提供するためにファイル トランスコーディング サービスを有効にしたとします。ボブがファイルをスペースに投稿すると(1、2)、トランスコーディング サービスは、ファイルの URL とキーを含む暗号化メッセージでアップロードの通知を受けます(3)。トランスコーディング サービスはこのメッセージを復号するキーを取得できるため(4)、ファイルを取得して(5)復号できます。実際のトランス コードを実行した後、トランスコーディング サービスは結果のプレビュー画像を暗号化し、ファイル サービスに投稿して(6)スペースに通知を送信します(7)。その後、スペースの他のクライアントはプレビュー画像を取得して復号し、その他のファイルと同じように表示できるようになります(8)。ここでは、以下の 2 つの重要な点に注意する必要があります。(1)復号されたお客様のコンテンツは、トランスコーディング サービスにのみ閲覧可能です。(2)企業 A がトランスコーディングを許可しない場合、トランスコーディング サービスはコンテンツを復号できません。

このフローに企業 A の KMS が関与していることに注意してください。トランスコーディング サービスが KMS A からメッセージ キーを取得できない場合、暗号化されたファイルをダウンロードすることもできません。つまり、(Webex Teams コアの)トランスコーディング サービスは、お客様がトランスコーディング サービスにキーを渡すように KMS を設定することでこのアクセスを許可した場合のみ、お客様のデータにアクセスできます。

暗号化された検索

あらゆるメッセージング システムで最も頻繁に使用される機能の 1 つは検索です。Cisco Webex Teams の検索は、検索機能が一度のみメッセージのプレーン テキストにアクセスして暗号化されたインデックスを作成し、その後はクライアントがクラウドで暗号化されたデータに対して直接検索を実行できるように設計されています。これと同じ技術によって、確実にセキュリティを保証した状態で eDiscovery などのサービスも提供できます。

検索プロセスには 2 つの主要な手順があります。メッセージの送信時にインデックスを作成することと、そのインデックスを使用してクエリを実行することです。両方の手順が、検索インデクサ サービスによってアシストされます。このサービスではエンドツーエンド クリティカル パスの一部であるプレーン テキストへのアクセスが必要となるため、他の Cisco Webex から分離されています。ハイブリッド データ セキュリティによって、企業は(独自の KMS を実行できるのと同様に)独自の検索インデクサを実行することもできます。これにより、Cisco Webex Cloud がプレーン テキストにアクセスしなくても検索を実行できます。

検索インデックスを構築するために、検索インデクサ サービスは組織内で送信されたすべてのメッセージのフィードを取得します。スペースにメッセージが送信されると、検索インデクサにコピーが送信されます。検索インデクサは組織の KMS から適切な暗号化キーを取得し、メッセージを復号します。検索インデクサは、最初にメッセージを個々の単語に分解し(トークン化)、次に各単語を原形に戻す(ステミング)ことで、メッセージのテキストを一連の検索可能な用語に変換します。次に、検索インデクサは KMS の検索インデックス キーによって、ハッシュベースのメッセージ認証コード(HMAC)アルゴリズムを使用して各検索用語をその用語を表すオペークな値に変換します。HMAC 変換は基本的に一方向の暗号化です。特定の HMAC 出力値を元のメッセージで表示されていた単語に戻すことはできません。インデクサはこのリストにランダムの「ノイズ」値をいくつか追加し、ルームのメッセージが頻度分析(ある言語における特定の単語の出現頻度を分析する)によって推測されないようにします。これらすべての手順が完了すると、検索インデクサは、特定のメッセージを一連の値に関連付けたインデックス エントリを安全にクラウドにアップロードできます。

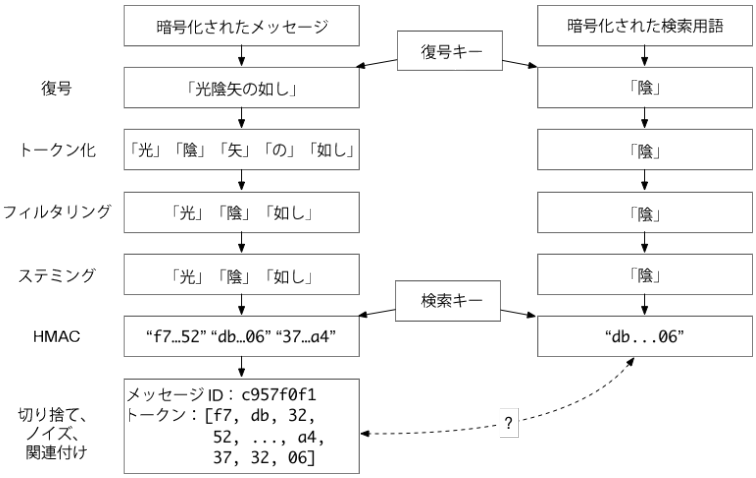

図 9. Webex Teams の暗号化された検索

検索を実行するために、クライアントはエンドツーエンドで暗号化されたメッセージによって検索インデクサにクエリを送信します。これは、クライアントとインデクサが 1 対 1 の対話をしているようなものです。検索インデクサは、メッセージを構成要素に分解するために元のメッセージに実行したのと同じプロセス（トークン化、ステミング）をクエリに対して繰り返します。ただし、要素に HMAC を適用する前に、検索インデクサは Cisco Webex からユーザが参加しているルームのリストを取得します。次に、検索インデクサは各ルームの検索キーを使用して、クエリの各要素の HMAC 値を生成します。したがって、10 個のルームのクライアントが 2 単語の検索クエリを入力すると、検索インデクサによって約 20 個の HMAC 出力値が作成されます。検索インデクサは Cisco Webex Cloud の検索サービスにこれらの値を渡します。Cisco Webex Cloud は、値を暗号化されたインデックスと比較し、一致したメッセージをクライアントに伝えます。

Webex Teams の検索機能は、セキュリティとユーザ エクスペリエンスのどちらも損なわないように設計されています。他のクラウド サービスでは検索を実行するためにクラウドでユーザのコンテンツを復号する必要がありますが、シスコのアプローチでは、クラウドがユーザのコンテンツにアクセスすることなく同様の迅速な検索体験を提供できます。

リアルタイムのメディア暗号化

ビデオ、音声、デスクトップの共有など、Cisco Webex Teams のすべてのリアルタイム メディアは Secure Real-Time Transport Protocol（SRTP）を使用して転送されます。SRTP によって、攻撃者に対するリアルタイム メディアの秘密保持性、整合性、信頼性を保護できます。現在、リアルタイムのメディアはエンドツーエンドで暗号化されていません。:**Cisco Webex は、ミキシング、配信、公衆電話交換網（PSTN）の相互運用性の目的でリアルタイム メディアを復号します。**

SRTP のセキュリティを将来的に向上させるために、シスコは IETF の Privacy Enhanced RTP Conferencing（PERC）作業部会にも推進役として参加しています。PERC の目標は、エンドツーエンドのメディアの暗号化を実現すると同時に、クラウドが提供する一部の機能との互換性を維持することです。この新しい標準の成熟に合わせて、Cisco Webex Teams ではこれを活用し、現在メッセージとファイルに向けて提供しているエンドツーエンドの保護をリアルタイム メディアにも適用する予定です。PERC は、当面の間は PSTN プロバイダーによるクラウド復号が必要な PSTN コールの復号には影響しません。

企業とユーザの選択

Webex Teams ではユーザと企業が、複雑な設定インターフェイスを介することなくプライバシーに関する選択を行うことができます。企業の管理者は次の項目を選択できます。

- シングル サイン オン（SSO）：管理者は、既存の SSO ソリューションと連動するように Webex Teams を設定できます。Security Assertion Markup Language（SAML）2.0 およびオープン認証(OAuth)2.0 を使用する ID プロバイダーがサポートされています。
- ディレクトリ同期：Microsoft Active Directory を使用している場合、管理者は従業員のライフサイクル変更がリアルタイムで Webex Teams に反映されるように設定できます。
- シスコ パートナーとのデータ共有：企業は QoS（Quality of Service）データとエンゲージメント データをシスコ パートナーと共有して、より高度なパートナー サポートを可能にするかどうかを選択できます。
- EU GDPR（EU 一般データ保護規則）に準拠するためのエンタープライズ プライバシー制御の詳細は、Webex サービスのプライバシー データ シート [英語] に記載されています。これらの制御は、エクスポートする権利、忘れられる権利、期限を決めたユーザのコンテンツの削除などの個人データの処理に関する権利を網羅しています。

ユーザは次の項目を選択できます。

- デバイス アクセス許可。Webex Teams アプリケーションでは、電話、マイク、カメラ、音声録音、画面共有、カレンダー、連絡先、ファイルおよび写真、プッシュ通知など、さまざまなデバイス アクセス許可がリクエストされます。ほとんどのプラットフォーム（特にモバイルプラットフォームと Web）では、これにはユーザの明示的な許可が必要で、ユーザはいつでも許可を取り消すことができます。
- プロキシミティ機能。モバイル デバイスでは、Webex Teams アプリケーションがアクティブな場合には超音波信号と Wi-Fi 信号がリッスンされるため、Webex Teams クライアントがシスコの音声およびビデオ エンドポイントと自動的にペアリングされます。これにはデバイスのマイクと Wi-Fi アンテナを使用する必要があるため、シスコでは、ユーザがこの機能をオフにできるようにしています。
- プロフィール写真。プロフィール写真が推奨されますが、Webex Teams を使用するための必須事項ではありません。
- 外部参加者インジケータ。Cisco Webex Teams アプリケーションでは、自社に属していない参加者がルームにいることが視覚的なインジケータによってユーザに示されます。
- ルーム モデレータ管理。参加者の中からモデレータを選択して、ルームのタイトルと参加者リストを排他的に管理できる権限を付与することで、Cisco Webex Teams のルームを管理できます。
- その他のプライバシー制御は Webex サービスのプライバシー データ シート [英語] に定義されています。

Cisco Webex Teams のデータ収集およびプライバシーの詳細は、Cisco Trust Center [英語] でご確認いただけます。

透過性

シスコでは、ユーザとお客様が選択内容について理解し、シスコに委託されたデータがどのように管理および保護されているかを認識できるようにしたいと考えています。そのために、階層的な透過性を導入しています。ユーザがリアルタイムの意思決定をするために役立つ短期的な情報は、Webex Teams アプリケーション自体で開示されています。より詳細な情報はシスコのサポート ページで利用でき、定期的に更新されます。シスコが収集する情報、情報の利用方法、情報の保護方法の詳細は、Webex サービスのプライバシー データ シート [英語] をご覧ください。

また、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る場合に、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、7 月～ 12 月の期間）、このデータを公開します。他のテクノロジー企業と同様、このデータはタイミングに関する制限に準拠し、提示されたレポート期間終了から 6 ヵ月後に公開します。

詳細については、Cisco Trust Center の透明性に関するセクション [英語] をご覧ください。

また、シスコでは法域内における合法的なデータの使用を可能にするために、以下に例を挙げる多数の転送メカニズムに投資しています。

- 拘束的企業準則
- EU・米国間およびスイス・米国間のプライバシー シールド フレームワーク
- APEC Cross Border Privacy Rules
- EU 標準契約条項

Webex Teams の使用状況の保護

コラボレーション ツールは、組織の全体的な運用セキュリティ アプローチに適合している必要があります。Cisco Webex Teams は、管理者が Webex Teams の使用を管理してリスクを低減するためのツールを提供します。また、Webex Teams はファイアウォールからコンテンツ管理システムまで、企業が安全のために使用するその他のツールと適切に連携します。

Webex Teams で共有したコンテンツの管理

情報共有は企業にとって非常に役立ちますが、それによってリスクも発生します。例えば、秘密情報が不適切に共有されるリスクや、コンプライアンスの目的で必要な時に重要な情報にアクセスできないリスクなどです。Cisco Webex Teams では、以下に挙げるように、企業がこれらのリスクを管理するためのツール スイートを利用できます。

- **アーカイブと保持**:Webex Teams 内のすべてのユーザ コンテンツは、定義した保持期間は保存され、その後削除されます。この保持期間は管理者がカスタマイズできます。保持期間が指定されていない場合は、デフォルトの保持期間が適用されます 🔨。Webex Teams は、外部のアーカイブ サービスとも接続できます。
- **データ損失の防止**:Webex Teams では、複数の DLP プロバイダーと統合してポリシー違反を特定し、即座に是正アクションを実行できます。
- **eDiscovery**:Webex Teams の eDiscovery コンソールを使用して、コンプライアンス管理者は関連するメッセージとファイルや、タイムスタンプ、スペース ID、参加者の ID などのコンテクスチュアル データを検索および取得できます。
- **コンプライアンス API**:コンテンツ管理にカスタムの統合を利用したい企業は、特別なコンプライアンス責任者の役割で使用される公開 API を利用できます。

Webex Teams の拡張

Cisco Webex Teams は、企業が Webex Teams を自動化して他のサービスに接続するためのオープン API を提供しています。Webex Teams を拡張するには以下の 3 つの方法があります。

- **ボット**では、コール録音サービスなど、全社規模の拡張機能が利用できます。ボットにアクセス権を付与する前に、ボットによってスペースを作成するか、ボットをスペースに招待する必要があります。スペース内であっても、ボットがアクセスできるのはそのボットを(「mention」によって)明示的に参照するメッセージのみです。
- **統合**では、パーソナル アシスタントやドキュメントの翻訳など、単独ユーザ向けの機能を拡張できます。統合は、同じスペース、メッセージ、ファイル、コールへのアクセスなど、Webex Teams において関連付けられたユーザと同じ能力を持ちます。統合は、ユーザ インターフェイスを持たずにインテリジェンスが追加された、クラウドまたはサーバによってホストされるクライアントと考えることができます。

- **ウェブホック**は、Webex Teams で特定のイベントが発生した場合に、ボットまたは統合が Webex Teams に外部サービスを「呼び出す」ように指示する方法です。ウェブホックには、Webex Teams に対してすでに可視化されているメタデータのみが提供されます。ウェブホックはエンドツーエンドで暗号化されたコンテンツにアクセスできません。例えば、スペースにメッセージがある場合にウェブホックに通知するようにユーザが設定した場合、ウェブホックにはメッセージの送信者やメッセージが送信されたスペースなど、Webex Teams に対して可視化されているメッセージ情報のみが通知されます。メッセージの内容は通知されません。

Cisco Webex API の詳細は、https://developer.webex.com/ [英語] をご覧ください。

学習と使用が簡単な API を開発者に提供するために、シスコでは、ボットと統合を Webex Teams のエンドツーエンドの暗号化システムと明示的に統合することを要求していません。代わりに、開発者は Webex Teams SDK または Webex Teams API サーバを使用できます。

SDK を使用することは、より安全なオプションです。開発者が Webex Teams SDK を使用すると、E2E 暗号化システムとのすべての統合作業が SDK によって処理されます。SDK は適切な KMS に対して直接証明され、すべての暗号化および復号がローカルで実行されます SDK ベースのボットと統合を使用するお客様は、ボットおよび統合のコードがセキュアなコンテクストで実行されていることを確認する必要がありますが、Cisco Webex がキーまたはコンテンツにアクセスする心配はありません。

SDK を使用することが不可能な場合、Webex Teams は、KMS との対話を処理してボットまたは統合の代わりにコンテンツを復号する API サーバを提供しています。ボットまたは統合が暗号化されたコンテンツ（メッセージまたはファイルなど）へのアクセスをリクエストした場合、API サーバは適切な KMS から必要な暗号化キーをリクエストし、コンテンツを復号してボットまたは統合に提供します。API サーバはセキュリティの観点から見てプレーン テキスト サービスであり、エンドツーエンドのクリティカル パスに配置されます。これは、企業のコンテンツにアクセスする権利を API サーバに与えるかどうかは各企業が判断することを意味します。

Cisco Webex のセキュリティは業界最高のレベルにありますが、お客様のセキュリティ要件はそれぞれ異なっています。このハイブリッド モデルを有効にする鍵は、お客様の選択にあります。お客様は、核となる Webex Teams システムのみを使用することも、ボットと統合で拡張することもできます。Cisco Webex は、適切に文書化された標準ベースの API を中心に設計されています。つまり、ボット、統合、ウェブホックはすべて、Webex Teams からの許可がなくてもお客様またはサードパーティによって導入できます。また、シスコは https://apphub.webex.com [英語] で一連のボットと統合を提供しています。

オープン プラットフォームでは、サードパーティの統合から企業のコンテンツをどのように保護するかという懸念が生まれます。Control Hub による統合管理によって、管理者（1）は利用可能な統合（2）、ユーザによるこれらの統合の使用状況（3）を可視化し、これらの統合に対して許可または拒否のポリシーを設定できます  。同様のボットの管理機能も利用できます  。

デバイスとブラウザの保護

Webex Teams によって共有した秘密情報をローカルの攻撃者から保護するために、Webex Teams を実行するデバイスを保護することが重要です。組織の Webex Teams クライアントの安全性を維持するために、Webex Teams は以下に例を挙げるような複数の方法を管理者に提供しています。

- モバイル デバイスを PIN で保護することを要求する
- デバイスが紛失したり、ユーザが組織を退職したりする場合に、Webex Teams のコンテンツをリモートで消去する

- 一定期間アクティブでなかった場合に、Webex Teams と Control Hub の Web クライアントのユーザを自動的にログアウトさせる 🔨
- 特定のタイプのクライアントからのアップロードまたはダウンロードを禁止する

さらに、これらすべての機能が Webex Teams のネイティブ機能です。個別のモバイル デバイス管理（MDM）またはモバイル アプリケーション管理（MAM）システムは必要ありません。ただし、Cisco Webex Teams を MDM または MAM で管理することもでき、以下に例を挙げる複数の MDM または MAM コントロールと連携することが検証されています。

- スクリーン キャプチャの防止
- コピー/ペーストの防止
- ローカル バックアップ
- リモート ワイプ
- PIN ロックの要求

予測可能なネットワーク フットプリント

企業が適切なバランスを取るのはますます難しくなっています。クラウドで導入されるアプリケーションの柔軟性も必要ですが、ネットワークの状況を把握できる安心感も求められています。Cisco Webex Teams は、定義した境界内に限定されるネットワーク トラフィック プロファイルを使用することで、両方のニーズを満たすことができます。これらの境界は、クラウドで導入される製品が必要とする柔軟性を実現すると同時に、悪意のあるトラフィックが入り込むリスクを制限できる広さです。

Cisco Webex Teams は、HTTPS/WebSockets の 2 種類のトラフィックと、リアルタイム メディアのみを送信します。HTTPS と WebSockets は Cisco Webex との通信のために使用され、TCP ポート 443 で実行されます。リアルタイム メディア パケットでは、小規模な範囲のポートで UDP が使用されます。メディア パケットは、指定した IP 範囲内にある Webex Teams メディア サーバと交換されます。Webex Teams のネットワーク要件の完全な説明は、こちらのコラボレーション ヘルプ記事でご確認いただけます。

Cisco Webex Teams の保護

Cisco Webex Teams には、外部の干渉から保護するために、セキュリティ メカニズムのスイートが組み込まれています。ユビキタスで高度な暗号化が搭載されているため、前述のエンドツーエンドの保護のみでなく、データは送信中と保管中も保護されます。Webex Teams のエンジニアリングはシスコの業界をけん引する慣行に従い、Webex Teams の脆弱性の可能性を低減しています。また、脆弱性が存在する場合は迅速に発見して修正できるようにしています。

通信のセキュリティ

Webex Teams のすべてのネットワーク通信は、一般に信頼されている認証局（CA）を使用して、Transport Layer Security（TLS）プロトコルによって保護されています。これには、クライアントとコアの間の通信、Webex Teams サーバ間の通信、コアとセキュリティ レルムでお客様がホストするサービスの間の通信が含まれます。このレベルの保護によって、お客様のネットワーク、送信ネットワーク、クラウド データセンターの攻撃者は Webex Teams の通信を読み込み、傍受、変更できません。

Webex Teams クライアントと Webex Teams コアの間の通信では「公開キー ピンニング」として知られる追加の技術が使用されます。公開キー ピンニングによって、サーバ偽装のリスクを大幅に低減できます。ピンニングなしでは、約 2000 の一般に信頼される認証局（CA）が発行する証明書を使用して、不正なユーザが Webex Teams の通信を傍受できます。ピンニングによって、このリスクを一握りの入念に吟味された CA に隔離できます。ピンニングによって許可する CA 自体に強力なセキュリティ慣行があることを検証するだけでなく、シスコでは、CA が決して署名権限を他者に委任しないように要求しています。これは、受任者の慣行がシスコの標準を満たしていないリスクがあるためです。このコミットメントは、発行者の認証慣行規定（CPS）および CA の証明書で（ゼロに設定された「pathLenConstraint」を含めることで）明示する必要があります。

一部のお客様のネットワーク環境には、TLS サーバを偽装するセキュリティ デバイスが含まれます。これらのデバイスは、「SSL 検査」デバイス/プロキシと呼ばれることもあります。デフォルトでは、これらのデバイスはピンニングと互換性がありません。クライアントに表示される証明書は、承認された CA のものではないためです。したがって、Webex Teams デスクトップ クライアントと Webex Teams Web クライアントはより柔軟なピンニング ポリシーを適用します。サーバの証明書がピンされた CA から発行された場合、または**管理者がホスト コンピュータにインストールした CA によって発行された場合**は TLC 接続を許可します。Webex Teams のルーム システム（SX、DX、MX、Room シリーズなど）は、お客様の CA を信頼するように設定することもできます。Webex Teams モバイル クライアントと Webex Board ではこの機能を利用できず、SSL 検査が実行されるネットワークでは使用できません。

暗号化されたストレージ

Webex Teams ではネットワークを移動するデータが暗号化されるだけでなく、「保管中」のデータにも暗号化が適用され、依存するストレージ デバイスの侵害に対して保護されます。ほとんどの Webex Teams サービスにおいて、お客様のデータは前述のエンドツーエンドの暗号化によってすでに暗号化されています。

ユーザの Webex Teams アプリケーションには、ユーザのクレデンシャル、ユーザが受け取ったメッセージとファイル、これらのコンテンツ アイテムを復号するためのキーが保存されています。これらはすべて、データセンターのサーバよりも盗難にあう可能性が高いコンピュータや電話に保存されます。Webex Teams アプリケーションは、すべての情報を暗号化されたデータベースに保存し、Windows データ保護 API など、プラットフォームが提供する API を使用してデータベースの暗号化キーを保護します。（Webex Teams Web クライアントは、現在暗号化されたストレージを使用していません）。さらに、企業の管理者は Webex Teams を使用して、クライアントのデバイスにキャッシュされたデータをリモートで削除できます。

企業の Webex Teams KMS によって、企業のコンテンツを暗号化するために使用されたキーのデータベースが管理されます。シスコが運用する KMS を利用する場合、このデータベースのレコードはメモリのみに保存されるマスター キーで暗号化されます。お客様独自の KMS を運用する場合、データベースはお客様が提供し、セキュアな設定ファイルに個別に保存されたマスター キーを使用して暗号化されます。マスター キーをローテーションする機能もあります 🔨。

プラットフォームとサービスのセキュリティ

Webex Teams は、ISO 27001:2013 認定と、SOC2 Type 2 および SOC 3 認定を受けています。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、脆弱性評価とペネトレーション テストの実施、サードパーティの監査者による毎年の監査の実施、インシデント対応時間の SLA の達成が必要です。

また、Cisco Webex Teams は HHS セキュリティ リスク評価ツールに基づく HIPAA 自己評価も実施しており、お客様の HIPAA コンプライアンスのニーズを満たすことができるため、医療分野でも使用できます。

Webex Teams ソフトウェアの開発、導入、運用は、シスコ セキュア開発ライフサイクル（CSDL）に従っています。

インシデント対応および脆弱性レポート

Cisco Product Security Incident Response Team（PSIRT）は、シスコ製品のセキュリティ インシデント対策を担当しています。Cisco PSIRT は、シスコの製品とネットワークに関係するセキュリティ脆弱性情報の収集、調査、およびレポートの公開を管理する専門のグローバル チームです。オンコールの Cisco PSIRT は 24 時間態勢で、シスコのお客様、独立系セキュリティ研究者、コンサルタント、業界団体、およびその他のベンダーと協力して、シスコ製品およびネットワークのセキュリティに関する潜在的な問題を特定しています。

個人または組織で製品のセキュリティに関する問題が発生している場合は、Cisco PSIRT にご連絡ください。シスコは、独立系の研究者、業界団体、ベンダー、お客様、さらに製品またはネットワークのセキュリティに関与する各種ソースからのレポートを歓迎します。Cisco PSIRT には以下のいずれかの方法でご連絡ください。

	緊急サポート
電話	+1（877）228-7302（北米内からのフリー ダイヤル） +1（408）525-6532（国際直通電話）
時間	24 時間、年中無休

	緊急を要しないサポート
電子メール	psirt@cisco.com
時間	メールで送信されたサポート リクエストについては、通常 48 時間以内に対応します。

詳細については、http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html [英語] をご覧ください。