ホワイトペーパー

Cisco Spark のセキュリティとプライバシー

バージョン 1.0（2016 年 6 月）

Cisco® Spark 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 Spark® アプリケーションは、Spark 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一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 Spark Cloud と Cisco Spark Messaging のセキュリティとプライバシーの概要を示します。

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に関する課題

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 Spark 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、シスコとサードパーティの統合により付加価値を提供することも可能です。Cisco Spark 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排他的に管理できます。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、コンテンツの暗号化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、Spark 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、暗号化されたデータに対して多数の付加価値機能を使用することもできます。Spark では、革新的なメッセージ インデックス、権限モデル、認証フロー、暗号化、導入モデルなどによって、Cisco Spark Cloud で復号されなかったコンテンツのグローバル検索などの機能もサポートされます。

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。しかし送信中の暗号化では、クラウド サービス プロバイダー自体にデータが漏洩することを防ぐことができません。Spark Cloud への接続、および Spark Cloud からの接続のすべては送信中に暗号化されますが、Spark ではさらに、アクセスが明示的に許可されない限り、シスコがユーザのコンテンツを参照できないようになっています。

Spark 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。Spark では、*難読化された ID*[1]、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、Spark のサービスにはこれらの保護機能が最初から組み込まれています。

エンドツーエンドのコンテンツ暗号化

Cisco Spark Cloud でのエンドツーエンドのコンテンツ暗号化に不可欠なコンポーネントが、Key Management Server（KMS）です。KMS は、Spark クライアントがメッセージやファイルの暗号化と復号に使用する暗号化キーの作成、保存、承認、アクセス許可を行います。Spark でエンドツーエンドの暗号化が可能になっているのは、KMS と、Spark Cloud のその他の部分で、アーキテクチャと運用が分離されているためです。それらはクラウド内の別個のレルムまたは信頼できるドメインに分離されているとも言えます。つまり KMS は*「セキュリティ レルム」*内にあり、Spark を構成するその他すべてのコンポーネント サービスは*コア*内に置かれます。

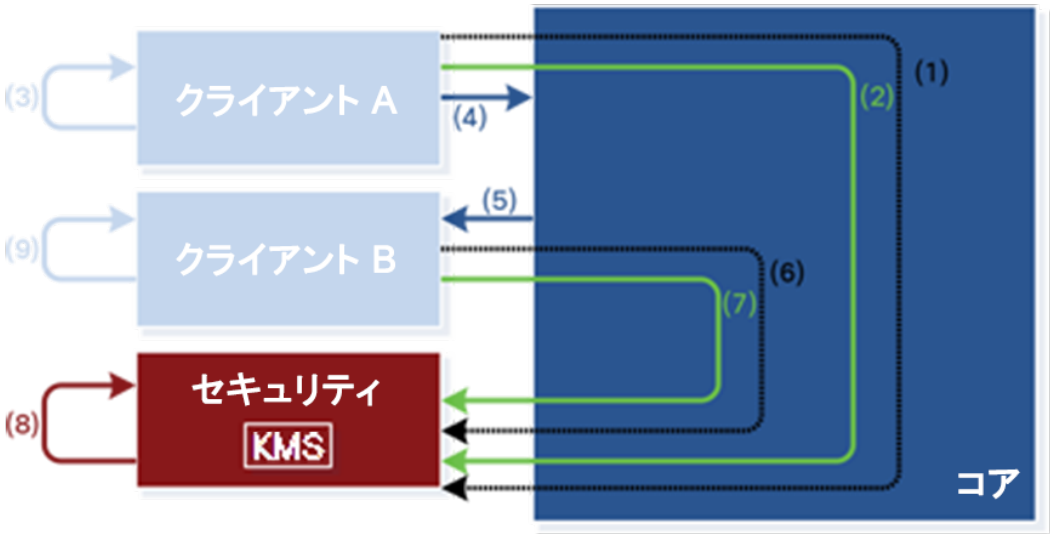
KMS との通信は Cisco Spark Cloud を通過しますが、エンドツーエンドで暗号化されるため、コアが読み取ることはできません。そして Cisco Spark Cloud 内の他の部分では使用されていないアクセス トークンによって認証されます。このモデルにより、暗号化キーに対する適切なアクセスが確保されると同時に、それらの通信または KMS に保存されているキーにコア サービスのコンポーネントがアクセスできないことが保証されます。シスコの場合、セキュリティ レルム内のサービスは、別個のテナント内の別個のインフラストラクチャ上で運用されます。セキュリティ意識の高い企業のお客様は、KMS を含むセキュリティ レルム サービスをオンプレミスで導入する場合もあるでしょう。それについては次のセクションで説明します。

---

[1] セクション「難読化された ID」を参照してください。

Spark ユーザがコンテンツを Spark ルームに送信する場合は、最初にユーザのクライアントで、図 1 の **(1)** に示すように、クライアントと KMS 間のセキュアなチャネルを確立する必要があります。クライアントと KMS 間のセキュアなチャネル用の共有秘密キーを確立するために、クライアントと KMS は、認証済みの一時楕円曲線ディフィー ヘルマン（ECDH）交換を行います。この交換により、メッセージをセキュアに交換できる共有対称キーが生成されます。

図 1. Cisco Spark におけるクライアント - KMS 間の通信



このチャネルを通過する情報およびキーをシスコまたはその他の第三者が確認または変更できないようにし、また中間者として操作できないようにするには、このチャネルでの認証が必要です。認証メカニズムでは、KMS で公開キー インフラストラクチャ（PKI）証明書を使用します。この証明書には、企業のドメイン名に一致する、共通名（CN）またはサブジェクトの別名（SAN）のエントリが含まれています。クライアントは、KMS サーバ証明書のパブリック部分を使用して、KMS に対する ECDH 交換の半分を暗号化します。KMS からの ECDH 応答は、KMS のサーバ証明書のプライベート部分を使用して署名されます [2]。これは ECDHE-RSA メカニズムとはわずかに異なり、クライアントが自身のキーを使用して署名するのではなく、サーバの公開証明書を使用して暗号化を行います。そのためクライアントは証明書を必要としません。ただしその場合は当然ながら、クライアントが KMS の証明書を認証できなければなりません。そのために KMS 証明書で、デスクトップおよびモバイル デバイスで広範に信頼されているパブリック認証局（CA）を利用するか、ユーザが Cisco Spark へのアクセスに使用するエンド デバイスに、企業がプライベート CA ルート証明書をプッシュする必要があります。クライアントに対するプライベート CA 証明書のプッシュを Cisco Spark が処理することはありませんが、Cisco Spark クライアントは、クライアントの信頼できる証明書ストアに存在するどの証明書も使用できます。

クライアントと KMS が、認証済みの ECDH メカニズムを使用して対称キーについて合意すると、**(2)** に示すように、クライアントはそのチャネルを使用して、1 つの Spark ルームとそのルーム内の参加者宛のコンテンツを暗号化する目的で、新しい暗号化キーを要求します。このキーをカンバセーション キーと呼びます。

ユーザがメッセージを書き込むと、クライアントがカンバセーション キー **(3)** を使用してメッセージを暗号化し、宛先ルームのルーム ID でラベルを付け、コアに送信します **(4)**。コアは暗号化された形式のメッセージを受信します。コアにはカンバセーション キーがないため、メッセージを復号できません。コアはメッセージのメタデータで指定されているルーム ID に関連付けられているユーザのリストをチェックし、ルーム内の他のユーザに暗号化されたメッセージを送信します **(5)**。さらにメッセージは、暗号化された形式でコアのメッセージ データベースに保存されます。このデータベースは適切なルームに関連付けられています。

[2] クライアントは KMS 認証トークンによって認証されます（「ルームの承認」セクションを参照）。

他のユーザのクライアントが受信した時点では、メッセージは暗号化されたままです。他のユーザのクライアントは KMS に問い合わせて、メッセージを復号するためにカンバセーション キーを取得します（**6**、**7**）。コンテンツの受信者（**6**）と関連付けられている KMS との交換は、最初の交換（**1**）と同じです。KMS は各ユーザを認証し、関連付けられたルーム内にいるという基準により、カンバセーション キーにアクセスする権限を確認します（**8**）。KMS は受信者にカンバセーション キーを配布し、メッセージを復号して読み取ることができるようにします（**9**）。

上記のフローでは、ホップバイホップとエンドツーエンドという、異なる 2 つの暗号化レイヤが使用されていることが重要です。前述したように、ユーザのコンテンツと、クライアント - KMS 間のインタラクションは、ユーザ コンテンツ用のルーム固有のカンバセーション キーとクライアント - KMS 間のコンテンツ用の一時キーを使用して、対称暗号化によってエンドツーエンドで暗号化されます。現在 Spark で使用されている対称暗号は AES256-GCM です。エンドツーエンドの暗号化コンテンツは、クライアントからサーバ、サーバからサーバ、およびサーバから他のクライアントに送り戻される間に、ホップバイホップの暗号化によってさらに保護されます。ホップバイホップの暗号化では Transport Layer Security（TLS）プロトコルが使用されます。TLS は、Web ブラウザが銀行やオンライン小売業者との通信に使用するプロトコルです。エンドツーエンドとホップバイホップの両方で使用される暗号化方式が現在最良の方法ですが、Spark はアルゴリズム アジリティと呼ばれる概念を基に設計されています。現時点で最も強力な方式が古くなり、業界が推奨する新しい方式がそれに代わる場合には、アルゴリズム アジリティにより、新しい暗号化メカニズムの迅速な導入が可能になります。

前述のようなユーザが生成したコンテンツには、Spark で共有されるすべてのメッセージ、ルームのタイトル、ファイルが含まれています。

カンバセーション キーの URI

カンバセーション キーは、一意の Uniform Resource Identifier（URI）によって識別され参照されます。エンドツーエンドの暗号化コンテンツがクライアントから Spark Cloud に送信される場合、ヘッダーにはカンバセーション キーの URI が含まれます。URI には、要求者が認証と承認チェックに合格すると仮定して、どの KMS がキーを生成したかに関する詳細と、キーの取得に使用できる場所が示されます。

多数のカンバセーション キーとキーのローテーション

Spark ルームにコンテンツを提供するクライアントごとに、少なくとも 1 つのカンバセーション キーが常に存在します。たとえば、Alice が自分のモバイル デバイスとラップトップから Spark ルームにコンテンツを提供し、Bob がラップトップから同じルームにコンテンツを提供するのと同時にモバイル デバイスでコンテンツを表示している場合には、3 つの対称カンバセーション キーがルーム内でアクティブになります。1 つは Alice のモバイル デバイス用、1 つは Alice のラップトップ用、もう 1 つは Bob のラップトップ用です。

カンバセーション キーは、ユーザが自発的に（退出）または強制的に（拒否）ルームから出たときに対応して、ローテーションされます。ユーザの退出を認識したクライアントは（「承認の表示」を参照）、そのルームに追加コンテンツを提供する前に、カンバセーション キーのローテーションを行う必要があります。Spark Cloud ではこの動作が強制されます。クライアント - KMS 間の対称キーも定期的にローテーションされます。

ルームの承認

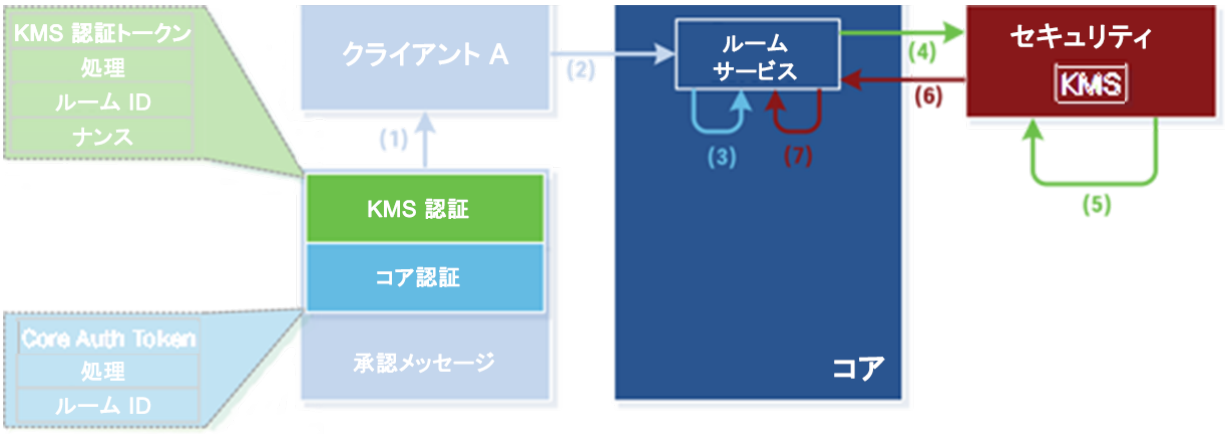
ユーザがルームで他のユーザを追加または削除する場合、ユーザのクライアントは、Spark とユーザの KMS の両方が、ルームの承認に対する変更を認識していることを確認する必要があります。クライアントでは、これらの変更について Spark と KMS に通知する承認メッセージが生成されます。承認メッセージは、2 つの異なるサブメッセージで構成されています。

- 一方はコア用のクライアントの認証トークン [3]、追加/削除操作、そしてその操作が適用される一意のルーム ID が含まれている承認変更操作ブロックです。
- もう一方は、KMS 認証トークン、追加/削除操作、その操作が適用される一意のルーム ID、および *ナンス*（1 回限り使用されるデータのランダム ブロック）が含まれている暗号化された承認変更操作ブロックです。

[3] トークンはすべて OAuth ベアラー トークンです。

サブメッセージは、カンバセーション キーの取得中にクライアントと KMS 間でネゴシエートされた、一時対称キーによって暗号化されます。重要なことは、暗号化されたサブメッセージでは KMS 認証トークンが使用される一方、コア宛のサブメッセージではコアの認証トークンが使用されることです。KMS の変更操作に暗号化レイヤを追加するとともに、こうした異なる認証トークンを使用することで、コアがクライアントを偽装して KMS に対する承認要求を改ざんすることを防止します。

図 2. 2 部構成の承認メッセージの生成



- クライアントは図 2 に示す 2 部構成の承認メッセージ (**1**)を生成すると、TLS を通じてコア内のルーム サービスにメッセージを送信します(**2**)。
- ルーム サービスは、コア認証トークンを含むコアのサブメッセージを検証し(**3**)、ルーム ID で指定されているルームを変更する承認を要求元のユーザが得ていることを確認します。
- 問題がなければ、ルーム サービスは、コアのサブメッセージに含まれるルーム ID とコア認証トークンから復号されたユーザの ID と合わせて、暗号化されたサブメッセージをユーザの KMS に転送します(**4**)。
- プレーンテキスト メッセージのルーム ID と認証済みのユーザ ID を含めることで、KMS は認証と承認でルーム サービス要求と KMS 要求が一致することを確認できます。KMS は受信したメッセージを復号し、KMS 認証トークンを検証し、要求元のユーザが指定されたルームを変更することに対して承認を得ていることを確認します(**5**)。
- 問題がなければ、KMS は要求された操作を適用し、正常に適用されたことをルーム サービスに通知します(**6**)。KMS の操作が適用された通知を受けると、ルーム サービスはプレーンテキスト操作を適用します(**7**)。

このアプローチの利点は、フェイト シェアリングが可能になることです。クライアントがルームでのユーザの追加または削除を要求すると、コアと KMS の両方において、ユーザが追加または削除されるか、または、追加または削除されません。これは一般的に*アトミック性*と呼ばれる特性で、2 つの操作が不可分の操作になります。それにより、コアと KMS の同期が維持されると同時に、暗号化されたコンテンツの承認をコアが制御し、コンテンツの復号に必要なキーの承認を KMS が制御するという、セキュリティ上の利点が得られます。

承認の表示

特定の Spark ルームでの承認済みユーザのリストは、同じ Spark クライアント内のルームにおけるその他すべての承認済みユーザが見ることができます。承認済みユーザのリストに加えて、ルームでは、ルーム内のコンテンツとともに参加、退出、および拒否アクティビティがインラインで表示されます。これらのインライン メッセージにより、ルームのメンバーは、ルームに誰が参加し誰が退出したか、またそれが誰によって行われたかを知ることができます。従業員が退職や解雇などによって組織を離れる場合、Spark では所属していたすべてのルームから強制的にその従業員を退出させます。これらにより、そのルームの他の参加者は、退出した従業員がルームの既存または将来のコンテンツにアクセスできないことを認識できます。他のすべての参加者は、カンバセーション キーのローテーションを行う必要があります。

キーに対する機能アクセス

現行の形式では、一部の機能は、シスコがキーに対するアクセス権を持っている場合のみ使用できます。そのような機能の 1 つがドキュメントのトランスコーディングです。これは、Microsoft Office ドキュメントなどの多数のファイル タイプをイメージ形式に変換し、受信者のプラットフォームではネイティブにサポートされていない形式を Web デバイスとモバイル デバイスですばやく表示できるようにする、バックエンド プロセスです。キー アクセスを必要とする機能は、その他すべてのユーザ クライアントと同じ方法でエンタープライズ KMS からキーを要求します。ただしその場合は、エンタープライズ KMS 内の特定のキーにアクセスすることを、エンタープライズ管理者によって特別に承認されているマシン アカウントが使用されます。マシン アカウントはユーザ アカウントと似ていますが、ユーザ アカウントはユーザ名とパスワードに関連付けられる一方、マシン アカウントはマシン ID とマシン キーに関連付けられ、M2M（Machine-to-Machine）認証に使用されます。

Spark ルームで共有する重要な資料に、シスコがアクセスすることを好まないお客様もいらっしゃいます。そのため Spark では、全社的なキー アクセスを必要とする機能をお客様がオフにできるようになっています。これらの機能をオフにすることで、企業の KMS 内の機能に関連付けられたマシン アカウントの承認が排除され、キー アクセスが行われなくなります。ただし、他社からの参加者がいるルームにドキュメントまたはコンテンツを社内ユーザがアップロードしている場合は、他社がクラウド KMS、またはキーへのアクセスを必要とする機能を使用することがあるため、コンテンツへのクラウド アクセスが発生する場合があります。

現在キー アクセスを必要とする全機能のリストと、それらの機能を無効にする手順については、Cisco Cloud Collaboration 管理ポータルを参照してください。「統合と拡張性」セクションでは、サードパーティが Cisco Spark プラットフォームに新機能を追加する方法について説明しています。

セキュリティ レルム導入オプション

前述のように、シスコではセキュリティ レルムと Cisco Spark Cloud のその他の部分を分離することで、Spark のファブリックにエンドツーエンドの暗号化を組み込んでいます。クラウド サービス プロバイダーとしてのシスコが、お客様のコンテンツにアクセスできないようにするために、より強力な保証を求めるお客様も存在するため、シスコは KMS を含むセキュリティ レルム内のサービスの導入に関して、柔軟な選択肢を提供しています。

お客様は、シスコがホストするセキュリティ レルム サービスを使用するか、オンプレミスでサービスを導入するかを選択できます。シスコでは各サービスの市販バージョンに加えて、シスコがコンテンツにアクセスできないことを企業のお客様が検証できるようにするため、KMS などのセキュリティ レルム サービスのソース コードも提供します。さらに、セキュリティ レルム内のすべてのサービスでは、RESTful HTTPS 経由の JSON などの業界標準のプロトコルを使用および提供します。またシスコは、シスコ サービスの完全互換品として機能するサードパーティのオープンソース ソリューションおよび商用ソリューションを将来実現することを視野に入れ、Cisco Spark で使用されている主要な管理手法の標準化にも取り組んでいます。適切に文書化され、標準に準拠したインターフェイスにより、セキュリティを重要視するお客様や、大幅なカスタマイズを必要とするお客様は、各種サービスを独自の実装方法で自由に構築できるようになります。

現時点で、セキュリティ レルムが Cisco Spark Cloud の外部でホストされている場合、シスコはお客様またはパートナーと協力してソフトウェアを運用します。この共同モデルでは、シスコはログや分析にアクセスし、またアップグレードを提供します。これらのログには、キーや、個人を特定できる情報が含まれることはありません。同様に、シスコがサーバのパフォーマンスを把握できるように、メトリックが集約されます。お客様またはパートナーは、ハードウェアの導入、およびサービス全体のプロビジョニングと設定を管理します。

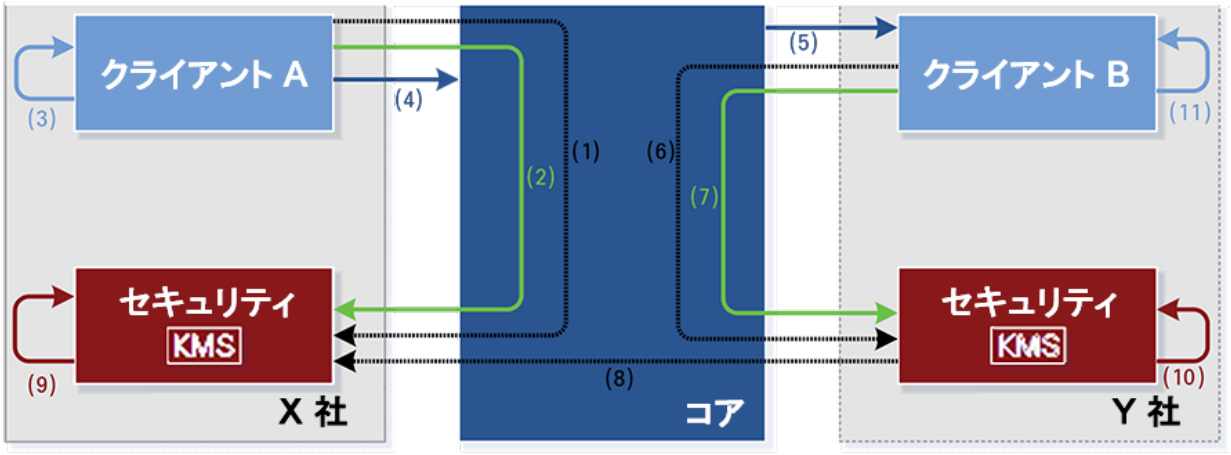
管理フローとインターフェイスが最終的に確定した時点で、パートナーまたはお客様が完全にホストし管理するモデルでセキュリティ レルムを利用できるようになります。このモデルでは、他のレルム内のサービスはシスコが引き続き運用しますが、セキュリティ レルムについては、シスコ パートナーがパートナーの施設内のインフラストラクチャで、またはお客様や任意のクラウド プロバイダーがお客様の社内インフラストラクチャで完全に運用を行います。その場合は、KMS、検索インデクサ、関連付けられているデータベース、さらにセキュリティ レルム内のその他すべてのサービスについて、パートナーまたはお客様が運用を完全に制御できます。

KMS アーキテクチャの標準化に向けたシスコの取り組みについては、http://cs.co/keymanagement [英語] を参照してください。

Key Management Server（KMS）のフェデレーション

Cisco Spark のユーザは 1 つの企業だけに関連付けられており、各企業では独自の KMS を所有していることになります。異なる企業に関連付けられている Cisco Spark ユーザが通信を行う場合でも、カンバセーション キーは 1 人のユーザからもう一方のユーザに渡される必要があります。そのために Cisco Spark では、フェデレーションと呼ばれるプロセスを使用します。フェデレーション プロセスの手順の多くは、前述の「エンドツーエンドのコンテンツ暗号化」セクションの手順と共通しています。ただし、各クライアントが関連付けられている KMS とのみ通信することと、2 つの KMS がキーを共有するために通信を行う手順があることが大きく異なります。従来のフェデレーション モデルとは異なり、KMS フェデレーションでは、お客様やパートナーによる設定やセットアップは不要です。全体的なサービスはとしては、すべてのユーザが世界中のユーザと通信できるクラウド モデルのままです。

図 3. 複数の企業にわたる Spark 通信



- すでに説明したように、Spark ユーザがコンテンツを Spark ルームに送信する場合は、図 3 の **(1)** に示すように、最初にユーザのクライアント（クライアント A）が、関連付けられている KMS（X 社）との間にセキュアなチャネルを確立してから、カンバセーション キーを要求する必要があります **(2)**。前述の通り、この場合も、認証済みの一時 ECDH 交換によって確立されたセキュアなチャネル **(1)** を使用します。
- 次にクライアント A は、対称暗号化とカンバセーション キーを使用してコンテンツを暗号化し **(3)**、Spark Cloud に送信します **(4)**。
- Spark Cloud はメッセージのメタデータで指定されているルーム ID に関連付けられたユーザのリストをチェックし（この場合は Y 社のユーザ）、暗号化されたメッセージが Spark によって受信者のクライアントに送信されます **(5)**。クライアント B が受信した時点では、メッセージは暗号化されたままです。

- クライアント B は Y 社の KMS にアクセスし、受信したメッセージ用のカンバセーション キーを取得します（**6**、**7**）。この要求を受信した Y 社の KMS は、カンバセーション キーの URI を確認して、キーがリモートの KMS にあると判断します。さらに Y 社の KMS は、コアを経由した X 社の送信元 KMS 宛の相互 TLS チャネルを確立し（**8**）、キーを要求します。
- この相互 TLS チャネルは、各企業の KMS に関連付けられている PKI 証明書によって認証されます。この PKI 証明書は、下位の CA または中間証明書を発行しない CA が発行する必要があります。

そのような CA のリストについては、Cisco Cloud Collaboration 管理ポータルを参照してください。

この場合の接続は、Spark のすべての接続と同様にコアを通じてルーティングされるため、ファイアウォール要件とリモートピアが最小になります。ただし、Spark でのその他すべての通信と同様にエンドツーエンドで暗号化されるため、コアでは内容を見ることができません。X 社の KMS はこの要求を受信すると、Spark ルームに関連付けられているユーザの承認リストをチェックして、Y 社のユーザが実際に Spark ルームに対するアクセス承認を得ていることを確認します。

X 社の KMS では、X 社に関連付けられているユーザだけを見ることができるため、Y 社のユーザを認証することはできません。したがって、照会する KMS が Y 社に属することを確認するには、Y 社の KMS が提供する PKI 証明書が必要になります。

- X 社の KMS は、キー要求を承認するために、Y 社から少なくとも 1 人のユーザがルームに有効に参加していることを確認します（**9**）。
- 照会する企業の KMS が認証され、承認チェックが実行されると、X 社の KMS は確立されている相互 TLS チャネルを通じて、要求されたカンバセーション キーを Y 社の KMS に送信します。
- Y 社の KMS はローカルのデータベースでキーをキャッシュし、承認チェックを実行して、要求元のクライアントがこのキーへのアクセスが承認されたユーザに属することを確認します（**10**）。
- 承認されると、Y 社の KMS がカンバセーション キーをクライアント B に配布し、クライアント B はメッセージを復号して読むことが可能になります（**11**）。

企業に関連付けられているユーザが企業に属さないユーザと通信する場合にも、同じ交換が行われます。ただし、関係する 2 つの KMS のうち 1 つを、シスコが運用し管理する点だけが異なります。

検証可能性

キー管理に使用するプロトコルを含め、Cisco Spark で使用するプロトコルは、このドキュメントの各所で参照されているように、IETF または W3C の既存の規格あるいは審理中の規格に従っています。これらのプロトコルを適切に導入することで、企業のコンテンツについてエンドツーエンドのセキュリティが確保されます。プロトコルのレベルは、お客様がパケット検査によって容易に確認できますが、セキュリティ レルム内の信頼できるサービス内部の仕組みは、簡単に確認できるものではありません。こうしたブラックボックス的な問題を解決するために、セキュリティ レルム サービスは監査ログを提供します。この監査ログを、クライアントの使用状況と、明示的に許可されているクラウド サービス アクセスの両方と比較することで、システムが適切に運用されているかどうかを確認できます。さらにシスコでは、企業のお客様がセキュリティ レルムに含まれるコンポーネントのソース コードにアクセスできるようにし、検査、コンパイル、導入用にバイナリ形式で提供されている同一のコンポーネントとのバイナリ比較を可能にします。

リアルタイムのメディア暗号化

音声、ビデオ、デスクトップ共有など、Cisco Spark 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 Cisco Spark Cloud では、ミキシング、分配、および公衆電話交換網（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。*

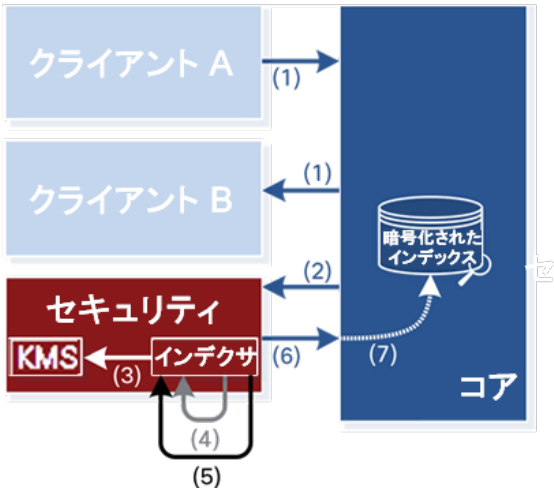
SRTP のセキュリティを将来的に向上させるために、シスコは IETF の新しい Privacy Enhanced RTP Conferencing（PERC）作業部会にも推進役として参加しています。PERC では、エンドツーエンドでメディアを暗号化しながら、ホップバイホップでの認証も可能にすることを目標としています。この新しい標準が成熟すれば、Cisco Spark ではそれをリアルタイム メディアの暗号化に活用して、リアルタイム メディアの暗号化キーが KMS によって裏付けられるようにします。それによって Cisco Spark Cloud では、PERC 互換通信の復号が不要になります。PERC 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。PERC の詳細については、https://datatracker.ietf.org/wg/perc [英語] を参照してください。

セキュアでスマートな暗号化検索

Spark Core ではコンテンツの内容が隠されるため、クラウド内でのメッセージ検索は不可能だと思われるかもしれません。しかしシスコは、Cisco Spark Core に復号機能がなくてもグローバルなメッセージ検索を可能にする、革新的な方法を編み出しました。

これを実現するのが、セキュリティ レルムに追加されたインデクサというコンポーネントです。KMS と同様に、インデクサはアーキテクチャ面と運用面の両方でコアとは分離されていますが、KMS と緊密に結びついています。インデクサは、グローバルなメッセージ検索に必要な 2 つの基本的なタスクである、検索インデックスの構築とクエリに関して、重要な役割を担っています。

図 4.　メッセージのインデックス シーケンス



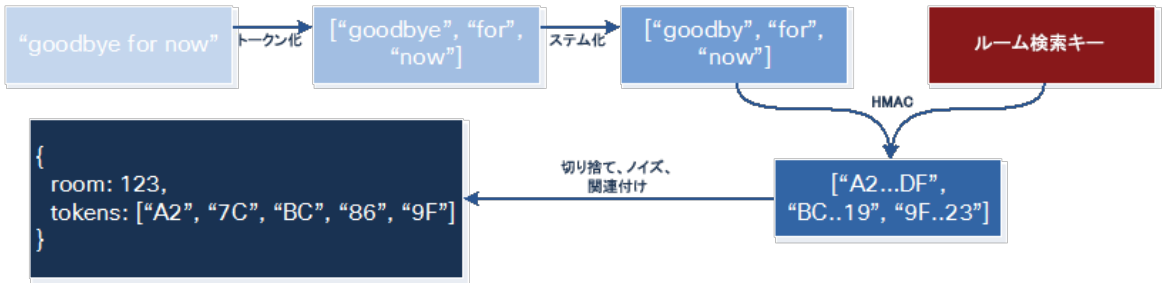
検索インデックスの構築

最初に検索インデックスを構築します。

- ユーザが Spark でメッセージを送信すると**(1)**、メッセージはエンドツーエンドの暗号化形式でインデクサに送信されます（図 4 の**(2)**）。インデクサはメッセージの復号に必要なカンバセーション キーを KMS に問い合わせます。インデクサは、エンタープライズ ポリシーに従ってすべてのルームに導入される、検索のための Spark Bot[4] です。
- KMS はインデクサに適切なカンバセーション キーを提供します。これは、インデクサがルームにアクティブに参加していて、ルームのリソースを復号する承認を得るためです**(3)**。
- インデクサはメッセージを復号し、メッセージを構成する各単語に分割します**(4)**。
- 次にインデクサは、ルーム固有の KMS に保存されている特別なルーム検索キーを使用して、各単語または各単語の語根に一方向の暗号ハッシュを適用します [5]**(5)**。たとえば「goodbye for now」は、「goodbye」、「for」、「now」に分割して、各単語をハッシュします。その結果、メッセージが投稿されたルームに属する、すべてのハッシュ済み単語のリストが得られます。ハッシュは基本的に一方向の暗号化であり、特定のハッシュを元のメッセージの単語に戻す方法はありません。インデクサはこのリストに複数のランダムな「ノイズ」ハッシュを追加し、頻度分析を通じてルームのメッセージを元に戻すことができないようにします（英語の文言には「and」や「the」が頻繁に現れるため、ノイズを追加することで、ルーム内のハッシュが同じ頻度分布と同じになることが防止されます）。
- 最後の手順として、インデクサがこのハッシュのリストを Spark Cloud に送信し**(6)**、送信されたリストは暗号化形式で検索インデックスに保存されます**(7)**。その結果 Spark Cloud では、ルームに関連付けられているすべてのメッセージのすべての単語について、Spark Cloud によって復号されない暗号化形式のインデックスが得られます。

[4] 以下の「*統合と拡張性*」を参照。
[5] 80 ビットに切り捨てられた SHA-256 HMAC を使用します。

図 5. メッセージング インデックスのデータ フロー

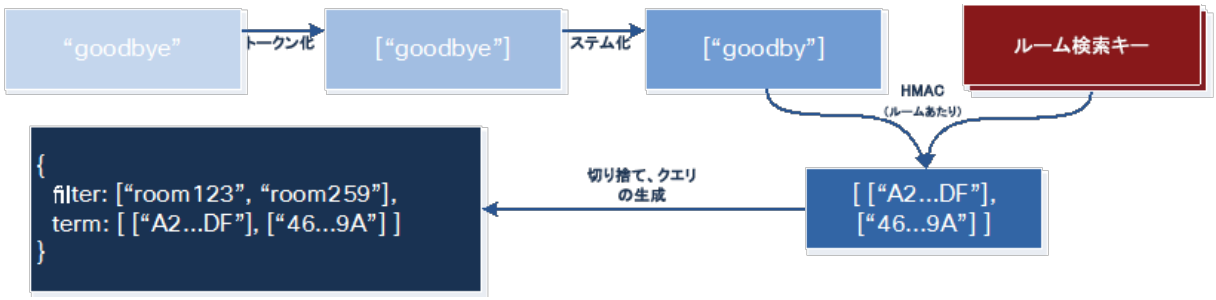


検索インデックスのクエリ

ユーザが検索を実行すると、ユーザが 1 対 1 でインデクサと会話するように、クライアントとインデクサが対話します。つまり、ユーザ間の対話についてすでに説明した、すべてのエンドツーエンドの暗号化が、ユーザとインデクサ間のクエリで使用されます。

具体的には、検索クエリは最初に、ユーザのクライアントとインデクサ間の通信を暗号化するためのエンドツーエンドの暗号化キーを使用して、ユーザ クライアントで暗号化されます。各ユーザは、特定のインデクサに関連付けられています。ユーザのクライアントは、暗号化されたクエリを Spark Cloud に送信します。これにより、暗号化されたクエリは、ユーザがアクセスを承認されているルームのリストと合わせてインデクサに転送されます。Spark Cloud は検索クエリを復号できません。これは、Spark Cloud がアクセスできないキー、つまり特定のクライアントがインデクサと対話するためのエンドツーエンドのカンバセーション キーによって暗号化されているためです。

図 6. 検索データ フロー



次にインデクサは、検索インデックスの構築時とまったく同じ手順を実行します。クエリを単語と語根に分解し、ユーザがアクセスできる各ルームの検索キーを使用して、それぞれの要素をハッシュします。したがって、10 のルームに属しているユーザが 2 語の検索クエリを入力すると、インデクサは最小 20、さらに各単語の語根の数に応じてそれ以上の数のハッシュ済み検索条件を生成します。インデクサはハッシュ済み検索条件のリストを Spark Cloud に送り返します。

それにより Spark Core は、検索インデックスで一致を検索することができます。インデクサから受信したいずれかのハッシュに関連付けられたルームが検索インデックスで見つかると、リストが構築され、ユーザのクライアントに送り返されます。クライアントでは、クライアント キャッシュからの関連付けられているカンバセーション キー、または KMS から取得した関連付けられているカンバセーション キーとその結果が組み合わされて、検索結果がユーザに表示されます。

両方の長所を活かす

Spark 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。1 回の検索では何千ものハッシュ済み検索条件の生成と比較が行われる場合がありますが、Spark の検索機能では、今日のインターネット検索に求められる効率性が実現しています。

統合と拡張性

Cisco Spark Cloud は画期的なプラットフォームであり、Cisco Spark は優れたチーム コラボレーション ツールですが、パートナーとお客様は、カスタマイズと拡張が必要になる場合もあるでしょう。シスコでは、簡単に習得して使用できる API を目指しています。開発者は、複雑なプラットフォームの複雑性にわずらわされずにアプリケーション開発に集中できるように、包括的でありながらシンプルな API を求めています。シスコでは、基盤となるプラットフォームの複雑性を排除しながら、API を洗練させる努力を重ねてきました。

Cisco Spark Cloud のコアがコンテンツにアクセスすることはありませんが、開発者、パートナー、またはお客様が、コンテンツへのアクセスが必要になるようなプラットフォーム拡張を行う場合もあるでしょう。そのため、Cisco Spark Cloud の拡張はコアの外部に置かれ、お客様またはユーザが明示的に有効にする必要があります。プラットフォーム拡張は Cisco Spark Cloud の外部にあるため、拡張をどこに導入するか、誰が管理するか、どのようなリソースにアクセスできるかを、お客様が選択できます。Cisco Spark の統合と拡張では、「キーに対する機能アクセス」セクションで説明した方法と同じ手順で、暗号化キーにアクセスする必要があります。

Cisco Spark では現在、ボット、アプリケーション、Webhook という 3 つのカテゴリの統合を定義しています。しかしお客様、そしてサードパーティは、シスコが予測していなかった新たな方向で、プラットフォームを拡張することもできます。Cisco Spark Cloud API の詳細については、https://developer.ciscospark.com [英語] を参照してください。

ボット

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得られます。ボットはルームを作成するか、アクセスする必要があるルームに招待される必要があります。ルームの招待は、エンタープライズ ポリシーから、またはすでにルームに参加しているユーザから出されます。

アプリケーション

アプリケーションは、パーソナル アシスタントやドキュメントの翻訳など、ユーザ単独の機能を拡張します。アプリケーションは多くの点で、ユーザ インターフェイスがない、クラウド ホスト型またはサーバ ホスト型クライアントであると見なすことができます。アプリケーションは、関連付けられているユーザがアクセスできるすべてのルームにアクセスできますが、ユーザは特定のルームからアプリケーションを排除することができます。

Webhook

Webhook では、ルームへのコンテンツの投稿や、新しいコンテンツの通知など、シンプル化されたコア機能に単一 URL アクセスを提供します。Webhook は、ボットのように ID を持っているか、アプリケーションのように特定のユーザの ID を利用するという点で、ボットやアプリケーションと同様に動作します。Webhook では、範囲が制限された長期的な OAuth2 アクセス トークンを URL クエリ文字列に組み込み、コンテンツのすべての暗号化と復号を Webhook ワーカー内で実行することで、シンプルな単一 URL を実現します。いずれの場合も、Webhook は単一のリソース（ルームなど）に範囲が限定されます。こうしたアクセス範囲の制限は、Webhook を追加した時点で設定されて固定されます。

企業とユーザの選択

Cisco Spark Cloud 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 モデルを適切に機能させるには、お客様の選択が鍵になります。お客様は、コアだけを使用するか、ボット、アプリケーション、Webhook によってコアを拡張するかを選択できます。企業が特定のボットとアプリケーションを許可するエンタープライズ ポリシーを定義すると、ユーザはそのポリシー内でアプリケーションを選択できます。Cisco Spark プラットフォームは、適切に文書化された、標準に基づく API によって設計されているため、コア外部のコンポーネント（ボット、アプリケーション、Webhook を含む）は、サードパーティや個人が開発したものから取得することができます。

証明書のピニング

Spark のクライアントとコア間の通信は、TLS で暗号化された接続を通じて送信されます。クライアントでは、*証明書のピニング*と呼ばれる手法によって、通信中の傍受、読み取り、変更を防止できます。シスコは、発行元の認証実施規定、または BasicConstraints 拡張の「pathLenConstraint」フィールドが 0 に設定されたルート証明書を通じて中間証明書を発行しない、少数のルート CA にサーバ証明書をピニングすることで、証明書パス内で発行証明書に続いて CA 証明書が発行されないことを示します。

データ プライバシー

Spark 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。Spark では、難読化された ID、きめ細かい管理者ロール、企業とユーザの選択、および透過性を含む、各種プライバシー 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。

難読化された ID

コラボレーション サービスでは、ユーザ ID について充実した概念を確立することが不可欠です。ユーザは、他のユーザを名前、電子メール アドレス、または電話番号で検索し、プロフィール写真によって ID を視覚的に確認して、チームのメンバーとすばやく接続することを求めています。同時に、ユーザ ID 情報はユーザと企業の両方の観点から機密性が重視される場合があります。コンテキストで必要とされるユーザ ID 情報のみが公開されるように制限することが、Spark の基本的な設計原則になっています。

ユーザ ID 情報の公開を制限するために、Spark Cloud では「実際」の ID と「難読化された」ID を区別しています。Spark のユーザ登録の一環として収集されるデータ（ユーザ名、電子メール アドレス、電話番号など）は「実際の ID」と考えられ、Common Identity と呼ばれる Spark Cloud コンポーネントのユーザ プロファイルに保存されます。各ユーザについては、ユーザの難読化された ID となる、128 ビットのランダムな Universally Unique Identifier（UUID）も生成されます。同様に企業についても、難読化された ID として、128 ビットのランダムな「組織 ID」が使用されます。Spark サービスでは、以下の場合を含め、可能な限り常に難読化された ID を使用します。

- **メッセージ ルーティング**：Spark 内のすべてのメッセージが、難読化された ID だけに基づいて、送信者から受信者にルーティングされます。たとえば前述した KMS とインデクサのすべてのインタラクションなど、個々のユーザに関連するクラウド内のすべてのクエリでも、難読化された ID が使用されます。
- **サーバ側のロギング**：Spark Cloud アプリケーション コンポーネントによって、トラブルシューティング目的で生成されたすべてのログでは、難読化された ID が使用されます。
- **分析**：Spark は DevOps モデルで動作します。シスコの開発チームは、パフォーマンスと使用状況に関するデータを分析して、サービス向上の方法を決定しています。開発チームでは、難読化された ID を使用した Spark の使用状況の記録を分析することで、そうした決定を行っています。

もちろん、Spark クライアント、Cisco Cloud Collaboration 管理ポータル、またはサードパーティ統合でユーザ ID または企業 ID を生成する段階では、承認済みのクライアントやクラウド サービス コンポーネントが実際の ID にアクセスする方法も用意されています。Spark クライアント、クラウド コンポーネント、アプリケーション、またはボットで実際の ID へのアクセスが必要な場合は、Common Identity に対して認証が行われ、承認済みの要求者に対してのみ、実際の ID 情報が提供されます。

きめ細かい管理者ロール

Spark のお客様とパートナーは、Cisco Cloud Collaboration 管理ポータルにアクセスできます。このポータルでは、試用、購入、アカウント設定、導入、カスタマー サポート、開発用 API の使用などが可能な、完全なサービス管理機能を利用できます。これらの機能では、ユーザやアカウント、製品の使用状況、設定情報などに関する機密情報にアクセスできるため、この管理ポータルは、それぞれアクセス可能な情報のサブセットが異なる、複数の管理者ロールをサポートするように設計されています。たとえば、サポート管理者はユーザ情報とサポート ログにアクセスでき、パートナーのセールス管理者については、集約された使用状況レポートやサービス トライアルの管理にアクセスが制限されます。完全な権限を持った管理者は、ポータルの全機能にアクセスし、組織内の他の管理者に適切なロールを割り当てることができます。

シスコでは、ロールをパートナーとお客様に割り当てるだけでなく、情報を必要とするシスコ管理者だけにアクセスを制限する目的でもロールを使用します。シスコのサポート管理者とエンジニアは、お客様とパートナーのトラブルシューティングを支援するためにサポート ログとユーザ情報にアクセスできますが、セールスおよびカスタマー サクセス担当者については、セールス管理者ロールに関係するアクセスに制限されています。

企業とユーザの選択

Spark 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 Spark を設定できます。Security Assertion Markup Language（SAML）2.0 および OAuth 2.0 を使用するアイデンティティ 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 Spark 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。

ユーザは次の項目を選択できます。

- **デバイスのアクセス許可**：ユーザが Spark を実行しているモバイル プラットフォームまたはブラウザ プラットフォームに応じて、Spark 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、写真、プッシュ通知など、さまざまなデバイス許可を要求します。ほとんどのプラットフォームでは、これらの機能にはユーザがいつでも取り消すことができる明示的な許可が必要になります。
- **プロキシミティ機能**：モバイル デバイスでは、Spark クライアントがアクティブな場合には超音波信号がリッスンされるため、Spark 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。この場合はデバイスのマイクが使用されるため、ユーザはマイクをオフにすることで、このペアリング機能を無効にすることができます。
- **プロフィール写真**：Spark を使用する場合、プロフィール写真は必須ではありません。
- **外部参加者インジケータ**：Cisco Spark クライアントでは、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**：ユーザは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、ルームを管理できます。

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され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。また Spark クライアント内でリアルタイムな意思決定ができるように、簡単な情報開示を行っています。詳細については、定期的に更新されているシスコのサポート ページを参照してください。シスコがどのような情報を収集して、どのように使用し、保護しているかの詳細は、シスコ オンライン プライバシー ステートメントと、Spark のプライバシーに関する補足事項で示しています。

プラットフォームとサービスのセキュリティ

シスコの Secure Development Lifecycle に加えて、Cisco Spark では、Spark プラットフォームおよびサービスについて、内部/外部のホワイトボックス/ブラックボックス侵入テストを頻繁に実施しています。Cisco Secure Development Lifecycle の詳細については、https://www.cisco.com/c/en/us/about/security-center/security-programs/secure-development-lifecycle.html [英語] を参照してください。

インシデント管理と企業のセキュリティ ポリシー

Cisco Product Security Incident Response

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受け取り、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 時間体制で、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。

セキュリティ脆弱性の疑いに関するレポートおよびサポート

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 には次の方法でご連絡ください。

	緊急サポート
電話	+1 877 228 7302（北米ではフリーダイヤル）、+1 408 525 6532（国際ダイヤル通話）
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	電子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] を参照してください。

顧客データの透明性および警察による要求

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、http://www.cisco.com/web/about/doing_business/trust-center/transparency-report.html [英語] を参照してください。

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