Cisco Webex の ゼロトラストセキュリティ

エンドツーエンドで暗号化された機密性の高い会議の業界標準を打ち立てる

© 2020 Cisco and/or its affiliates. All rights reserved.

目次

12 年にわたって E2E セキュリティを提供してきた実績 3

エンドツーエンドのユーザエクスペリエンス 4

標準規格に準拠した暗号化 6

概要 12

今後の方向性 13

まとめ 14

© 2020 Cisco and/or its affiliates. All rights reserved.

世界中の何百万人もの人々が、会議に Webex を使用しています。Cisco Webex は、多くの大企業、政府や自治体のお客様から信頼を得ているオンライン会議プラットフォームです。Webex を使用して、学校でのオンライン授業から、患者の診察、議会や投票まで、毎日あらゆることが行われています。

世界中のさまざまな場所にチームが分散しているのに加え、対面での接触がますます制限されているため、リモート作業の需要が急増しています。それに伴い、コラボレーションツールを使用して機密性の高い会議を行うことの必要性も高まっています。Webex は、他のどのコラボレーションベンダーよりも長い時間をかけて、このニーズに応えてきました。

Webex には、ミーティングについてはオプションで強力なエンドツーエンド（E2E）暗号化を、メッセージングについては常時オンのエンドツーエンド暗号化をサポートしてきた長い歴史があります。ゼロトラストセキュリティは、次の 3 つの重要な点で同じ流れを踏襲しています。

1. 標準規格に準拠し、正式に検証された暗号化基盤の確立
2. エンドツーエンドでアイデンティティを検証することによる、エンドツーエンド暗号化の確立
3. 現在の Webex® デバイスと Webex アプリケーションに対するサポートの拡張

このホワイトペーパーでは、エンドツーエンドのセキュリティの背景と、ゼロトラストセキュリティの仕組みに関する技術的基盤について説明します。

12 年にわたって E2E セキュリティを提供してきた実績

Webex は長年にわたって E2E 暗号化をサポートしてきました。Webex Meetings に初めてエンドツーエンドの暗号化が実装されたのは、12 年以上もさかのぼる 2008 年のことです。2015 年に登場した Webex Teams™（当時の名称は Cisco Spark）では、リリース当初からすべての会話が E2E で暗号化されてきました。

「エンドツーエンド（E2E ）」のセキュリティは、ユーザがコンテンツを送信してから相手がそれを受信して表示するまでの全体を通して、コンテンツを保護します。中間者がコンテンツを傍受したり改ざんしたりすることはできません。参加者以外のユーザはおろか、クラウド会議サービスのプロバイダーでさえも会議を傍聴することは不可能です。つまり Webex は会議の内容を確認できずに会議サービスを提供する必要があり、これには技術的な課題も伴います。

© 2020 Cisco and/or its affiliates. All rights reserved.

	ネットワーク攻撃者	パッシブな攻撃（盗聴）	アクティブな攻撃（偽装）	
転送中/保管中の暗号化	✔	✘	✘	非 E2EE アプリケーション
E2E 暗号化	✔	✔	✘	レガシー E2EE、コンシューマ アプリケーション
E2E 暗号化 + アイデンティティ	✔	✔	✔	Webex のゼロトラストセキュリティ

図 1.
E2E セキュリティのレベル

図 1 に示すように、ビデオ会議プロバイダーが E2E 暗号化メカニズムにどれだけ投資しているかによって、利用できる保護レベルが異なります。E2E セキュリティは、転送中および保管中だけ暗号化する方式よりも優れています。E2E セキュリティを実装済みだと主張する大半のサービスでは、パッシブな攻撃からのみ保護されます。パッシブな攻撃からの保護のみであっても、会議の録音や録画を盗聴されることは防げるため、意味がないわけではありません。しかし理想は、パッシブな攻撃とアクティブな攻撃の両方から保護することです。アクティブな攻撃では、会議プロバイダー自体が正規の参加者になりすまし、会議に参加できてしまう可能性があります。アクティブな攻撃を防ぐには、E2E 暗号化に加えて、E2E **アイデンティティ**レイヤも必要になります。

そこで Webex はゼロトラストセキュリティを採用することで、会議を新しい強力な暗号化方式で保護します。エンドツーエンドでアイデンティティを検証することで E2E 暗号化を確立させるため、あらゆる種類の攻撃から会議を保護します。

エンドツーエンドのユーザエクスペリエンス

技術的な詳細をご説明する前に、エンドツーエンドで保護された会議に参加する際の画面について説明します。ここでは Webex デバイスの画面を使って説明しますが、Webex アプリの操作方法もこれと同様です。E2E 暗号化会議を作成するには、会議のスケジュール担当者が適切な会議タイプを選択します（図 2）。

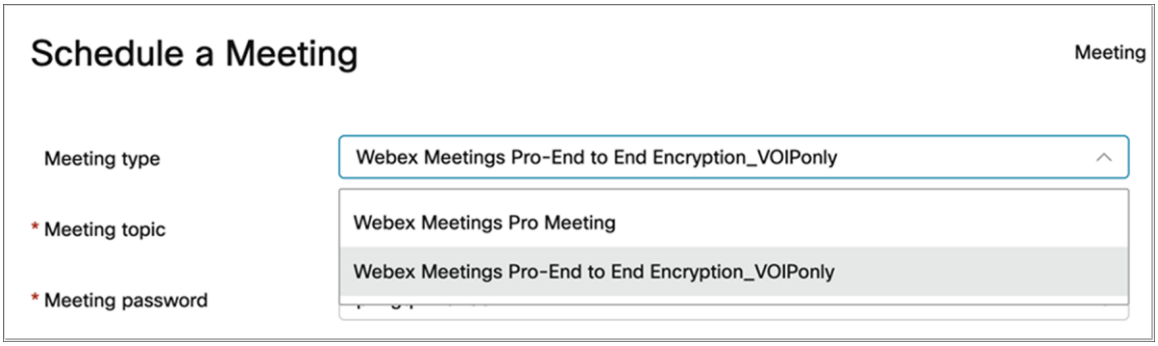

図 2.
E2E 暗号化会議のスケジューリング

© 2020 Cisco and/or its affiliates. All rights reserved.

参加者が会議に参加すると、E2E 暗号化会議に参加していることを示す「ロック付きのシールド」アイコンが表示されます。このアイコンをタップすると、会議がどのように保護されているかについての詳細情報を確認できます（図 3）。

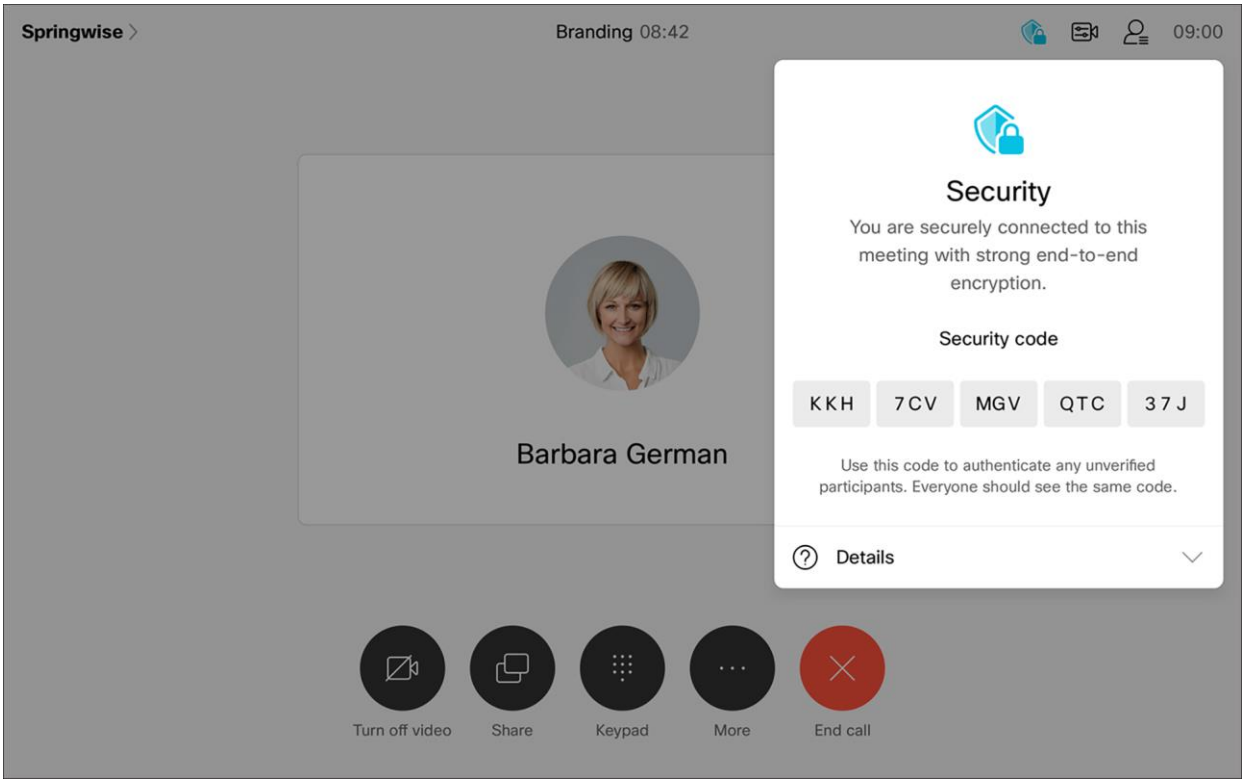

図 3.
E2E 暗号化会議内のセキュリティ情報

© 2020 Cisco and/or its affiliates. All rights reserved.

最後に、Webex アプリケーションの会議参加者リストに、E2E で保護された方法で参加者のアイデンティティが検証されているかどうか（シスコ以外の誰かが参加者のアイデンティティを検証済みかどうか）が示されます（図 4）。また参加者は、全員が同じセキュリティコードを持っていることを確認することで、参加者全員が会議の様子が同じであることを確認し、なりすまし攻撃から安全であることを確認できます。

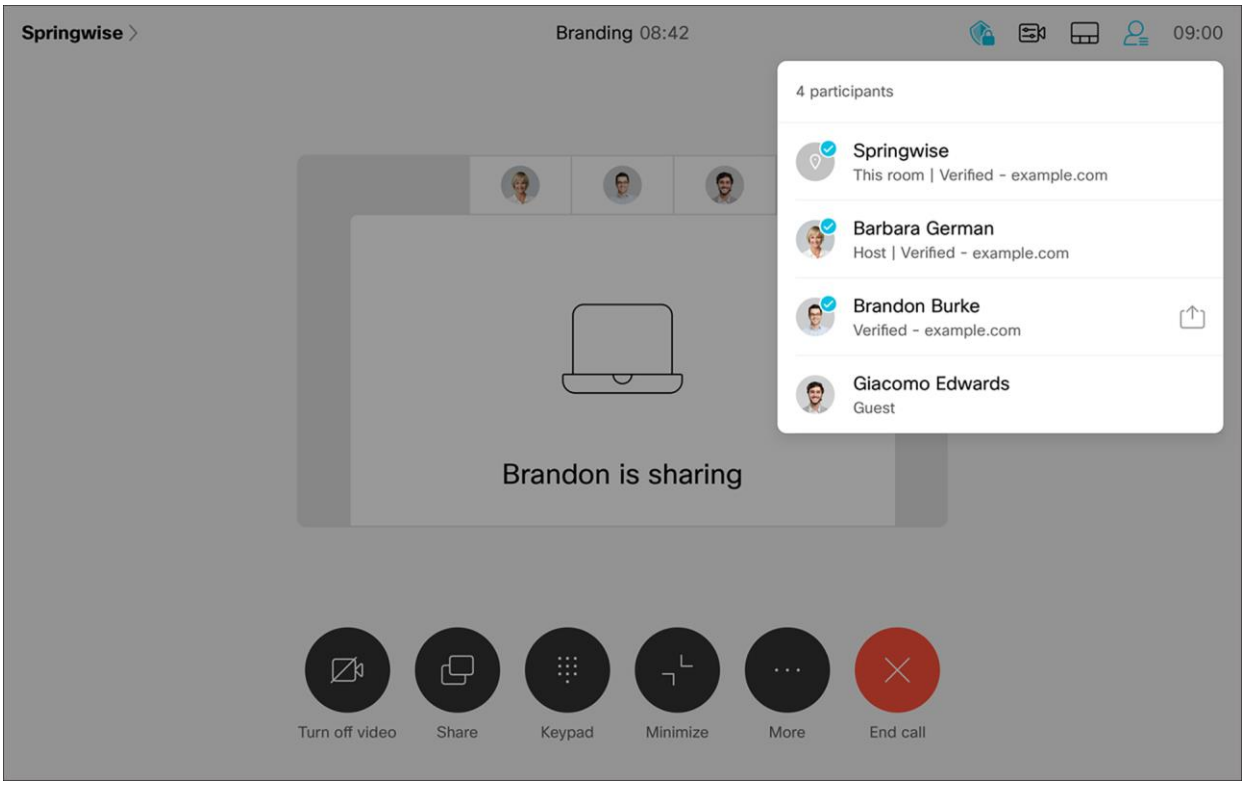

図 4.
エンドツーエンドでのアイデンティティの検証

標準規格に準拠した暗号化

ゼロトラストセキュリティは、業界標準の暗号化プロトコルに基づいて構築されています。シスコは、Google、Cloudflare、Wickr、Wire など、セキュリティおよびプライバシーの分野をリードする他の企業と協力して、ゼロトラストセキュリティを推進しています。シスコは、Secure Real-Time Protocol（SRTP）、DTLS-SRTP、STIR/SHAKEN、WebRTC などのテクノロジーを使用して、第 1 世代のセキュアな Voice over IP（VoIP）を主導しましたが、現在ゼロトラストセキュリティでも同じことを行っています（図 5）。

© 2020 Cisco and/or its affiliates. All rights reserved.

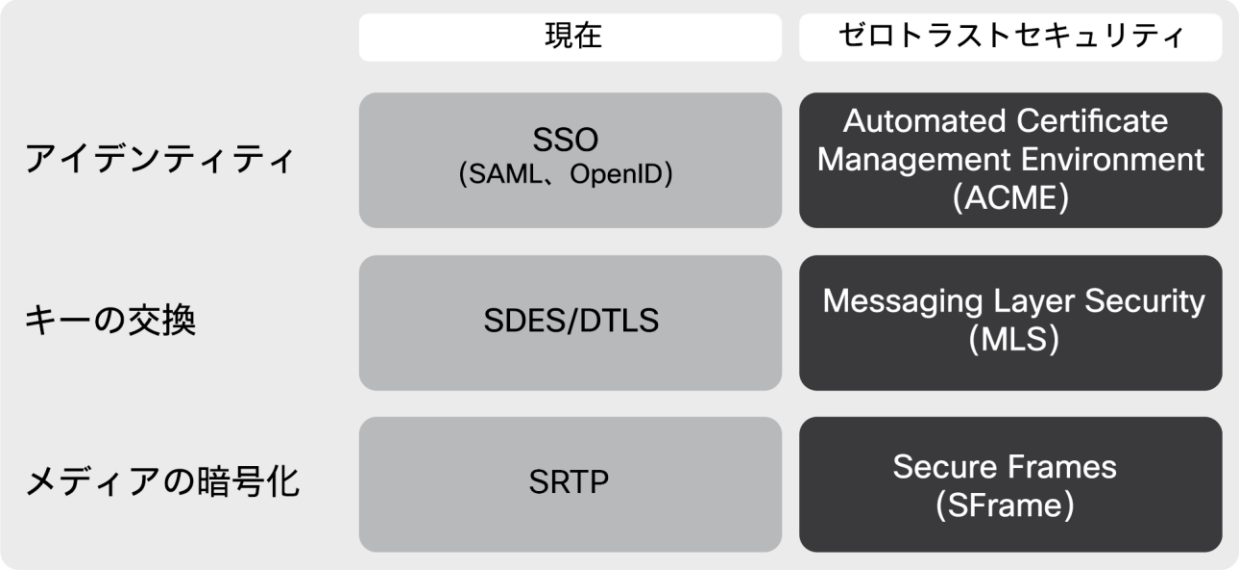

図 5.
ゼロトラストセキュリティの標準規格

このシステムには大別して 3 種類のレイヤがあります。各レイヤでは、古いホップバイホップ テクノロジーを採用した上で、それにエンドツーエンドの保護レイヤを追加して強化しています。3 つのレイヤの概要は次のとおりです。

- **アイデンティティ。**E2E のアイデンティティでは、アイデンティティを証明するクレデンシャルをクライアント自身が持つ必要があります。現在使用されている Web 証明書の半分以上は、Automated Certificate Management Environment（ACME）プロトコルを使用して発行されています。Webex はエンタープライズ アイデンティティ システムを活用するための拡張機能と ACME を併用することで、堅牢なアイデンティティ検証にシームレスなユーザエクスペリエンスを実現しています。
- **キーの交換。**E2E 暗号化用のキーは、E2E 会議に参加しているクライアントが設定します。これにより、会議プロバイダーがキーにアクセスすることを防ぎます。キーは正式に検証された堅牢な環境で保護されます。そこで使用されるのが、オープンソースコミュニティで開発された技術から発展した、新たな標準規格である Messaging Layer Security（MLS）プロトコルです。
- **コンテンツの保護。**最後に、会議の実際のメディアコンテンツにはエンドツーエンドの保護が必要です。SFrame（Secure Frames）は、リアルタイムでメディアを暗号化するための高速でシンプルな暗号化フレームワークです。最小限のオーバーヘッドで暗号化レイヤを追加できるのが特徴です。

これらのテクノロジーについて、下から順番にもう少し詳しく見ていきましょう。

© 2020 Cisco and/or its affiliates. All rights reserved.

軽量なメディアの暗号化

メディア暗号化方式は、会議の参加者が共有するキーを取得し、そのキーを使用して、音声、ビデオ、画面共有など、会議で共有される実際のコンテンツを保護する方法です。プロトコルレベルでは、メディア暗号化方式は、暗号化されたデータの各ユニットを使用して、いくつかの追加情報を送信する必要があります。最も重要なのは、（1）受信者にパケットの復号方法を指示するヘッダーと、（2）パケットが改ざんされていないことを受信者が確認するために使用する認証タグです。たとえば、SRTP の暗号化ユニットは RTP パケットですが、SRTP は RTP ヘッダーをセットアップに使用し、パケットの最後に認証タグを付加します。

これらすべての追加情報により、E2E 暗号化会議に必要な帯域幅が増加するため、SFrame は必要最小限のフレーミングを提供します。SFrame ヘッダーは、使用するキーを示し（これによりキーのローテーションが可能になります）、初期化ベクトルを定義する一意のシーケンス番号を提供します。この後に、E2E キーで暗号化されたコンテンツと認証タグが続きます。SFrame ヘッダー、コンテンツ、タグはその後 SRTP パケットにラップされます。これにより、SRTP はネットワーク攻撃者によってインスペクションや変更が行われないようこれらを保護し、SFrame は会議プロバイダーのメディア要素から保護します（図 6 の例を参照）。

図 6.
SFrame によるメディア暗号化

この必要最小限のアプローチには、他にもいくつかの利点があります。SFrame は基盤となるトランスポートに依存しないため、RTP over QUIC や RIPT などの新しいテクノロジーとの上位互換性があります。マルチパケットユニット（フレーム全体など）で動作するように SFrame を設定して、暗号化のオーバーヘッドをさらに削減することもできます。

© 2020 Cisco and/or its affiliates. All rights reserved.

グループキーの交換

グループが信頼できないチャネルにしかアクセスできない場合に、グループ間で秘密キーを設定するということについて、不思議に思われるかもしれません。実のところ、これを実現する技術は 1980 年代に初めて開発されました。今や Web ブラウジングの 90% 以上で使われている Transport Security Layer（TLS）が、まさにそれに該当します。Messaging Layer Security（MLS）は、この機能をグループに拡張したものです（TLS はポイントツーポイントでのみ機能します）。そのため、会議プロバイダーが信頼できない場合でも、この機能を使用して会議キーを設定できるのです。

MLS には、重要なセキュリティ機能がいくつかあります。それは次のとおりです。

- グループの認証されたメンバーだけが知っている共有キーを確立する
- グループのすべてのメンバーが、誰がグループの中にいるのかを一貫して把握する
- メンバーがグループに参加またはグループから退出するときに共有キーをローテーションする

1 つ目の機能は、SFrame でメディアを暗号化するために使用するキーを提供します。また、2 つ目の機能にとって、E2E アイデンティティの出発点となります。3 つ目の機能により、現在会議に参加しているメンバーだけがメディアを復号できるようになります。参加前または退出後（または強制退出された後）は、メディアを復号できません。

これらすべてを実現するために、会議のクライアントは、会議の重要な時点で MLS メッセージを交換し、各時点での会議の参加者を正確に含む MLS グループを維持します。Webex はクライアント間でメッセージをルーティングしますが、MLS によりこれらのメッセージが保護されるため、Webex は安全に処理できます。図 7 に、メッセージの流れを示します。

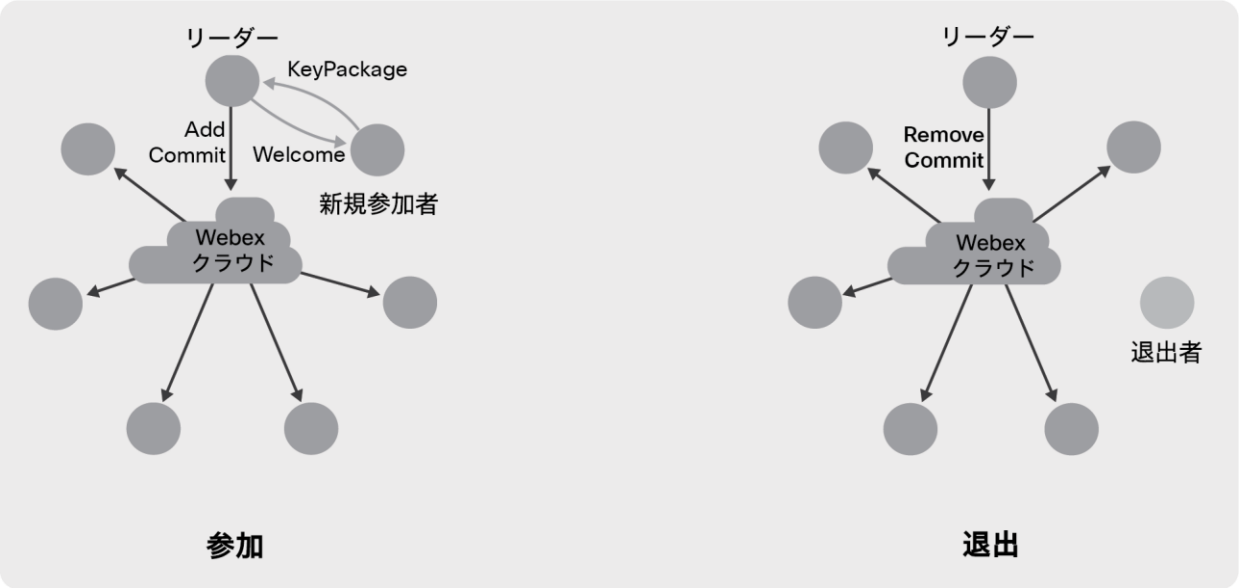

図 7.
MLS によるグループキーの管理

© 2020 Cisco and/or its affiliates. All rights reserved.

- **作成：**会議に最初に参加した人（主催者かどうかを問わず）が会議の MLS グループを作成し、MLS の目的上の「リーダー」になります。任意の時点で、会議の参加者の 1 人がリーダーに指名されます。ほとんどの場合、会議の主催者がリーダーとなります。セッションが始まると、MLS はすべての会議参加者にリーダーとして機能するための暗号化情報を付与しますが、Webex は混乱を避けるために 1 人をリーダーに指名します。
- **参加：**新しい参加者が会議に参加する場合は、MLS KeyPackage メッセージ（公開キーと認証情報が含まれる）をリーダーに送信し、参加を要請します。リーダーはそれに対して Welcome メッセージで応答し、メッセージ内で会議の他の参加者についての情報を共有します。また、リーダーは Add メッセージと Commit メッセージをグループにブロードキャストします。Add メッセージは、会議にすでに参加している参加者に、新規参加者について通知します。Commit メッセージにより、現在の参加者全員が古いグループキーをハッシュして、拡張されたグループの新しいキーを取得します。Welcome メッセージにより、このキーが新規参加者に提供されます。
- **退出：**誰かが会議から退出した場合、リーダーがその退出者をロックアウトします。リーダーはこれを行うために、会議に残っている参加者全員に MLS の Remove および Commit メッセージをブロードキャストします。Remove メッセージは、残った参加者に、誰が退出したのかについて通知します。一方、Commit メッセージは、残ったすべての参加者（退出者以外）用に新しいキーを暗号化します。残った参加者は、古いグループキーで新しいキーをハッシュし、退出者が持っていないキーを取得します。退出者がリーダーの場合は、Webex は新しいリーダーを指名し、新しいリーダーは古いリーダーを削除します。

参加と退出の両方で、MLS がグループの新しいキーを生成することに注意してください。参加または退出が行われるたびに、会議の参加者のキーは、数秒以内に新しいキーに更新されます。MLS は、1 回の Commit で複数の Add および Remove トランザクションを適切に処理することもできます。これにより、会議の開始時や終了時など、不要でコストのかかるキーローテーションが立て続けに発生するのを回避できます。各ローテーションの後に、会議の参加者は古いキーのコピーを削除するため、いずれかのキーが侵害されても、古い会議のコンテンツは保護されます。会議の最後に、参加者は残りのキーをすべて削除します。これにより、E2E 会議のコンテンツがどこかに保存されていても、復号できなくなります。

キーローテーションを行うことで、会議への参加または強制退出に数秒余分にかかる場合がありますが、会議の参加者リストに表示されていない参加者はコンテンツを復号するキーを持てなくなるため、明快なセキュリティアシュアランスを実現できます。

エンドツーエンドで検証されたアイデンティティ

エンドツーエンドでアイデンティティを検証するには、シスコが改ざんできないように、シスコの外部にアンカーリングされたクレデンシャルが必要です。シスコは、追加のメカニズムの導入を希望されるお客様にはこのレベルのアシュアランスを提供できますが、あらゆるユーザと会議に適用できるようにレベルを下げたアシュアランスメカニズムも提供しています。

MLS は、会議の参加者を認証するために標準の X.509 証明書を使用します。証明書は、特定の署名キーの所有者が指定されたアイデンティティを持っているという、信頼できる「認証局」によって署名されたステートメントです。会議の各参加者は、次のいずれかの方法で証明書を取得します。

- **SSO に対応した組織のクライアントの場合：**ユーザが SSO を使用して Webex にログインすると、クライアントは ACME のための拡張機能とともに SSO ログインを使用し、信頼できる認証局に対してユーザのアイデンティティを証明します。認証局は、その証明に基づいて証明書を発行します。ACME はプロセス全体を自動化するため、ユーザの操作なしで、プロセス全体をバックグラウンドで実行できます。このフローを通過するクライアントは、自身の証明書を使用して電子メールアドレスを他のクライアントに対して証明します。
- **組織の管理者によって E2E 用に設定されたデバイスの場合：**シスコはすでに、Webex デバイスにドメイン名を提供するツールを管理者に提供しています。E2E アイデンティティをサポートするために、Webex はこ

© 2020 Cisco and/or its affiliates. All rights reserved.

のツールを拡張し、ドメイン名の標準 ACME プロセスを使用してデバイスの証明書を自動的に取得できるようにしています。デバイスはこの証明書を使用して、会議の他の参加者に対して、ドメイン名を正しく表していることを証明します。

- **それ以外の場合（ゲスト、非 SSO ユーザ、プロビジョニングされていないデバイス）**：デフォルトでは、Webex クライアントまたは Webex デバイスは Webex 認証局から証明書を取得します。この証明書には、シスコが検証したアイデンティティが、他のクライアントに提示できる形で反映されます。

E2E 暗号化会議の参加者リストには、各ユーザの認証ステータスが表示されます。上記の最初の 2 つのオプションは、シスコが改ざんできないという点では、真の意味で E2E で検証されたアイデンティティを提供します。この 2 つのケースでは、参加者リストには参加者が属するドメインが表示されます。たとえば図 8 に示す会議では、Barbara と Brandon が example.com の検証済み電子メールアドレスを持ち、Springwise ルームシステムが example.com の検証済みドメイン名を持っていることがわかります。Webex から取得した証明書は、より限定的な保護を提供します。この場合、Webex 認証局に侵入できた攻撃者がユーザに偽装できます。これはアイデンティティ保護をまったく行わないよりは安全ですが、同じ証明書を使用している会議の参加者は検証済みとしてマークされません。

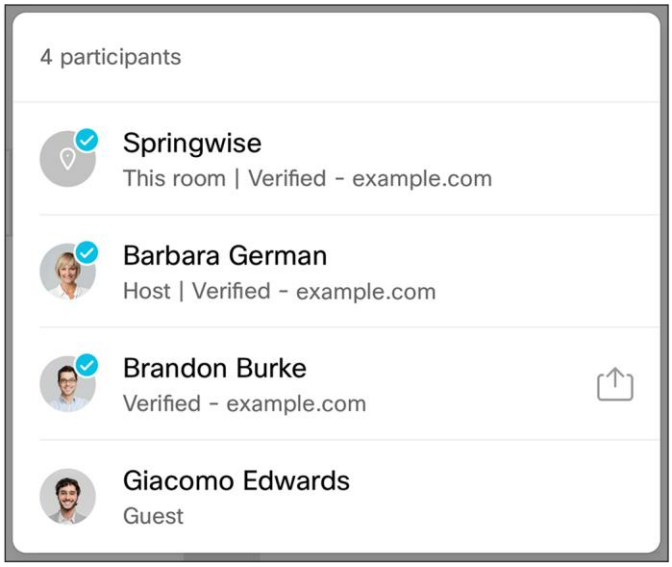

図 8.
参加者リストに表示された検証済みアイデンティティ

© 2020 Cisco and/or its affiliates. All rights reserved.

これらの手順を補強するために、Webex は会議の「セキュリティコード」も提供しています。セキュリティコードは、MLS プロセスの出力として計算される、人間が判読できる短い文字列で、会議の暗号化状態（グループのキーや参加者から提示された証明書など）が要約されたものです。このコードは、偽装攻撃を検出するために使用できます。これは、偽装攻撃を受けた場合、少なくとも 1 人の参加者が他の参加者と異なる暗号化状態を持つことになるためです。ただし、偽装を排除できるのは、全員が同じコードを持っていることを全員が確認した場合のみです。参加者が互いに同じコードを持っていることを確認した場合、各参加者は自分のアイデンティティが相互に正しく表示されることを知っていますが、そのコードを確認しない参加者は、偽装している可能性があると考えられます。図 9 は、会議でのセキュリティコードの表示例を示しています。

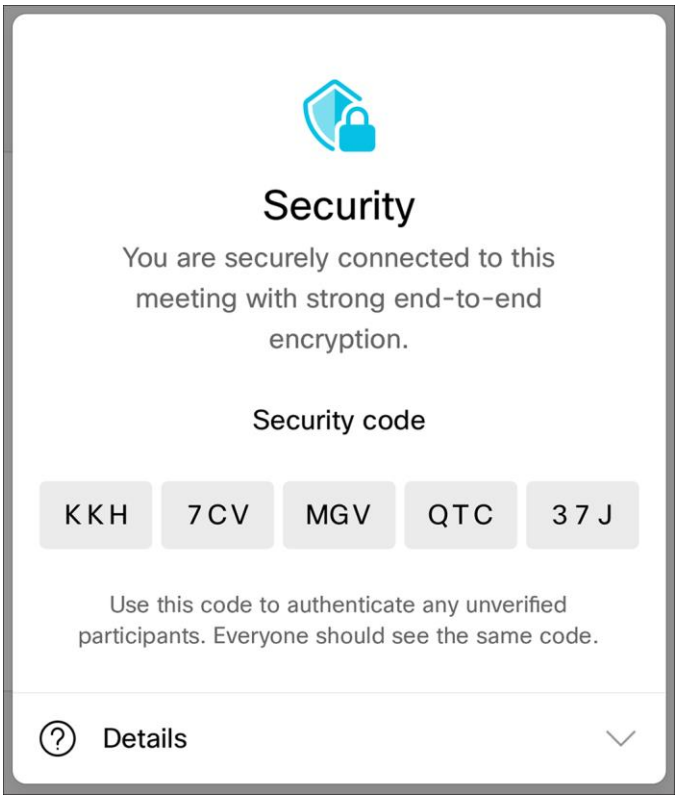

図 9.
偽装から保護するためのセキュリティコード

セキュリティコードは、偽装攻撃に対して非常に強力な防御を提供します。このコードは MLS プロトコルの一部であるため、堅牢なセキュリティ分析が行われています。セキュリティコードは会議の状態に密接に関連付けられているため、誰かが会議に参加するたびにセキュリティコードが変更されます。そのため、会議の参加者は、誰かが参加するたびにセキュリティコードを再確認する必要があります（退出が偽装攻撃のきっかけになることはないため、誰かが退出してもコードはローテーションされません）。

概要

ゼロトラストセキュリティは 2021 年第 1 四半期にリリースされる予定で、Webex 会議の E2E セキュリティが次の点で大幅に改善されます。

- 標準規格に準拠し、正式に検証された暗号化
- E2E で検証されたアイデンティティ
- 本機能のリリースとともに販売されるすべての Webex デバイスをサポート

© 2020 Cisco and/or its affiliates. All rights reserved.

- パーソナル ミーティング ルームでの E2E 暗号化をサポート

現在の機能と同様に、ゼロトラストセキュリティにはいくつか制約があります。E2E 暗号化会議は、以下をサポートしていません。

- Webex Web アプリケーション
- SX、DX、MX シリーズなどの古い Webex デバイス
- シスコクラウドサービスによって提供される、プレーンテキストメディアへのアクセスを必要とする以下の機能
  - ネットワークベースの録画（NBR）
  - セッションデータ、トランスクリプト、議事録のなどの保存
  - リモートコンピュータの共有
  - PSTN または SIP の相互運用性

今後の方向性

シスコは今後、クラウドの権限を必要最小限に留め、かつお客様がデータを制御できるようにするという原則に基づき、E2E で暗号化された会議をいくつかの面で改善していく予定です。

お客様が承認したサービスの統合：E2E 暗号化会議で現在無効になっている機能のほとんどは、シスコが運用するサーバ上の処理メディアによって提供されていることが原因で無効になっています。E2E 暗号化会議からシスコが除外されると、これらのサーバから会議機能を提供できなくなるためです。ただし、一部のお客様がセキュリティと機能のトレードオフを別の形で求めていることも認識しています。そこでシスコは、そうしたニーズにもバランス良く応えられるよう、特定サービスを会議「ツール」として統合できるツールを開発しています。シスコのオープンで標準規格に準拠したアプローチの利点の 1 つは、パートナーや他のベンダーが Webex の E2E 暗号化を簡単に統合できることです。これにより、お客様はシスコが提供するサービスに加えて、サードパーティのサービスも導入可能になります。

このような柔軟性が E2E 暗号化会議のセキュリティを損なうことがないようにするために、どのようなコンテキストでどのようなサービスが許可されているかを定義するための堅牢なポリシーフレームワークをお客様に提供します。たとえば、企業の IT 管理者は、一切のサービスが許可されず、機能が制限される「高セキュリティ」会議と、少数の承認済みサービスの追加が許可される「中セキュリティ」会議を定義することができます。

© 2020 Cisco and/or its affiliates. All rights reserved.

分散型アイデンティティ：現在の SSO ベースの戦略により、SSO に対応したすべてのユーザに E2E で検証されたアイデンティティを広範囲で提供できます。しかし最終的には、お客様が独自の E2E 認証局を使用できるようにしたいと考えております。これにより、会議の参加者の認証に関与する要素が減り、お客様が実際に会議のセキュリティを制御できるため、全員のセキュリティが向上します。言い換えると、シスコは**分散型**のアイデンティティ エコシステムの実現を目標としています。分散型システムでは、標準規格に準拠することが何より重要です。分散化を完全なものにするには、追加の標準規格がいくつか必要になりますが、現在シスコが導入しているテクノロジーは、E2E アイデンティティ機関と、証明書を必要とするクライアントとの間の相互運用性の基盤となるものです。

ユビキタスな E2E セキュリティ：一部の会議だけでなく、あらゆるものを E2E で保護する必要があります。このビジョンを達成するための最初のステップは、Webex 会議に参加できるすべてのエンドポイントで E2E セキュリティを実現することです。その最初の候補となるのは、Webex Web アプリケーションとクラウドに接続されたシスコの電話機ですが、最終的にはシスコのオープンで標準規格に準拠した E2E アーキテクチャにより、Session Initiation Protocol（SIP）インフラストラクチャにも導入できるようになる見込みです。

このホワイトペーパーで説明したイノベーションは、常時オンの E2E 暗号化の長期的なビジョンへの明確な道筋を示しています。ユーザがどこからでも接続でき、組織が会議で必要な機能を安全にオプトインできるようになると、すべての機能をオンにした非公式のアドホック会議から、セキュリティが高く完全に保護された会議まで、すべての Webex 会議で E2E 暗号化を使用できるようになります。E2E 暗号化により、会議のコンテンツは承認された参加者のみが利用できるよう保護されます。また、会議ごとに適切な参加者を設定できる利点も生まれます。

まとめ

機密性の高いビデオ会議への需要は今も増加しています。そこで Webex は、標準規格に準拠した暗号化、エンドツーエンドで検証されたアイデンティティ、Webex アプリケーションと Webex デバイスの両方から使用できる柔軟性を特長として、エンドツーエンドで保護された会議における業界標準を目指します。オープンで標準規格に準拠したアプローチにより、パートナーのエコシステムと連携しながらエンドツーエンドの保護を拡張することで、より幅広い顧客ニーズに対応できる見込みです。

©2021 Cisco Systems, Inc. All rights reserved.
Cisco、Cisco Systems、および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。
本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。
「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(1502R)
この資料の記載内容は 2021 年 3 月現在のものです。
この資料に記載された仕様は予告なく変更する場合があります。

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

C11-744553-00JA 21.03