Zoom暗号化

はじめに

本ドキュメントの目的は、Zoomプラットフォームに使用される暗号化手段に関する情報を提供することです。当社の暗号化設計における目標は、お客様のさまざまなニーズに対応しながら、可能な限りプライバシーを保護することです。

いくつかの異なるユースケースと、個人ユーザーがZoomに接続できる方法があります。次のドキュメントは、プラットフォームへの潜在的なインターフェースによって使用される暗号化方法を概説しています。

Zoomクライアント使用時

Zoomは、Mac、Windows、iOS、Android、Linux向けの機能豊富なクライアントソフトウェアパッケージを提供します。このパッケージは、さまざまな暗号化テクノロジーを利用してユーザーのプライバシーとセキュリティを支援します。**クライアントからZoomクラウドに送信されるすべての顧客データは、次のいずれかの方法を使用して転送中に暗号化されます。**

TLS 1.2

ZoomクライアントとZoomのクラウド間の接続では、HTTPSが推奨される通信方法です。これらの接続は、TLS 1.2暗号化と、信頼できる商用認証局が発行するPKI証明書を利用します。一般的な使用例には、クライアントへのサインイン、ミーティングのスケジュール作成、チャット、投票、ファイルの共有、ミーティング中の質疑応答などがあります。TLS 1.2は、リアルタイムコンテンツへの対応など、他の通信ストリームのバックアッププロトコルとしても機能します。

高度暗号化標準

ユーザーデータグラムプロトコル（UDP）を介してデータが送信されるリアルタイムコンテンツ（ビデオ、音声、コンテンツ共有）に対応するようなユースケースでは、ECBモードでAES-256を使用してこれらの圧縮データストリームを暗号化します。当社はこれをすぐにAES-256 GCMにアップグレードする予定です。さらに、高度暗号化標準で暗号化されたビデオ、音声、およびコンテンツ共有の場合、いったん暗号化されると、別のZoomクライアントまたはZoomコネクタに到達するまでZoomのミーティングサーバーを通過する間、暗号化されたままになり、データを別のプロトコルに変換できます。

SRTP

Zoom電話機製品は、AES-128-ECBを利用したセキュア リアルタイム転送プロトコルを使用して、データセンターとの間で送受信される通話を暗号化、保護します。この機能はまもなくAES-256 GCMにアップグレードされます。

Webブラウザ使用時

Zoomでは、完全な管理コンソール、クラウドレコーディングへのアクセス、APIエンドポイントの広範なセット、ミーティング用のWebベースのクライアントなど、多くの豊富な機能を提供するWebインターフェイスを提供しています。**WebブラウザからZoomクラウドに送信されるすべての顧客データ（当社のWebサイトやWebミーティングクライアントを含む）は、転送中に次のいずれかの方法で暗号化されます。**

TLS 1.2

Zoom Webサイトへの接続は、TLS 1.2暗号化と、信頼できる商用認証局が発行するPKI証明書を利用します。このポータルを通じて、個人はZoomアカウントに関連付けられたさまざまな機能にアクセスし、その操作を管理し、他のシステムと統合できます。暗号化の強度とWebサイトへの接続に使用される特定の暗号は、サイトへのアクセスに使用されるブラウザと、ネゴシエーションされた一般的な暗号化方式の結果によって異なります。

AES-256

TLS暗号化に加えて、ZoomのWebサイトでは、特定のユースケースで追加の暗号化処理を施しています。たとえば、クラウド録画、チャット履歴、ミーティングのメタデータなどの顧客データは、AES-256 GCMを使用して保管され、キーはクラウドのキー管理システム（KMS）によって管理されます。ユーザーがWebアセンブリを利用してZoom Webクライアントを使用してミーティングに接続すると、Zoomは、Webアセンブリを活用し、AES-256 ECBで暗号化されるミーティング用サーバーから直接、ユーザー データグラム プロトコル（UDP）を介して、リアルタイムでコンテンツ（ビデオ、音声、コンテンツ共有）を送受信します。

サードパーティ製のデバイス/サービスを使用する場合

オープンプラットフォームとして、Zoomはさまざまなサービスとデバイスがシステムに接続できます。こうしたものには、ZoomミーティングへのH323/SIPデバイスの接続、一般的なストリーミングサービスでのブロードキャスト、標準の電話回線を使用したミーティングへの呼び出し（非アプリ経由）などの使用例のサポートが含まれます。この統合では、特定のサードパーティ製デバイスまたはサーバー固有の通信プロトコルを利用する必要があるため、暗号化方法は、そのデバイスで可能なものに限定されます。**したがって、当社はサードパーティ製のデバイスやサービスで暗号化を使用することを推奨しますが、これらのデバイスやサービスを介して送信される顧客データは、Zoomのシステムとの間の転送中に暗号化されない場合があります。ですが、そのデータがZoomのシステムに到達すると、その時点で暗号化され、システムを通過する間は暗号化されたままになります。**サードパーティ製のデバイスが暗号化をサポートしている場合、次の方法のいずれかを使用して暗号化される可能性があります。

TLS 1.2

デバイスがサポートしている場合、ZoomはTLS 1.2上でネゴシエーションを実行します。例えば、SIPデバイスが暗号化対応であれば、TLSがシグナリングに使用されます。

高度暗号化標準

デバイスがサポートしている場合、ZoomはSIPまたはH323エンドポイント上の高度暗号化標準を使用してビデオ、音声、画面共有などのミーティングコンテンツの暗号化をネゴシエーションします。

結論

複数のメディアや通信プラットフォームでコラボレーションが行われる今日の世界で、Zoomはお客様のセキュリティの保護に取り組んでいます。サードパーティ製のデバイスには、暗号化をZoomプラットフォーム外部の広範な統合に拡張する機能が提供されます。Zoomのプラットフォーム内では、お客様のコンテンツが確実に暗号化されます。