



2020年4月6日

お客様各位

ZVC Japan 株式会社

エンドツーエンドの暗号化に関するコメントについて

平素は格別なるご高配を賜り、誠にありがとうございます。

表題の件につきまして、Zoom ブログ上に「The Facts Around Zoom and Encryption for Meetings/Webinars」の件名で説明を掲載しておりますが、以下に日本語でご説明申し上げます。原文は弊社正式ブログ (<https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/>) にてご確認いただけます。

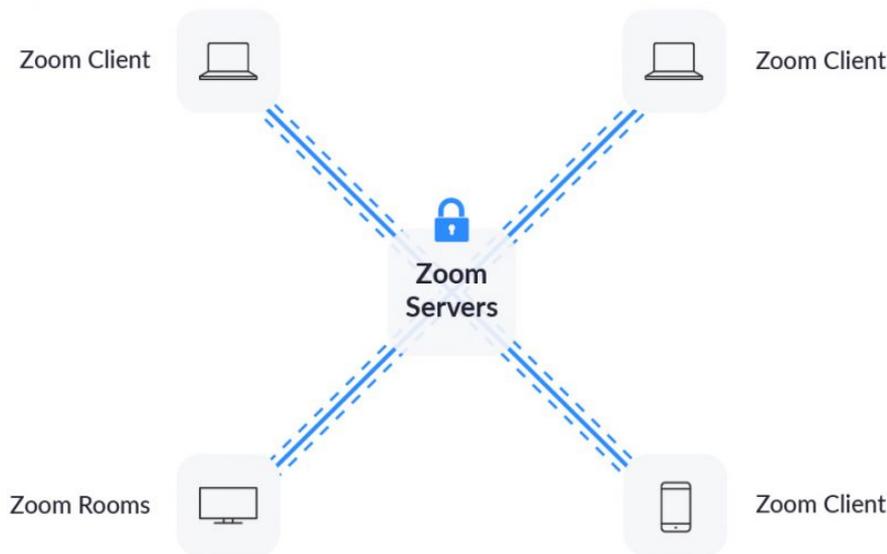
まず始めに、弊社の暗号化の実装に対しての議論の中で、Zoom の会議はエンドツーエンドで暗号化されているという表現により、混乱を引き起こしたことをお詫びします。Zoom は、可能な限り多くのシナリオでコンテンツを保護するために暗号化を使用するよう常に努力しており、その精神に基づき、「エンドツーエンド暗号化」という言葉を使用しています。お客様を欺くことを意図したものではありませんが、一般的に受け入れられているエンドツーエンド暗号化の定義と、私たちがどのように使用していたかに矛盾があることを認識しています。このブログは、この矛盾を是正し、当社のネットワーク上を流れるコンテンツをどのように暗号化するかを正確に明らかにすることを目的としています。

当社の暗号化設計の目標は、クライアントベースの多様なニーズに対応しつつ、可能な限り最大限のプライバシーを提供することです。

参加者全員が Zoom クライアントを使用しており、会議が録画されていない会議では、すべてのビデオ、オーディオ、画面共有、およびチャットのコンテンツを送信側のクライアントで暗号化し、受信側のクライアントに到達する前のいかなる時点でも復号化しません。

Zoom クライアントには以下のものが含まれます。

Zoom アプリを実行しているラップトップまたはコンピュータ
Zoom アプリを使用したスマートフォン
ズームルーム



すべての参加者が Zoom アプリを使用しているこのシナリオでは、送信プロセスの間、いかなる時点でも Zoom のサーバーや従業員にユーザーコンテンツが利用可能になることはありません。

Zoom は、ユーザーに可能な限り多くの接続方法を提供するために、通信チャネルの多様なエコシステムをサポートしています。ユーザーが電話（アプリではなく従来の電話回線を介して接続）や SIP/H.323 ルームベースのシステムなど、Zoom の通信プロトコルを本質的に使用しないデバイスを使用して Zoom の会議に参加する場合、Zoom の暗号化をその電話やデバイスで直接適用することはできません。とはいえ、私たちの目標は、可能な限り伝送プロセス全体でデータを暗号化しておくことです。これを実現するために、暗号化された会議とレガシーシステムの間で翻訳するための専用のクライアントを作成しました。当社ではこれらを Zoom コネクタと呼んでいます。

ズーム・テレフォニー・コネクタ

ズーム会議室コネクタ

Skype for Business コネクタ

クラウドレコーディングコネクタ

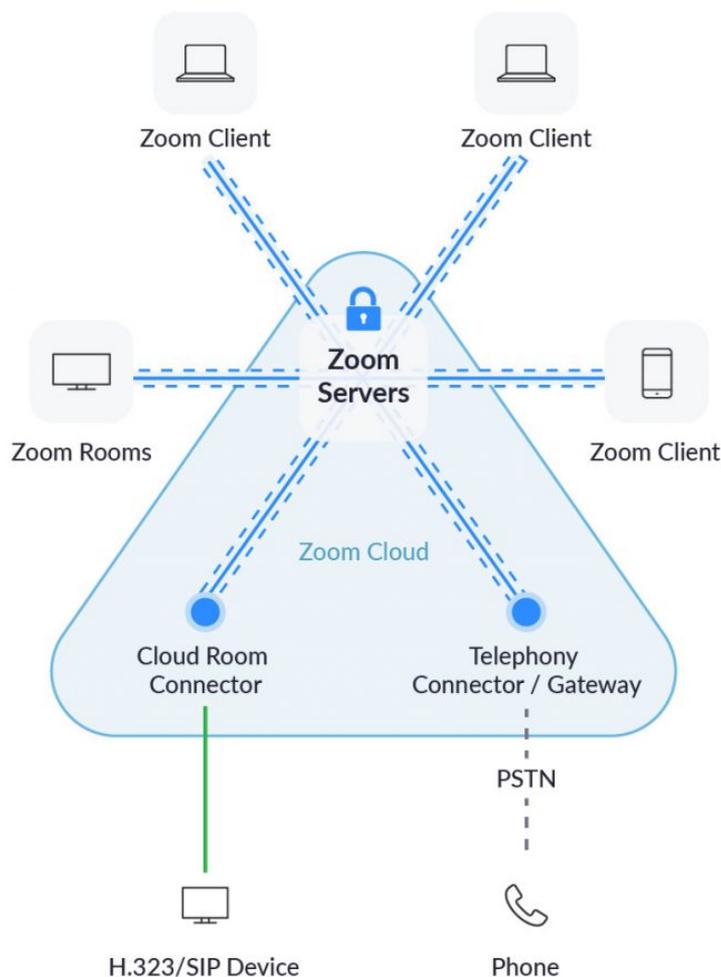
ライブストリーミングコネクタ

これらのコネクタは、事実上 Zoom のクラウドで動作する Zoom クライアントです。コンテンツは各コネクタにおいても暗号化されたままで、可能な場合は各コネクタと最終的な接続先（Zoom 以外のルームシステムなど）との間でデータを暗号化します。

コネクタは、会議主催者の操作により会議に招待され、会議のサービスの実行を支援することができます。この例としては、ライブ・ストリーミング・コネクタがあります。これは Zoom クライアントとして機能し、会議のコンテンツを他のウェブキャスティング・サービスなどで使用するライブ・ストリーミング形式に変換することができます。



コネクタが必要なシナリオにおいても、クライアント間でコンテンツを暗号化することで、お客様のコンテンツにアクセスできる Zoom 社のシステム数を減らし、より深い防御の役割を果たすことができるため、価値があると考えています。



このプロセス全体が 24 時間、世界中のお客様のニーズを満たすことを保証するために、Zoom は現在、これらのシステムのための鍵管理システムをクラウド上で維持しています。重要なことは、Zoom は、ユーザーが会議中に共有するあらゆるコンテンツへの不正アクセスを防ぐために、堅牢で検証された内部統制を導入していることです。

Zoom は、傍受目的でライブ会議を解読する仕組みを構築したことはありませんし、参加者リストに反映されずに従業員などを会議に挿入する手段も持っていません。

また、Zoom のクラウド・インフラストラクチャを活用しつつ、鍵管理システムをユーザー環境内で管理することができるソリューションも今年後半に提供される予定です。さらに、企業のお客様は、復号化と翻訳プロセスを自分たちで管理したい場合は、当社のコネクタの特定のバージョンを自社のデータセンター内で実行するオプションがあります。



当社は、セキュリティとプライバシーに関して、正しいことをすることをユーザーに約束しており、その重要性を理解しています。病院、大学、学校、および世界中の組織が接続と運用を維持するために Zoom に依存している中、当社は暗号化を使用してこれらの重要な機関のデータを保護するために行った作業を誇りに思っています。

以上