Zoom 加密

簡介

此份文件的目的為提供資訊，以瞭解使用在 Zoom 平台上的加密方式。我們的加密保護設計旨在盡可能提供最高等級的隱私性，並同時支援客戶群的多元需求。

個人連線到 Zoom 連線時，有幾種不同的使用狀況和可能進行的方式。下列文件概述潛在介面在與平台連線時可使用的加密方式。

使用 Zoom 用戶端時

Zoom 為 Mac、Windows、iOS、Android、Linux 提供多樣化功能的用戶端軟體套件，這些套件充分運用一系列的加密技術以提高使用者隱私和安全。**由用戶端傳輸至 Zoom 雲端的所有客戶資料在傳輸時，都經過下列其中一種方式加密。**

TLS 1.2

對於 Zoom 用戶端和 Zoom 雲端之間的連線，HTTPS 是較適合選用的通訊方式。連線時充分運用 TLS 1.2 加密和由可信賴商業認證機構核發的 PKI 認證。幾個常見的使用狀況包括登入用戶端、排程會議、聊天、投票、分享檔案和會議中問答。TLS 1.2 也可為其他通訊資料流做為備用協定，例如會議即時內容。

進階加密標準 (AES)

針對資料是透過使用者電報傳輸協定 (UDP) 傳輸的使用狀況，例如會議即時內容（視訊、聲音、內容分享），我們使用 ECB 模式的 AES-256 來為這些壓縮的資料串流加密。我們預期很快可升級到 AES-256 GCM。此外，針對以進階加密標準 (AES) 加密的視訊、聲音、內容分享，在到達另一個 Zoom 用戶端和 Zoom 連接器，協助將資料轉譯成另一個協定前，則維持通過 Zoom 會議伺服器時的加密方式。

SRTP

Zoom 電話產品使用經 AES-128-ECB 加密的安全即時傳輸協定，以保護進出我們資料中心傳輸的電話對話。此項功能很快可升級為 AES-256 GCM。

使用網頁瀏覽器時

Zoom 提供包含眾多特色功能的一道網頁介面，功能包括有完整的管理主控台、雲端錄製存取、廣泛的 API 端點集，以及網頁型會議用戶端。**所有自網頁瀏覽器傳輸到 Zoom 雲端的客戶資料（包括我們網站和透過我們網路會議用戶端者），在傳輸時會透過下列其中一種方式加密。**

TLS 1.2

連線至 Zoom 網站時充分運用 TLS 1.2 加密和由可信賴商業認證機構核發的 PKI 認證。個人可透過此入口網站，存取與 Zoom 帳戶相關的眾多特色功能，管理操作過程，並與其他系統整合。用於和網站連線時的加密能力和特定加密方式，將視使用來存取網站的瀏覽器，以及一般共用加密方式的協商結果而定。

AES-256

除 TLS 加密外，Zoom 網站也為特定使用狀況使用其他加密。例如，包括雲端錄製、聊天歷史和會議中繼資料的客戶資料透過金鑰使用 AES-256 GCM 以靜態方式儲存，此金鑰由雲端中的金鑰管理系統 (KMS) 管理。當使用者使用 Zoom 網頁用戶端以網頁組合 (web assembly) 連線到會議時，Zoom 將直接從以 AES-256 ECB 加密的會議伺服器，透過使用者電報傳輸協定 (UDP)，傳送和接收會議即時內容（視訊、聲音、內容分享）。

使用第三方裝置/服務時

做為開放平台的 Zoom 提供不同的方式，為一系列的服務和裝置與我們的系統進行連線。此包括對使用狀況的支援，例如連線到 Zoom 會議、透過常見串流服務廣播，和以一般電話線路（即非透過我們應用程式）撥入會議的 H323/SIP 裝置。由於這些整合服務必須利用特定第三方裝置或伺服器特有的通訊協定，因此僅限於使用該裝置可提供的加密方式。**因此，我們雖鼓勵使用第三方裝置和服務的加密，但透過這些裝置和服務所傳輸的客戶資料在進出 Zoom 系統傳輸時可能無法獲得加密。然而，資料到達 Zoom 系統時立即在該端點加密，而且在我們系統的整個傳輸期間內都會保持加密。**如果某一第三方裝置不支援加密，可能可使用下列一種方式來加密。

TLS 1.2

如裝置支援，Zoom 可透過 TLS 1.2 來協商。例如，如某一 SIP 裝置已啟用加密，此訊號將可使用 TLS。

進階加密標準 (AES)

如裝置支援，Zoom 將協商使用 SIP 的進階加密標準 (AES) 或 H323 端點來為會議內容（視訊、聲音、內容分享）加密。

結語

在現今社會的各個媒介和通訊平台上都可見協作的運用，因此 Zoom 致力於保護我們客戶的安全。當第三方裝置進入這套協作架構時，我們為我們平台之外的多種整合服務提供延伸加密的能力。我們確保客戶在我們平台內的內容都有加密。