

● より安心、より便利に。 Zoomの医療分野での活用

ZVC Japan株式会社 (Zoom Video Communications Japan)
公共・文教営業部 アカウントエグゼクティブ

相原健一

● はじめに

日本国内における延べミーティング参加者数が300万人/日を超えるまでにご利用いただいているZoom Meetings(以下Zoomミーティング)ですが、数年前までは単純に組織内での会議用途としての利用がほとんどでした。その後、コロナウィルス感染対策もあり外部との業務でのやりとり、そして「Zoom飲み会」をはじめとするプライベートな利用にも広がりました。また、その結果、使い勝手や品質、一般の方々への認知度を背景に、顧客とのコミュニケーションが必要なサービス、例えば教育、技術サポート、健康指導などをリモートで行うためのプラットフォームとして企業や団体に採用いただくことも増えました。

また、ハイブリッドなワークスタイルへの取り組みの一環として、対面のコミュニケーションの場においても、専門性の高い人材の有効活用、配置の見直しによる補完ツールとしても使われています。例えば言語通訳や手話通訳が必要な場合に通訳者のみオンラインで必要なタイミングだけ参加してもらう、という活用の仕方も最近では見られるようになりました。

● そもそもZoomとは

Zoom Video Communications, Inc.(以下Zoom) 創業者兼CEOのEric S. Yuanは、Webexの創設時の主要エンジニアでした。Ericらはコミュニケーションの活性化

で世の中をより豊かにしたいとWebexを開発しました。その後、WebexがCisco社に買収されEricも開発担当の責任者になりましたが、買収以降のWebexのクオリティーに満足できず、もっとビデオを使ってユーザーをハッピーにしたいというビジョンを掲げ、数十名の主要エンジニア達と共に2011年に米国カリフォル



図1 Zoomはビデオファーストのユニファイドコミュニケーション プラットフォーム

ニア州にてZoomの母体となる会社を設立しました。

ビデオ会議の専業ベンダーとしてスタートし、その後、ウェビナーやクラウドPBX(IP電話)のサービスなどを拡張し、最近ではUCaaS(Unified Communication as a Service)業界のリーダーとして位置付けられています。Zoomはコミュニケーションを円滑にすることによって、人々がHappyになることを目的として「Delivering Happiness」をポリシーに事業を展開しています(図1)。

Zoomとしては、ユーザーの皆様からのフィードバックをもとに、共通のニーズを拾い上げ、すぐさま機能強化につなげていくことができるスピード感を大事にしています。

これは、「Delivering Happiness」を実現する上で、非常に大切なことであり、会社としても重要視している取り組みです。

医療分野におけるZoomサービスの活用

官民間問わず様々な業務においてご利用いただいているZoomの各サービスですが、医療分野においてももちろん多くご活用いただいています(図2)。

教育や学会など含めたコミュニティの場においてZoomのミーティングやウェビナーをご利用いただくことは一般的になってきました。また、医療機関と患者間であれば、遠隔健康医療相談はもとよ

り、オンライン診療アプリとZoomミーティングを連携させてご利用いただくなど、遠隔医療の分野で活用機会も増えました。

また、放射線部門領域においても、画像の画面共有をしながら情報交換を行うことも多いと聞いています。

最近ではコロナ禍における院内への一般人の入館制限を背景とし、面会をオンラインで手軽に実施したいというニーズから、Zoomミーティングの使い勝手の良さや繋がりやすさを高く評価いただき、採用に至ったというお話もよくいただきます。

セキュリティについて

前述の通り米国に本社のあるZoomは、米国の法規制に準じた経営と、米国立標準技術研究所 サイバーセキュリティフレームワーク(NIST CSF)と整合性が取れたセキュリティプログラムを実行しており、情報セキュリティマネジメントシステム<ISMS>に関する国際規格(ISO/IEC27001:2013)や米国公認会計士協会(AICPA)の定めるSOC2 Type2などの公的なセキュリティ認証を取得し、医療や金融などの特にセキュリティ要件の厳しい業界においても安心してご利用いただいております。また、Zoom運用時のセキュリティ機能についても継続的に強化していることから、Zoomのセキュリティ

面での懸念点はないと外部調査でも報告されています¹⁾。

一方で、実際にユーザー自身の環境へ適用した場合、ユーザーのセキュリティポリシーに応じた形で適切に認証とアクセス制御を行い、外部からの不正アクセスを防ぐとともに、データを保護し情報漏洩を防がなければなりません。

サイバーセキュリティ基本法に基づき、内閣に設置されるサイバーセキュリティ戦略本部が、令和3年7月7日に公開した「政府機関等のサイバーセキュリティ対策のための統一基準群」令和3年度版においても、Web会議サービス利用時の対策に係る項目が新設されました。政府機関等の対策基準策定のためのガイドライン(令和3年度版)では、

1. 要機密情報を取り扱う場合は、可能な限りエンドツーエンド(E2E)の暗号化を行うこと。
2. 会議室にアクセスするためのパスワード等をかける。
3. 待機室を設けて参加者と確認できた者だけを会議室に入室させる。
4. なりすましや入れ替わりが疑われるなどの不審な参加者を会議室から退室させる。

などが対策方法として挙げられています。

また、ログ(証跡)を取得し定期的に確認を行うことで、不審なアクセスがないかの発見的な統制を行う必要があります。さらにビデオ会議中のリスクに対応することも必要です。

ビデオ会議を安全に実施いただくためにはさまざまな対応が求められますが、ここでZoomの提供する強力かつ詳細なセキュリティ設定をいくつかご紹介させていただきます。

●E2EE

ミーティング開催時の暗号化については、256-bit AES-GCMを用いた暗号化とエンドツーエンド暗号化(End to End Encryption : E2EE)のどちらかを利用するオプションがあります。E2EEは主催者が暗号化鍵を生成し、参加者に配布します。これにより、サービスを提供しているZoomのサーバー側には鍵が保持されないため、参加者以外の鍵の不正利用による覗き見を回避することができます。



図2 医療分野における活用シーン