お客様各位

ZVC Japan 株式会社
カントリーゼネラルマネージャー
佐賀文宣

Zoom のセキュリティ・プライバシーへの対応状況（4 月 16 日）

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。

さて、Zoom のプライバシーとセキュリティをめぐり、メディアに多く取り上げられたことについて、ご心配をおかけし申し訳ございません。
弊社は、一連の指摘に速やかに対処し、これまでと同様に、皆様に対して正しく、オープンに情報をご提供したいと考えております。

弊社の創設者、兼、最高経営責任者（CEO）、エリック・ユアンが、お客様向けに掲載いたしました文書(*)に詳細が記述されておりますが、一連のセキュリティとプライバシーに関する機能の精査と追加は、私共のプラットホームが、元々は IT 管理者をお持ちの、企業のお客様に向けてつくられてきた一方、昨今の状況下で、今までよりはるかに多くの、特に個人ユーザーが、想定外の方法で Zoom をご利用いただくようになったことに起因します。
これまでに多くの企業が私共のアプリケーション、ネットワーク、およびデータ層を綿密に検証したうえで、Zoom をお選びいただきました。しかし、ここ数週間で、主に個人ユーザーのユースケースでの懸念がメディアに取り上げられ、広く報道されている新しい問題が明らかになりました。
既に最新版のクライアントにほぼ全ての修正が反映されておりますので、更新いただくことで安心してご利用いただけます。

*弊社の創設者兼最高経営責任者（CEO）エリック・ユアンから皆様へのメッセージ
https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/
日本語訳はこちらです。
https://sites.google.com/zoom.us/zoomjapanfaq/zoomblog/a-message-to-our-users

上記メッセージおよびその後に取られた個別事象への対応状況を以下に補足いたします。

＜Facebook へ不要な情報送信について＞
影響を受ける環境: iOS 環境で 4.6.9 より前のバージョンのクライアントをご利用の場合
→対処: 3 /27 公開の 4.6.9 以降の最新版 iOS クライアントをご利用ください。
https://support.zoom.us/hc/en-us/articles/201361943-New-Updates-for-iOS
・原因となっていた Facebook ログインの為の SDK は使用を停止しました。
※事象の詳細 https://sites.google.com/zoom.us/zoomjapanfaq/zoomblog/zoom-use-of-facebook-sdk-in-ios-client?authuser=0

＜Windows 認証情報取得に関する脆弱性について（バージョン 4.6.9 で対応）＞
影響を受ける環境: Windows 環境でユーザがチャット上に共有された UNC リンクをクリックした場合
→対処: 4/2 公開の 4.6.9 以降の最新版 Windows クライアントをご利用ください。
https://support.zoom.us/hc/en-us/articles/201361953-New-Updates-for-Windows
・UNC リンクの悪用に繋がる問題を修正しました

＜Mac 版インストーラに関する脆弱性について（バージョン 4.6.9 で対応）＞
影響を受ける環境: Mac OS 環境で 4.6.9 より前のバージョンをご利用の場合
→対処: 4/2 公開の 4.6.9 以降の最新版 Mac クライアントをご利用ください。
https://support.zoom.us/hc/en-us/articles/201361963-New-Updates-for-macOS
・ローカルアクセスが可能なユーザが Zoom のインストーラを悪用して権限昇格できる問題およびウェブカメラやマイクにアクセスできる問題を修正しました

＜セキュリティボタンの追加（バージョン 4.6.10 で追加）＞
ホストの利便性を高めるため、それまでメニューの様々な場所にあったミーティングのロック、待機室等のセキュリティに関わる機能を新しく作った セキュリティボタン内に集約いたしました。
https://sites.google.com/zoom.us/zoomjapanfaq/zoomblog/zoom-product-updates-new-security-toolbar-icon-for-hosts-meeting-id-hidden?authuser=0

<不審なユーザの参加防止>
管理者の方は自社のポリシーに即した設定がされているか、改めてご確認ください。
今までもパスワードロックと、待機室機能はございましたが、無料ユーザと 1 ライセンスのみの有料ユーザーは初期値で、それらのセキュリティ機能が有効となるよう変更いたしました。（複数ライセンスをお持ちの有料ユーザーは、これまで通りに設定可能です。）
https://support.zoom.us/hc/ja/articles/360041408732-April-2020-Setting-updates-for-free-accounts-and-single-Pro-users

招待していないゲストを Zoom イベントから遠ざける方法は下記のブログでも紹介させていただいております。
https://sites.google.com/zoom.us/zoomjapanfaq/zoomblog/keep-uninvited-guests-out-of-your-zoom-event?authuser=0
『Zoom ミーティングを安全に実施するための 10 の方法』も合わせてご参照ください。
Zoom Japan FAQ サイト(https://sites.google.com/zoom.us/zoomjapanfaq/)から 4/17 以降にご覧いただけます。

＜待機室機能の脆弱性について＞
参加者が待機室にいる間にセッションキーを送信する仕様になっておりましたが、サーバー側の変更で、ミーティング参加が許可されて初めて送信されるように仕様を変更しました。

＜エンドツーエンドの暗号化＞

弊社の暗号化の実装に対しての議論の中で、Zoom のミーティング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。
https://sites.google.com/zoom.us/zoomjapanfaq/zoomblog/facts-around-zoom-encryption-for-meetings-webinars?authuser=0
なお、クラウド録画を有効にしているミーティングでも、Zoom クライアントと Zoom サーバー間は暗号化されております。

＜中国本土のデータセンターを経由していたことについて＞
前例のないパンデミックの間に世界中の人々の助けになろうという緊急性の中で、私たちはサーバーの容量を追加し、(アウトブレイクが始まった中国から開始し)迅速に展開しました。その過程において、Zoom では通常のジオフェンシングのベストプラクティスを完全に実施することができませんでした。その結果、本来は接続できないはずの中国のシステムへの接続が許可されたミーティングがあった可能性があります。その後、この問題は修正されました。
https://sites.google.com/zoom.us/zoomjapanfaq/zoomblog/response-to-research-from-university-of-torontos-citizen-lab?authuser=0
対策として、Zoom の有料会員のお客様は、アカウントがリアルタイムのミーティング・トラフィックに使用できるデータセンターのリージョン(地域)をカスタマイズできるようになります。
https://sites.google.com/zoom.us/zoomjapanfaq/zoomblog/coming-april-18-control-your-zoom-data-routing?authuser=0

＜50 万以上の Zoom アカウント ダークネットで売買＝報道＞
個人ユーザーにサービスを提供しているウェブサービスがこの種の攻撃の標的になることは一般的で、悪意のある者が他のプラットフォームから不正に入手したクレデンシャルを手当たり次第にテストして、ユーザーが他の場所でも同じクレデンシャルを使っているかどうかを調べる方法などがあります。
この種の攻撃は、通常、シングルサインオンシステムを使用している大企業のお客様には影響を与えません。
当社では、これらのパスワードダンプとその作成に使用されたツールを発見するために複数の調査機関と連携し、また、ユーザーを騙してマルウェアをダウンロードさせたり、クレデンシャルを引き出そうとする数千のウェブサイトをシャットダウンするための機関とも連携をしています。今後も継続的に調査を続け、漏洩していることが判明したアカウントをロックし、ユーザーにパスワードをより安全なものに変更するよう注意を促します。また、この取り組みを強化するために追加の技術ソリューションの導入も検討しています。

＜脆弱性情報の売買=報道＞
この噂を受けて、弊社は業界をリードする評判の高いセキュリティ会社と協力して、24 時間体制で調査を行っています。現在までのところ、これらの主張を裏付ける証拠は見つかっていません。

＜その他、今後の対策について＞

Zoom は 90 日の間、新規開発を止め、プライバシーとセキュリティ強化に努めます。
https://sites.google.com/zoom.us/zoomjapanfaq/zoomblog/update-on-zoom-90-day-plan-to-bolster-key-privacy-and-security-initiatives?authuser=0

今後、英語版の情報のご提供後、速やかに下記にて日本法人でも情報をご提供してまいります。
https://sites.google.com/zoom.us/zoomjapanfaq/

以上