関係各位

# セキュリティ情報： Zoom 会議実施時に注意すべき事項について

2020 年 4 月 10 日
（一社）日本マーケティング・リサーチ協会

平素より協会活動にご協力をいただき、誠にありがとうございます。

新型コロナウイルス感染症の世界的な蔓延を受け、ビデオ会議用ソフトウェア・アプリケーション等を使用したテレビ会議や遠隔コミュニケーションが急速に普及しつつあります。それらの中でも、その簡便性から Zoom アプリの利用が一気に広がり、すでに多くの皆様が使用されていることと存じます。

先般、この Zoom にセキュリティ面の脆弱性が指摘され、ネット上の話題にもなりました。対策も速やかに公表されておりますので、皆様におかれましては以下の対応を徹底していただきますよう、強くお願いいたします。

## Zoom に指摘された問題点と対策

| 指摘された問題点 | 対　策 |
|---|---|
| ① システム面の脆弱性（例）<br>・ チャット機能に関わる処理の脆弱性<br>・ 悪意あるユーザーによる情報窃盗の可能性<br>（仕掛けられたリンクをクリックした場合） | ⇒ アプリのバージョンアップで解決できます<br>・ バージョン 4.6.10 にアップデートする<br>（スタートページ右上のアイコンから「アップデートを確認」をクリック） |
| ② 運用面の課題<br>・ 招かれざる客が入場する可能性<br>（パスワードが設定されていない場合など）<br>・ 悪意あるユーザーによる会議妨害の可能性<br>（ある大学では講義妨害が実際に発生） | ⇒ 上記のバージョンアップ＋会議ホストの運用強化で対応します<br>・ 必ず会議ごとにパスワードを設定・通知する<br>・ ホストは「待機ルーム」を使用し、承認された人しか会議に入れないようにする<br>・ 不規則発言等をする参加者が出た場合、ホストが強制ミュートまたは強制退去させる |

## それでも残るリスクへの対応（Zoom に限らず、テレビ会議システム全般）

例えば悪意ある参加者が、「会議画面をビデオ撮りする」ことによる情報漏洩リスクはシステム的に防ぎようがありません。これは Zoom に限らず、あらゆるテレビ会議等に共通する課題です。

会議主催者は、すべての参加者にセキュリティ確保のための注意喚起・教育を徹底させるとともに、最重要な議題や資料は Zoom 等のテレビ会議には流さないことなどを検討してください。

皆様のご協力をよろしくお願いいたします。

（参考）IPA：情報処理推進機構の発表「Zoom の脆弱性対応について（4/3 付）」
https://www.ipa.go.jp/security/ciadr/vul/alert20200403.html

以上