



Kagawa Cyber Security Information

香川県サイバーセキュリティ連絡ネットワーク通信Vol.49

～ ビデオ会議アプリ「Zoom」について ～ 最新のバージョンにアップデートしていますか??

新型コロナウイルス(COVID-19)の蔓延に対する懸念が高まっている中、多くの企業が在宅勤務に移行しています。そこでテレワークには欠かせないビデオ会議アプリ「Zoom」の利用が急増していますが、セキュリティ対策の必要性も指摘されています。

ビデオ会議アプリ「Zoom」の特徴

- 専用のソフトの必要なし、初期設定が簡単
- 同時に100人（有料版は1000人）が参加して通話可能
- タブレット、スマホ、Windows、Mac等端末やOSに左右されず使用可能
- 維持費が安く、通信環境が安定している etc

新型コロナウイルスのため、在宅勤務の一環で「Zoom」を導入する企業が急増に伴い、セキュリティの問題（脆弱性）が噴出
利用者（全世界） 2019年12月

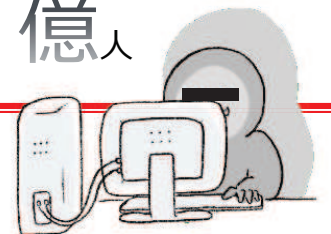
1,000万人

2020年3月

2億人

脆弱性

- ビデオ会議参加用パスワードを設定していないと、URLを知れば誰でも会議に参加できてしまう
- Windows版のチャット機能を通して、ログイン情報等の認証情報等が盗まれる危険性が存在している
- Mac版のアプリには、マイクやカメラに不正にアクセスされる危険性が存在している



- 1 常に最新のバージョンを利用する
※Version4.6.9以上に!! (Zoomのアカウント画面から確認できます)
- 2 利用のルールを決め、機密性の高い情報を扱う場合は「Zoom」を利用しない
- 3 会議用のURLは不特定多数には公開せず、パスワードを設定する
- 4 アカウントのID、パスワードは使いまわしをしない

