

ビデオ会議ソフトのセキュリティ

Security issues on video conference softwares.

Hiroki Kashiwazaki (CCRD, NII)

表 1 オンライン会議ツールの比較

機能	Polycom	Skype	Cisco Webex	Zoom	Microsoft Teams	Google Hangouts	BlueJeans
画面シェア	○	○	○	○	○	○	○
チャット	×	○	○	○	○	○	○
チャットログ保存	×	○	○	○	×	×	×
録音	×	○	○	○	○	△(*2)	×
録画	×	○	○	○	×	△(*2)	×
お絵かき	×	×	○	○	×	×	×
他者管理	○	×	○	○	○	○	×
ブラウザ内実行	×	△(Chrome/Edge)	△(*4)	△(*4)	△(*5)	○	×
Androidアプリ	○	○	○	○	○	○	○
iOSアプリ	○	○	○	○	○	○	○
NAT 下利用	△	○	○	○	○	○	○

(*1): 別途録音/録画機材が必要, (*2): Enterpriseのみ, (*3): ミュートから ON のみ可能
 (*4): 利用できる機能については制約あり, (*5): Microsoft Edgeのみ

編者: 松崎 悠樹(元), 宮下 勇樹, 池田 隆, 北口 謙介, 山本 昌良, 宮下 秀, 村上 悠太郎, 石原 誠, 田橋 孝人, 佐藤 伸, 中村 隆, 佐藤 人, 三浦 和正, 大塚 博典
 制作: 株式会社サイバーセキュリティ研究所(元)・株式会社 東京大学インターネットセキュリティセンター (ICT), Ver. 2020-07-09 (2020.7.9更新)

NIST CYBERSECURITY INSIGHTS a NIST blog

Preventing Eavesdropping and Protecting Privacy on Virtual Meetings

Conferences calls and web meetings—virtual meetings—are a constant of modern work. And while many of us have become security-conscious in our online interactions, virtual meeting security is often an afterthought, at most. Who hasn't been finishing one call when attendees of the next call start joining – because the access code is the same? In the moment it may be annoying, or even humorous, but imagine if you were discussing sensitive corporate (or personal) information. Unfortunately, if virtual meetings are not set up correctly, former coworkers, disgruntled employees, or hackers might be able to eavesdrop or disrupt them. Using some basic precautions can help ensure that your meetings are an opportunity to collaborate and work effectively – and not the genesis of a data breach or other embarrassing and costly security or privacy incident.

So...where to start? Most virtual meeting services have built-in security features, and many providers will give you <https://www.nist.gov/blogs/cybersecurity-insights/preventing-eavesdropping-and-protecting-privacy-virtual-meetings>

- If available, use a dashboard to monitor attendees – and identify all generic attendees.
- Don't record the meeting unless it's necessary.
- If it's a web meeting (with video):
 - Disable features you don't need (like chat, file sharing, or screen sharing).
 - Consider using a PIN to prevent someone from crashing your meeting by guessing your URL or meeting ID.
 - Limit who can share their screen to avoid any unwanted or unexpected images. And before anyone shares their screen, remind them not to share sensitive information inadvertently.

- 仮会議のセキュリティに関する組織のポリシーに従う。
- アクセスコードの再利用はやめましょう。しばらくの間、同じコードを使用していた場合、おそらく想像以上に多くの人がそれを共有している可能性があります。
- 話題が機密性の高いものである場合は、OTPや会議の識別子コードを使用し、多要素認証も検討しましょう。
- ロビー (待機室) 機能を使用し、ホストが参加するまで会議を開始できないようにします。
- 出席者が参加したときに音を鳴らしたり、名前をアナウンス

- 出席者が参加したときに音を鳴らしたり、名前をアナウンスしたりして通知を有効にします。これがオプションでない場合は、会議の司会者が新規参加者に自分の名前を名乗るように促します。
- ダッシュボードがある場合は、ダッシュボードを使用して出席者を監視し、一般的な出席者をすべて識別します。
- 必要な場合を除き、会議を録音しないようにします。
- ビデオ会議であれば...
 - 不要な機能 (チャット、ファイル共有、画面共有など) を

- Follow your organization's policies for virtual meeting security.
- Limit reuse of access codes; if you've used the same code for a while, you've probably shared it with more people than you can imagine or recall.
- If the topic is sensitive, use one-time PINs or meeting identifier codes, and consider multi-factor authentication.
- Use a "green room" or "waiting room" and don't allow the meeting to begin until the host joins.
- Enable notification when attendees join by playing a tone or announcing names. If this is not an option, make sure the meeting host asks new attendees to identify themselves.

内閣サイバー(注意・警戒情報) @nisc_forecast

【注意喚起】(1/2)
 Zoom社が、Web会議サービスにおけるセキュリティ等に関する指摘への対応状況についてメッセージを出しています。
 サービスをお使いになる際はセキュリティ関連情報や事業者の対応状況等に注意し、アップデートを行うなど必要に応じて臨機応変に対応することが重要です。

(続く)

午前11:14 · 2020年4月3日 · Twitter Web App

IPA Better Life with IT 情報処理推進機構

HOME 情報セキュリティ 産業サイバーセキュリティセンター 社会基盤センター 高齢者セキュリティセンター 外国人の育成 情報処理推進機構 情報処理推進機構受託事業

情報セキュリティ

Zoomの脆弱性対策について

情報セキュリティ

Zoomは、ゼロ日脆弱性プログラム。

<https://www.ipa.go.jp/security/ciadr/vulaler/20200403.html>

Zoomを用いたオンライン講義を安全に進めるために
情報基盤センター 2020.4.6

オンライン講義に用いることができるソフトウェアの一つであるZoomについて、セキュリティ上の懸念がいくつか報道されております。

その内容は、

- Zoomのソフトウェア等のセキュリティ上の問題点
- Zoomの仕様によるもので、実際には問題にならないと考えられること、または運用上の配慮で問題を回避できると考えられること

に分かれます。このうち、前者については、Zoom側で対応が進んでおり、私どもが把握している範囲ではすべて対処済みとなっています。但し、ソフトウェアを最新版にアップグレードしておくことが重要です。後者については、特に運用上の配慮が必要なものが、講義中に第三者がミーティングに参加して音声や画像等で妨害する。いわゆるZoom bombingと呼ばれる事象です。本学のオンライン講義でもすでに妨害が報告されております。

Zoom bombingを防ぐためには、

- 外部の人間が講義に入ってくることをないようにする
- 妨害されたときの対処を確認しておく

ことが必要です。以下、具体的に対応策を示します。

https://apps.adm.s.u-tokyo.ac.jp/WEB_info/pub/5750/Zoom.pdf

付記：Zoomのセキュリティに関する報道等について

Zoomのセキュリティに関して、いくつかの報道がなされています。以下は、4月5日現在で確認できた報道について、その深刻度や解決状況等をまとめたものです。全体として、Zoomのソフトウェアおよびシステムにはいくつかのセキュリティ上の問題点が存在しましたが、現在までにすべて解決しています。このため、最新のソフトウェアを用いることが重要です。

一方、その他の問題は、Zoom Bombingのように、Zoomの機能に欠陥があるというよりも、使い方に気を付ける必要がある事象です。

以下の表に、報道等で指摘されている問題点と、その内容をまとめてみました。

問題点	報道されたメディア(代表的なもの)	内容	解決状況/深刻度
		Zoom社は、end-to-endで暗号化しているという表現をしています。Zoomは、映像の送りが先に暗号化されているため、音声は暗号化されていない。	端末とサーバの間では暗号化されている。Zoomは、映像の送りが先に暗号化されているため、音声は暗号化されていない。

メールアドレスが漏洩している	Gigazine	同じドメイン名を持つユーザーを同一組織の人間であるか、利用者をコンタクトリストに載せていた。大手でない(Gmail, Yahoo, hotmailなどでない) メールサービスプロバイダと契約した場合、ドメインが同じであることから同じ組織の所属者みなされ、加入者間でコンタクトが漏洩していた。	東京大学では、相互にコンタクト情報が閲覧できないようにする措置を取っている。
インストール時に管理者パスワードを取得し、これを用いて自動でインストールするという手法を取っている	Gigazine	Mac: Zoomのインストーラが、システムからの要求のように見せかけて管理者パスワードの入力を求めることが問題視されている。	修正済み (April 2, 2020 Version 4.6.9 (19273.0402))



RESEARCH NEWS ABOUT

<https://citizenlab.ca/2020/04/zooms-waiting-room-vulnerability/>

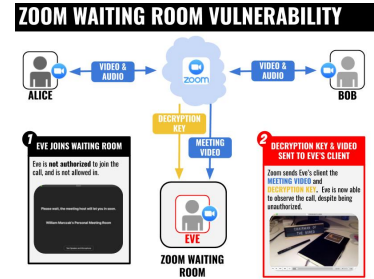
Research > App Privacy and Controls

Zoom's Waiting Room Vulnerability

By Bill Marczak and John Scott-Railton April 8, 2020

Zoom's Waiting Room Vulnerability

This research note is a follow-up to our April 3, 2020 report on the [confidentiality of Zoom Meetings](#). In this note, we describe a security issue where users in the "waiting room" of a Zoom



INFORMATION SECURITY NEWSPAPER

<https://www.securitynewspaper.com/2020/04/08/hackers-leak-zoom-accounts-username-passwords-full-names-and-email-addresses/>

HOME DATA SECURITY + VULNERABILITIES TUTORIALS + INCIDENTS MALWARE NEWS VIDEOS

LATEST VIDEOS

HACKERS LEAK ZOOM ACCOUNTS' USERNAMES, PASSWORDS, FULL NAMES AND EMAIL ADDRESSES

COMPANIES ARE ASKING THEIR EMPLOYEES TO TURN OFF THEIR SMART SPEAKERS WHILE WORKING FROM HOME

ZOOM-BOMBING: HACKERS SHOW PORNOGRAPHIC AND RACIST CONTENT DURING UNIVERSITY OF MASSACHUSETTS VIDEOCONFERENCE

Share this...

Forced social distancing has unusually driven the use of remote communication platforms such as Skype, Hangouts, WhatsApp and mainly Zoom, which has shown a pronounced growth in terms of its number of users a couple of months ago, mention specialists of a **cyber security course**. Academic institutions, government offices and private companies have resorted to using Zoom to maintain their primary activities relatively normal.

行政院 Executive Yuan

About Newsroom Policies Multimedia COVID-19 Health Education Videos

Executive Yuan orders agencies to step up video conferencing security

Date: 2020-04-07
Source: Department of Information Services, Executive Yuan

Vice Premier and leader of the Executive Yuan's overall cyber security mission Chen Chi-mai on Tuesday said that Taiwan enacted its Cyber Security Management Act in 2019 with the goal of implementing information and data security measures, as well as defending the nation's critical communications infrastructure. The act stipulates that all organizations introducing information and communication systems should not utilize goods or services that raise data security concerns. In addition, procurement priority should focus on

<https://english.gov.tw/Page/81BF209c3E998568493876a-0aa7-4b84-8fba-1b3a-1183845f>

GOOGLE BUSINESS TECH

Google bans its employees from using Zoom over security concerns

The Zoom backlash has arrived at Google

By Nick Statt | @nickstatt | Apr 8, 2020, 3:55pm EDT

Google is issuing a ban on the use of the Zoom teleconferencing platform for employees. The company is citing security concerns with the app that have arisen since Zoom became one of the most popular services for free video chatting during the COVID-19 pandemic. The news was first reported by [BuzzFeed News](#) earlier today.

Google emailed employees last week about the ban, telling workers who had the Zoom app

<https://www.theverge.com/2020/4/8/21213978/google-zoom-ban-security-risks-hangouts-meet>

<https://threatpost.com/cisco-critical-update-phishing-webex/154585/>

threatpost Cloud Security Malware Vulnerabilities Waterfall Security Spotlight Pod

Unbreakable Smart Lock Drives FTC Ire for Deceptive Security Claims Zoom Taps Ex

Cisco 'Critical Update' Phishing Attack Steals Webex Credentials

私見

- Zoomは「ここ90日はセキュリティに注力する」と述べているので、その動向をウォッチするコストをかけつつならば、使う価値があるかもしれない。
- 「せっかく購入したのだから」のような「Zoomを使うことが目的化している」ことについては再考を。Cisco Webexが180日キャンペーンをやっていることですし。
- 冗長化は大事。事業の継続性、高可用性が重要。