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	×（*1）	○	○	○	×	△（*2）	×
録画	×（*1）	○	○	○	×	△（*2）	×
お絵かき	×	×	○	○	×	×	×
他者管理	○	×	○	○	○	△（*3）	×
ブラウザ内実行	×	△（Chrome/Edge）	△（*4）	△（*4）	△（*5）	○	×
Andrid 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

綿田朗, 柏崎礼生, 宮下健輔, 池部実, 北口善明, 山井成良, 荻下秀, 村上豊志男, 石島晃, 石橋美人, 佐藤聡, 中村豊, 林治郎, 松本直人, 三島和宏, 大谷紘, 仲田秀夫: オンライン学術会議の運営に関する一考察, 研究報告インターネットと運用技術（IOT）, Vol. 2020-IOT-49 (2020) [to appear]

NIST

CYBERSECURITY INSIGHTS a NIST blog

Preventing Eavesdropping and Protecting Privacy on Virtual Meetings

Conference 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

- 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.

- 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.

- 仮想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

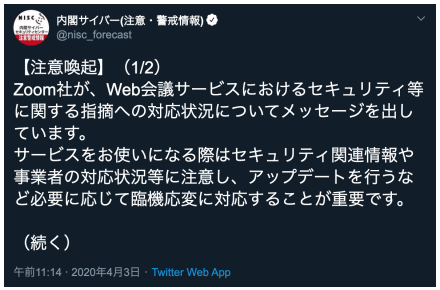
- 出席者が参加したときに音を鳴らしたり、名前をアナウンスしたりして通知を有効にします。これがオプションでない場合は、会議の司会者が新規参加者に自分の名前を名乗るように促します。
- ダッシュボードがある場合は、ダッシュボードを使用して出席者を監視し、一般的な出席者をすべて識別します。
- 必要な場合を除き、会議を録音しないようにします。
- ビデオ会議であれば…
  - 不要な機能（チャット、ファイル共有、画面共有など）を

- 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）を無効にします。
  - URLや会議IDを推測されて会議が中断されるのを防ぐために、パスワード(PIN)の使用を検討してください。
  - 不要な画像や予期せぬ画像が表示されないように、画面を共有できる人を制限します。また、誰かが画面を共有する前に、機密情報を不用意に共有しないように注意してください。

zoom

ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM

FedRAMP



https://www.ipa.go.jp/security/ciadr/vul/alert20200403.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

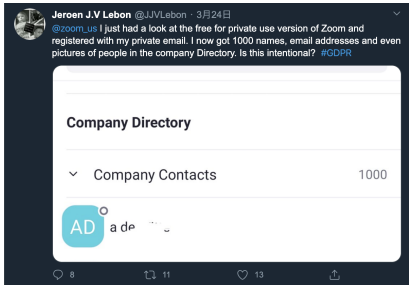
オンライン講義に用いることができるソフトウェアの一つであるZoomについて、セキュリティ上の懸念がいくつか報道されております。
その内容は、
・Zoomのソフトウェア等のセキュリティ上の問題点
・Zoomの仕様によるもので、実際には問題にならないと考えられること、または運用上の配慮で問題を回避できると考えられること
に分かれます。このうち、前者については、Zoom側で対応が進んでおり、私どもが把握している範囲ではすべて対処済みとなっています。但し、ソフトウェアを最新版にアップデートしておくことが重要です。後者については、特に運用上の配慮が必要なのが、講義中に第三者がミーティングに参加して音声や画像等で妨害する、いわゆるZoom bombingと呼ばれている事象です。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、
1. 外部の人間が講義に入ってくることがないようにする
2. 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/p/pub/5756/Zoom.pdf

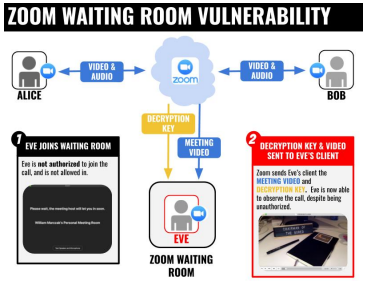
付記：Zoomのセキュリティに関する報道等について

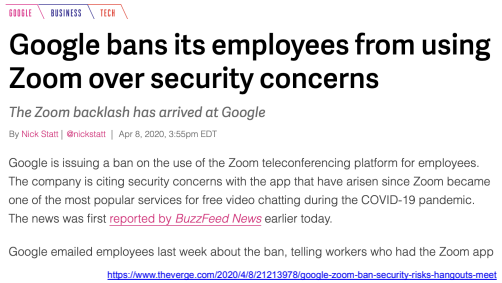
Zoomのセキュリティに関して、いくつかの報道がなされています。以下は、4月5日現在で確認できた報道について、その深刻度や解決状況等をまとめたものです。
全体として、Zoomのソフトウェアおよびシステムにはいくつかのセキュリティ上の問題点が存在しましたが、現在までにすべて解決しています。このため、最新のソフトウェアを用いることが重要です。
一方、その他の問題は、Zoom Bombingのように、Zoomの機能に欠陥があるというよりも、使い方に気を付ける必要がある事象です。
以下の表に、報道等で指摘されている問題点と、その内容等をまとめました。

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	端末とサーバの間では暗号化されている。Zoomは、映像

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
オンライン通話がEnd-to-Endで暗号化されていない	Gigazine Routers	Zoom社は、end-to-endで暗号化しているという表現をしたことがあるが、サーバにおいては復号化されて処理されているため、配信者と参加者間で常に暗号化されているわけではない。但し、配信者とZoomサーバ、Zoomサーバと参加者間では暗号化されており、第三者が盗聴（盗視聴）できるわけではない。	端末とサーバの間では暗号化されている。Zoomは、映像の送り先ごとに映像品質の調整などをしているので、サーバでの復号はほぼ不可欠。サーバ側で復号された情報を扱うのはクラウドサービスでは普通。クラウドに置けないほどの高度に機密性が高い情報のやり取りにはZoomを使うべきではない。（そういう場合は別途考慮要）
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を同一組織の人間であるとみなし、利用者名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とみなされ、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)）







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。