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。

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

これには、

a) Zoomの認証機能を用いて、東京大学のメールアドレス(u-tokyo.ac.jp)でZoomにサインインしている者しか参加できないようにする

b)第三者がZoomミーティングのアクセスに必要な情報を知り得ず、安易に推測もできないようにする。

の２つの方法があります。

a)が有効で本来の対策ではありますが、現段階では学生全員が東京大学のメールアドレスでサインインしたうえでオンライン講義に参加する方法を把握している状況ではありません。このため、この方法を用いると本来参加できるべきなのに参加できない学生が出る可能性があります。このため、当面の対策はb)となります。これには、

・ミーティングにはパスワードを設定する。

・ミーティングに参加するための情報が外部に漏れないように管理する。

ことが重要です。パスワードを設定しないと、9桁（もしくは10桁）の数字が一致すればミーティングに入れますから、ランダムに数字を設定してどこかのミーティングに参加できる可能性があり、荒らしに会っているミーティングは多くがこの状態と推測されます。すでにパスワードがない状態でオンライン講義を設定されている方も、パスワードを設定してください。

ミーティング情報の管理では、ミーティングIDとパスワードや、ミーティングのURL(標準設定ではURLの中にパスワード情報が埋め込まれています）が外部に知られないように慎重に扱い、受講生へ周知する際にも、学内者しかアクセスできない場所に置くように徹底する（公開された講義HPなどには書かない）ことが必要です。また、学生がSNS等で発信しないように注意しておくことも重要です。ミーティングIDはなるべく毎回変更し、パーソナルミーティングIDは使わないことも有効と考えられます。UTAS，ITC-LMSはどちらも学内者(UTokyo Accountの保持者)しかアクセスできない場所であるため、それを通知する場所として利用できます。

東京大学授業カタログからの公開情報について

UTASを用いて授業を通知する際、シラバス中の「詳細情報」に新設された「オンライン授業URL」の欄に書くことを推奨しておりますが、その他の欄に自由記述をしているケースが散見されています。その場合シラバス中のいくつかの欄（詳細は以下）が東京大学授業カタログ（ https://catalog.he.u-tokyo.ac.jp/ ）に掲載、公開されている（またはい

た）ことにご注意の上、必要な対策（以下に記述されていたオンライン会議情報はこれ以上使わず、URLを作り直す）を取っていただきたいと思います。以下が、過去のある時点で公開されていたオンライン会議情報です。

> 3月27日以前に、UTASシラバス情報「授業の目標、概要」「授業計画」「授業の方法」「成績評価方法」「教科書」「参考書」「履修上の注意」「その他」欄にかかれていた情報。

それ以降に書かれた情報はマスキング処理が施されて情報がそのまま授業カタログに載らないようにしておりますが、さらなる検証と対策を施す予定です。

2. 妨害されたときの対処

何らかの方法で第三者にオンライン講義に参加されてしまった場合の対処としては、事前に行っておくことと、妨害が発生したときに行うことがあります。

2.1. 事前準備

- 講義を補助してくれる補助者がいる場合には、補助者もミーティング中の操作ができるように共同ホストにしておきます。これは、ミーティング予約時に設定しておくこともできますし、開催時に「参加者」ウィンドウから設定する事もできます。
- 画面を共有できるのはホストのみとしておきます。現在は、予約作成時の標準設定は「ホストのみ」となっています。参加者に画面を共有させる必要があるときは、ミーティング中に変更することができます。
- 参加者に、共有画面に線や文字、図形等を記入する「コメント（注釈）」を許可しない設定としておく。現在は、予約作成時の標準設定では許可しないようになっています。
- ファイル転送、参加者同士のチャット（プライベートチャット）はできないようにしておきます。現在は、予約作成時の標準設定ではできないようになっています。

なお、上記の標準設定は、4月5日以前に作成した予約では異なっていることがあります。また、ミーティングの参加前に必ずホストが承認するようにする「待機室」を用いることも考えられますが、人数の多い講義では全員を確認するのは現実的ではないこと、開始後に参加する参加者をそのたびごとに承認しなくてはならないなどの問題があります。「待機室」機能を使用する際にはこの点にご留意ください。

2.2. ミーティング中の操作

ミーティング中にできることは、以下のようなことがあります。これらの機能を用いて妨害を排除します。以下の操作の説明は、WindowsおよびMacの場合で説明しています。

- 参加者を強制的に退出させる
  - コントロールツールバーの「参加者の管理」をクリックし、参加者ウィンドウを表示する。退出させたい参加者の上にマウスカーソルを置き、詳細メニューから「削除」を選ぶ。当該参加者は、以後このミーティングに参加できなくなります。
- ミーティングをロックする
  - 参加者ウィンドウの下の詳細メニューで「ミーティングをロックする」を選択すると、以後、新たにミーティングに参加することができなくなります。遅れて参加しようとした学生も参加できなくなりますので、注意してください。
- 参加者が画面共有できるかどうかを制御する
  - コントロールツールバーの「画面を共有」の右側にある「^」をクリックすると高度なオプションのメニューが表示されます。ここで画面を共有できるのは誰かを選択できます。
- 個々の参加者のビデオ送信を止める

- 参加者ウィンドウの個々の参加者名の横にあるビデオマークをクリックすることで、ビデオ送信を止めることができます。

・ 全参加者をミュートし、ミュート解除できないようにする

- 参加者ウィンドウの下の「すべてミュート」をクリックします。現れるメニューで、「参加者に自分のミュート解除を許可します」のチェックを外して「はい」を選択します。補助者（共同ホスト）がこの操作を行うと、ホストもミュートされますので注意してください。

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
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)）

前項のインストーラを利用して、攻撃者が直接Macを操作することで、管理者権限の操作が行える脆弱性が存在	Techcrunch	Mac：当該Macを操作できなければ攻撃できない	修正済み（April 2, 2020 Version 4.6.9 (19273.0402)）
攻撃者が直接Macを操作することで、カメラとマイクにアクセスできる。	Techcrunch	Mac：当該Macを操作できなければ攻撃できない	修正済み（April 2, 2020 Version 4.6.9 (19273.0402)）
Macに秘密裏にウェブサーバーをインストールしていた	Gigazine		2019年7月の出来事で、Apple, Zoom双方のアップデートにより修正済み
Facebookアカウントを持っていない人のデータもFacebookに送っていた	Gigazine	iOS: ユーザ情報をユーザに無断でFacebookに送信	修正済み（March 27, 2020 version 4.6.9 (19213.0327)）
Zoomの「出席者追跡機能」を有効にすると、会議のホスト役は通話相手がPCの前から離れているかどうかを確認できる。プライバシー侵害との指摘。	Gigazine	参加者が Zoomから30秒以上視線をそらせている場合にホストに表示	当該機能は使用できなくなっている。
Zoomの画面共有機能などを用いてポルノ映像を見せるなどの嫌がらせ行為 Zoom bombing	Gigazine	いわゆる「荒らし」。Zoomの問題というより、使い方の問題。特にミーティングIDだけでパスワードがないと、9桁の数字が一致すれば入れてしまう。ランダムに番号を選んで試すケースも考えられる。	・パスワード付きミーティングにして、パスワード、ミーティングIDを外部に知られないようにする。 ・認証されているユーザしか参加できないようにする。 ・「荒らし」を受けた時の対応手段を周知しておく
Windowsでチャットへの UNC貼り付けを用いた攻撃に対する脆弱性	ZDNet	Windows: チャットにUNC(Universal Naminb Convention)を用いたパスを書くと、クリッカブルなハイパーリンクになり、これを誤ってクリックすることで認証情報を窃盗されたり任意の実行可能ファイルを起動されたりする可能性がある。	修正済み（April 2, 2020 Version 4.6.9 (19253.0401)）

Zoomの、プライベートのはずの録画を他者に見られてしまう。	Washington Post	外部の動画公開サイトにZoomから連携してアップロードする際に、あるルールで決められたファイル名が付く。どのようなファイル名の動画があり得るのか推定できてしまい、名前を知っていればアクセスできる場合は、外部の人間がプライベートなはずのZoom録画を視聴できてしまう。	Zoom外の外部サービスに録画を置くときだけ起きる。単にZoomの録画機能を使うだけなら（クラウドでもローカルでも）関係ない。 記事中にも"It does not affect videos that remain with Zoom's own system." と記載。
	Gigazine	https://gigazine.net/news/20200402-zoom-should-not-use/	
	Routers	https://jp.reuters.com/article/spacex-zoom-video-commn-idJPKBN21K160	
	Techcrunch	https://jp.techcrunch.com/2020/04/02/2020-04-01-zoom-doom/	
	ZDNet	https://japan.zdnet.com/article/35151756/	
	Washington Post	https://www.washingtonpost.com/technology/2020/04/03/thousands-zoom-video-calls-left-exposed-open-web/	