[2020/04/06 時点の Zoom についての Ver.]

［情報共有］ Zoom による遠隔授業・会議の際の情報セキュリティに関する留意点について

近日、メディア等にて不安視されている、遠隔会議用システム Zoom に関する留意点を情報セキュリティ本部・サイバーメディアセンター 全学支援企画部門にて纏めましたので、情報共有を差し上げます。

[安全に授業・会議を開催する為の諸設定]

以下、箇条書きにて留意点について情報共有させて戴きます。

・ミーティング ID クラッキング防止策を推奨します。

設定方法：ミーティング ID オプションを探し、[自動生成]を選択します。

・会議をパスワードで保護する事を推奨します。

設定方法：会議のスケジュール画面にて、[会議のパスワードを要求する]の横にあるチェックボックスをオンにします。

・ズーム待合室を作成することを推奨します。

主催者（教員）がログインするまで、学生達同士の会話を抑制する事もできます。参加者が通話にログインすると、カスタマイズ可能な待合室の画面が表示され、主催者が参加を許可するまで通話に参加できない機能があるのでこの設定を推奨します。

・画面共有のユーザを限定する事を推奨します。

Zoom の通話中に画面をハイジャックさせない為に、画面の共有を許可されているユーザのみが画面共有できる設定である事を確認してください。

設定方法：

○会議を始める前にこの設定を有効にする方法

Zoom Web ポータル（デスクトップアプリではない）に移動し、設定で[個人]> [設定]> [会議中（基本）]に移動して、画面共有を探し、ホストのみが共有できるオプションをチェックします。

○通話中にユーザを限定する設定方法

下部にあるホストコントロールを使用して、他のユーザーが画面を共有できないように設定。画面の共有の横にある上向きのニンジンの様なアイコンをクリックする。詳細共有オプションを選択し、主催者のみを許可することを選択する。

・参加者へのアノテーション機能を無効にする事を推奨します。

画面または画像を共有している間、Zoom には参加者が見たものに注釈を付けること

ができる優れた機能がありますが、この機能がハイジャック攻撃の対象となります。
設定方法：Web アカウントの[会議中（基本）]セクションで注釈機能を無効にします。

・会議から迷惑な参加者を追い出す事も可能です。

上記設定等を設定せずに通話を行わなければならない場合や、これらの機能を回避し、通話中にとても迷惑をかけたり悪戯を行ったりする者が居た場合、会議から追い出す事も可能です。

設定方法：

〇通話中の会議で誰かを追い出す操作

通話中に、右側の参加者ペインに移動します。迷惑な人の名前にカーソルを合わせ、オプションが表示されたら、[削除]を選択する。

☆デフォルトでは、追放されたゲストは再参加できません。

☆迷惑な人を間違えて追い出してしまっても、 再び参加させる設定ができます。

この機能を有効にするには、

Web ポータルに移動し、[設定]> [会議]> [会議中（基本）]に移動する。

[削除された参加者に再参加を許可する]という設定を切り替えておきます。

・主催者は参加者のカメラをオフにする事ができます。

誰かがビデオで不適切な行為を行っている場合、またはビデオに技術的な問題がある場合、主催者は参加者パネルを開き、その人の名前の横にあるビデオカメラアイコンをクリックし、参加者のカメラをオフにできます。

・参加者の画像やアニメーション GIF 等のファイル共有が不要な場合は無効化設定を推奨します。

Zoom ミーティングのチャットエリアでは、参加者は画像やアニメーション GIF などのファイルを共有できます。その機能が不要な場合、ファイル転送を無効にできます。この機能はデフォルトでオンになっているため、通話等を悪戯画像等で妨害されたくない場合は、積極的に無効にする事をお薦めします。

設定方法：自分の会議の場合は、Zoom Web アプリ（デスクトップアプリではありません）で[設定]を開きます。左側で、[個人]> [設定]に移動します。次に、[会議中（基本）]をクリックします。ファイル転送が表示されるまで、少し下にスクロールし、無効に設定できます。

・参加者同士の会話が不要な場合はプライベートチャットを抑制できます。

Zoom コールを主催している間に、 参加者の誰かがプライベートメッセージを送信して、別の参加者に嫌がらせをする可能性があります。または、参加者同士雑談し始めるかもしれません。 プライベートチャットを無効にすることでこれを防ぐことができます。プライベートチャットを無効にしても、パブリックチャットには影響しません。 パブリ

ックチャットには、通話中の全員が表示して参加できます。

・有料アカウントの場合、サインイン時に参加者を限定できます。

招待に使用したのと同じメールアドレスを使用してサインインする必要がある機能が使えます。

操作方法(例):認証プロファイルと呼ばれるオプションを探して、設定を有効にすると、会議に参加しようとする他のユーザーには、画面が承認された参加者専用であることを知らせる通知が画面に表示されます。

参考出展：https://www.pcmag.com/how-to/how-to-prevent-zoom-bombing
PC Magazine より。

[Zoom の脆弱性に関する情報共有]

・2019 年 7 月 17 日以前の Zoom の MACOS バージョンにリモートでコードが実行できてしまう脆弱性が見つかって、広く MAC ユーザに知れ渡ってしまった。(攻撃者が増える可能性がある。)

・Zoom の内部データのデバイスへの転送や個人情報の管理者への閲覧権限について、盟約されていない状況下で扱われている。と、プライバシーの漏洩が危険視されている。
Facebook アカウントで利用する時は要注意との事。(現在はパッチがあたっている。)

・Zoom に関する設定時の MacOS 標準で無いログインダイアログについては注意が必要。

・Zoom 利用時に攻撃することにより、root 権限にエスカレーションしてコードを実行できてしまうクラッキング手法も見つかっている。

・Zoom 利用時に攻撃することにより、コードインジェクションで Zoom を乗っ取れるクラッキング手法も見つかっている。

・Zoom で利用する Web カムのシステムに巣食う悪意を持ったプロキシー等を存在させることができる。(OS 上でサービスを監視する事で、詳しい知識を持っていれば、見つける事もできる。)

情報出展：(日本シーサート協議会の脅威情報 WG による情報共有より。)
Patrick W さんの blog を参考に。
https://objective-see.com/blog/blog_0x56.html