お客様各位

2020 年 4 月 6 日

ＮＥＣネッツエスアイ株式会社

「Zoom-Bombing」と呼ばれる事象への対処方法について

平素格別のご高配を賜り、厚く御礼申し上げます。
また共創ワークソリューション Zoom をご利用頂き、誠にありがとうございます。

昨今、「Zoom-Bombing」と呼ばれる愉快犯的な行為の発生が報告されています。
具体的には、Zoom を使ったオンライン会議や遠隔授業に第三者が参加し、不快な画像を表示するなどして会議の進行妨害、参加者に対する嫌がらせを行う行為となります。

このような行為に対しては、本来 Zoom サービスが備えている標準のセキュリティ設定の適用や、ミーティングの主催者（以降ホスト）が所定の操作を行うことにより、未然に回避することが可能です。

以下にその設定例を記載いたしますので、ご利用者様各位におかれましてはご参考にして頂き、より安全に Zoom ミーティングをご利用頂けますようお願い申し上げます。

1)報告されている事象：

・第三者が何らかの方法でミーティング ID を認知または類推することで、不正に Zoom ミーティングに参加し、画面共有やチャット等の利用により不快な画像、文言を参加者の端末に表示させる。

・攻撃対象となりうる Zoom ミーティング：

・下記「対処方法１～４」に例示するいずれかのセキュリティ設定を行っておらず、ミーティング ID が何らかの方法により認知・類推された Zoom ミーティング

※ミーティング ID の認知・類推を防ぐ手段については、後述 3)の推奨対策例をご参照ください。

2)弊社にて推奨する対処方法

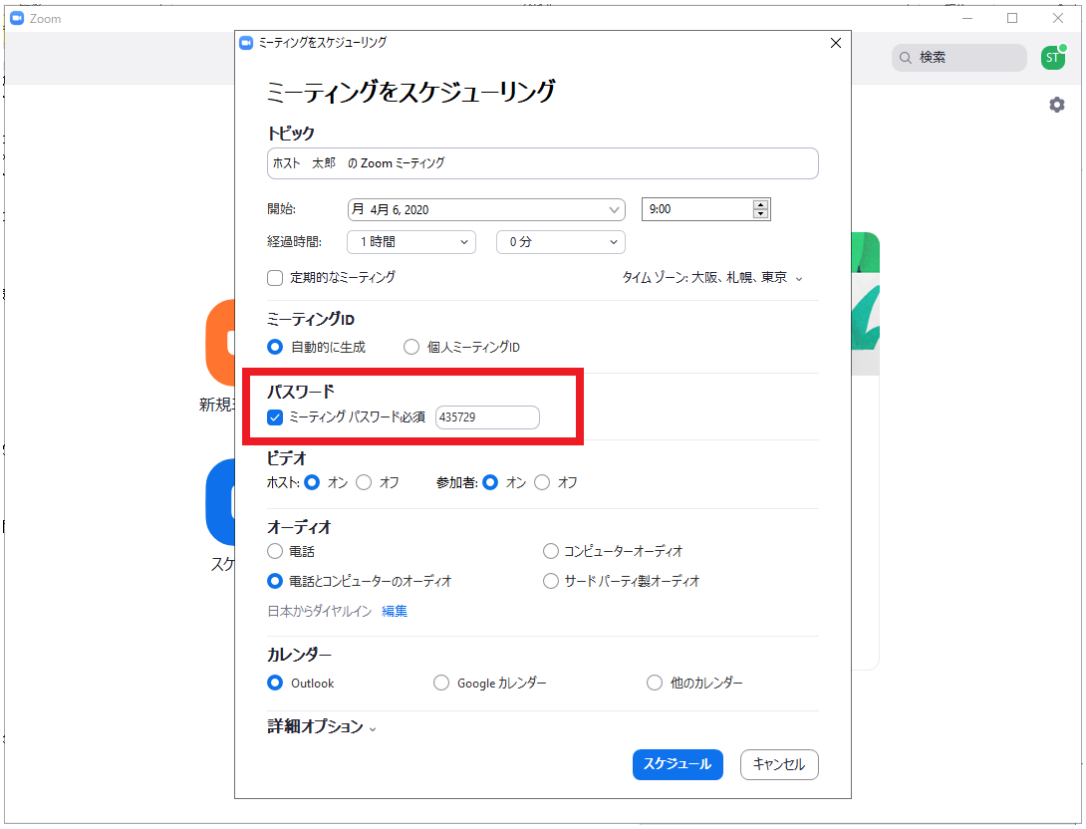
下記のいずれか一つの対処を行うことにより、Zoom-Bombing を未然に防ぐことが可能です。

・対処方法１：

ホストが Zoom ミーティングをスケジュールする際に、パスワードを設定する。

Zoom アプリケーションにログイン後、「スケジュール」を開き、「パスワード」にて「ミーティング パスワード必須」にチェックを入れます。

ランダムで設定されたパスワードが表示されますが、利用者側で変更が可能です。

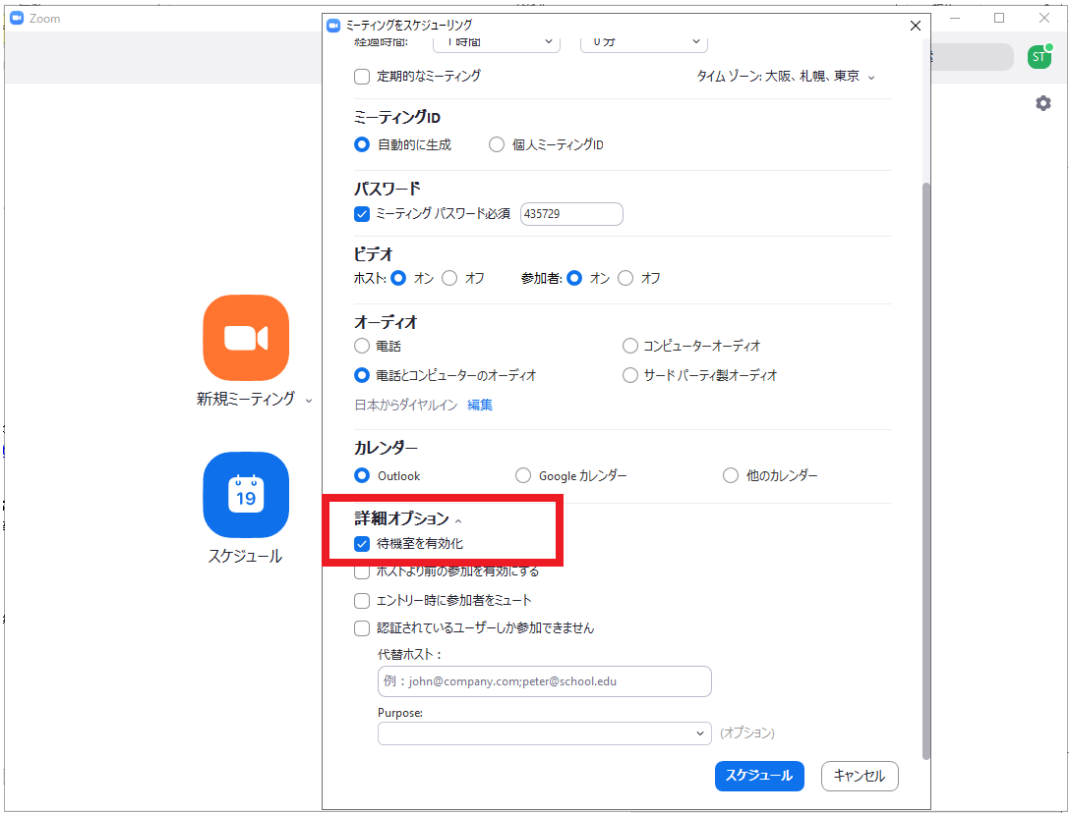


上記の対処により、参加者はミーティングへの参加時にパスワードの入力を求められるようになります。

・対処方法２：

ホストが Zoom ミーティングをスケジュールする際に、待機室機能を有効化する。

Zoom アプリケーションにログイン後、「スケジュール」を開き、「詳細オプション」にて「待機室を有効化」にチェックを入れます。



上記の対処により、参加者はミーティング ID を入力後、参加待ちの状態となり、主催者の許可によってはじめてミーティングに参加できるようになります。

・対処方法３：

ホストが、Zoom ミーティング開催中に「ミーティングをロックする」を実行する。

Zoom ミーティング中にアプリケーションのウィンドウ下部「参加者を管理」をクリックし、右下の「詳細」から「ミーティングをロックする」をクリックします。

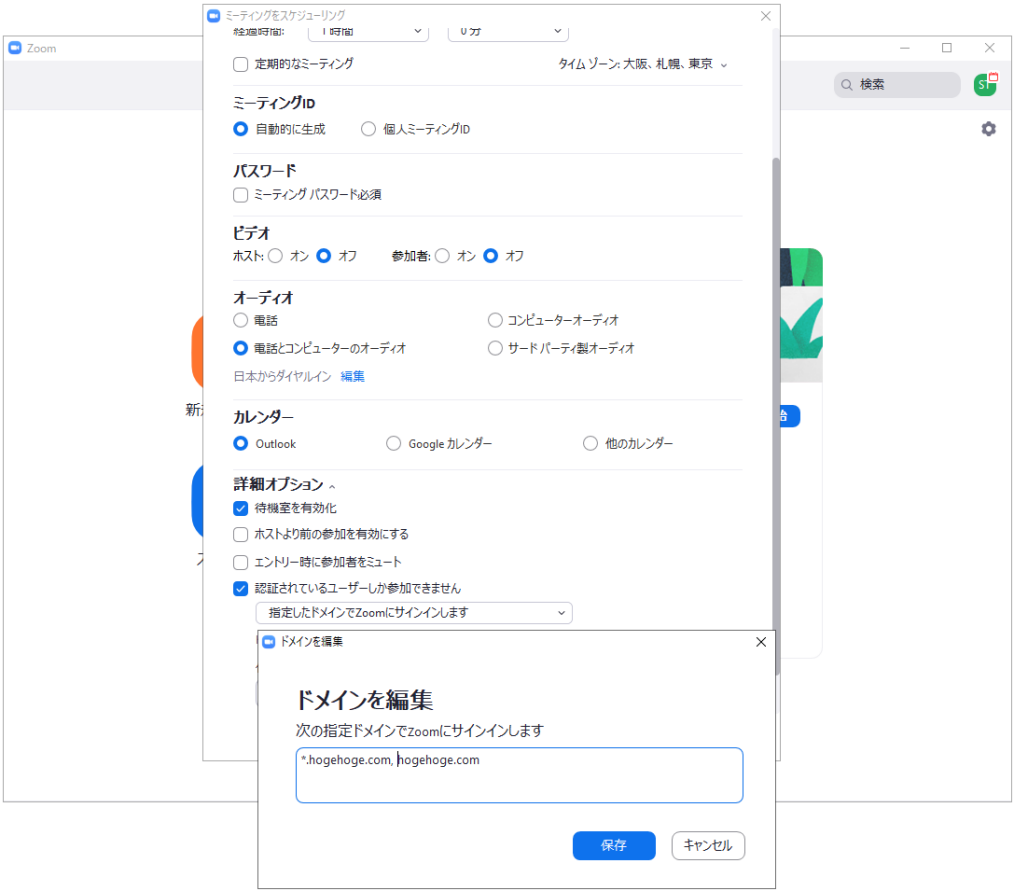
上記の対処により、ロック実施以降のミーティングへの参加を防止します。

（同様の操作により、ロック解除も可能です）

・対処方法４：

ホストが、Zoom ミーティングをスケジュールする際に、参加できるユーザーのドメインを指定する。

Zoom アプリケーションにログイン後、「スケジュール」を開き、「詳細オプション」にて「認証されているユーザーしか参加できません」にチェックを入れます。
その後「編集」をクリックし、参加させたいユーザーのドメインを“ , ”（カンマ）区切りで入力後、「保存」をクリックします。



上記の対処により、設定されたドメインを持つユーザーアカウント（メールアドレス）で Zoom アプリケーションにログインした参加者のみ、会議に参加することが可能です。

※上記対処方法１～４については、管理者権限にて Zoom アカウント全体に設定を有効化・強制することが可能です。
導入ユーザー様での利用ケースに応じ、適用する対処及び管理方法をご検討ください。
弊社で Zoom サービスをご契約のお客様は、契約者向けサイトにて管理者マニュアルをダウンロード願います。

3)ミーティング ID の認知・類推を防ぐ手段について

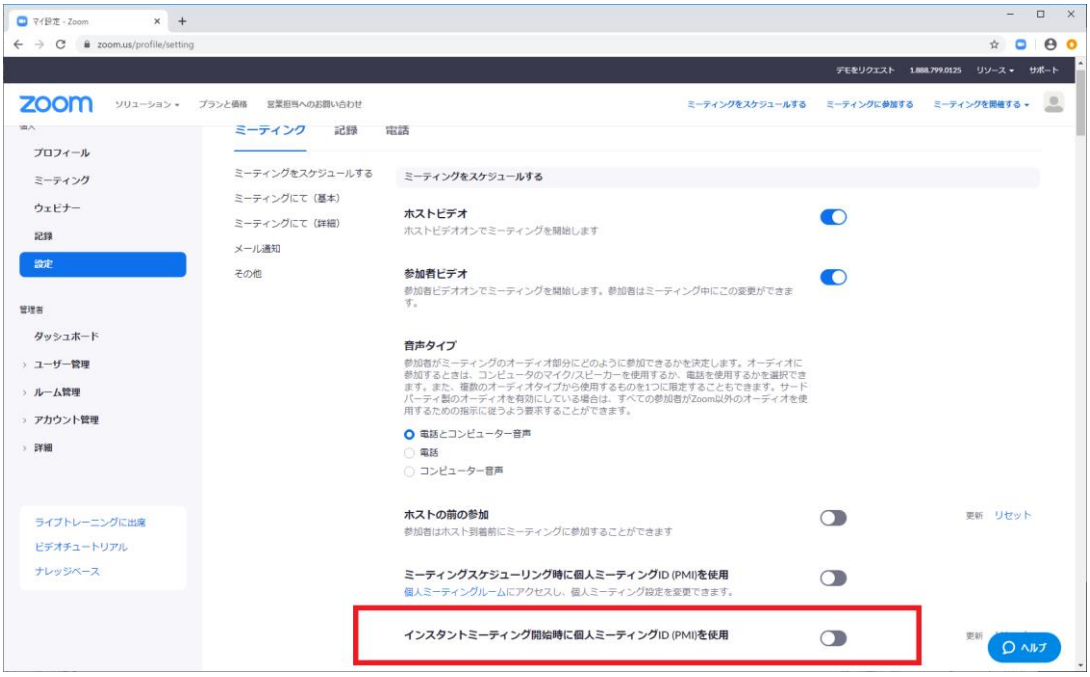
以下に例示する対策を推奨いたします。

・ミーティング ID を Web ページや SNS 等、第三者の目に触れる場所に記載せず参加者に個別に通知する**（最も重要です）**

・不特定多数が参加する可能性のあるミーティングに対し、パーソナル（個人）ミーティング ID を使用せず、スケジュールの際に自動的に生成する設定とする。

※インスタントミーティング（Zoom アプリケーション上で「新規ミーティング」をクリックすることで開始するミーティング）に対しても、自動的に生成する設定を適用することが可能です。

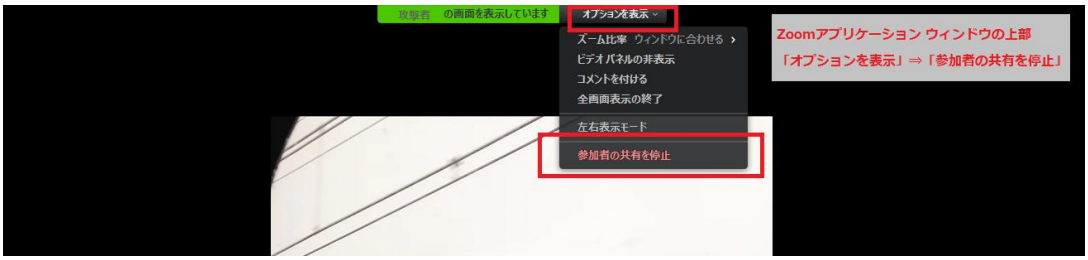
ホストが設定サイト https://zoom.us/profile/setting にサインインし、「インスタントミーティング開始時に個人ミーティング ID (PMI)を使用」項目を OFF（右側のスイッチをクリックして灰色に設定）します。



3)（ご参考）実際に Zoom-Bombing に遭遇した際の対処方法

上記のいずれの設定も行っていない場合に、Zoom-Bombing を停止させる方法を記載します。

ホスト（ミーティング主催者）の操作により、画面の共有を停止させる。



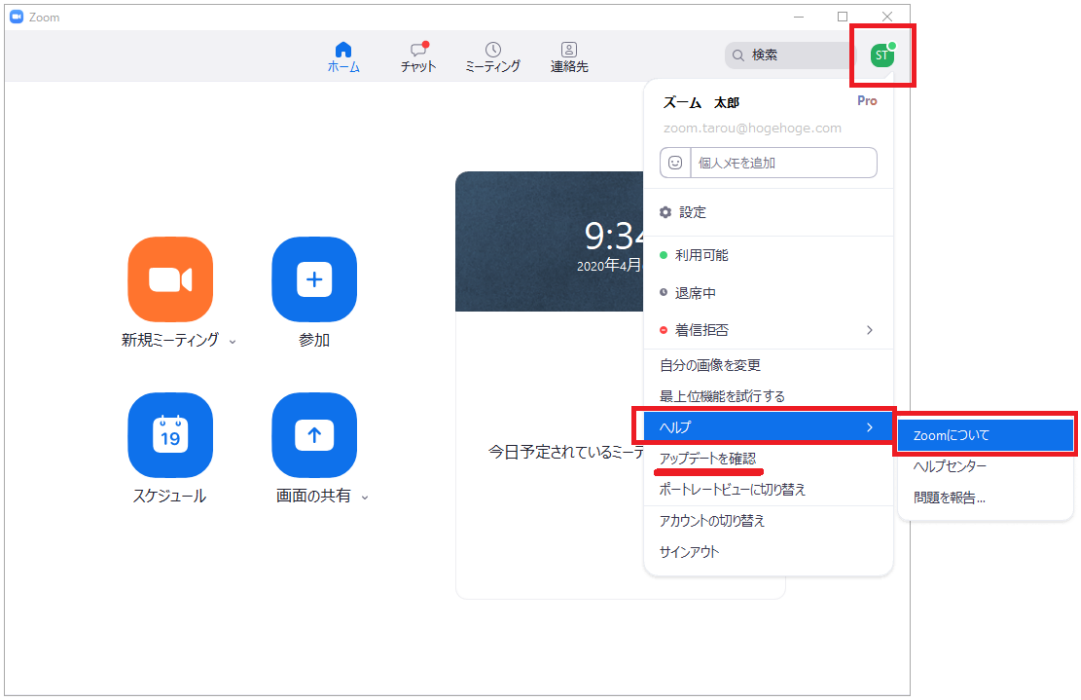
画面共有の停止後に、ホストの操作により「参加者」一覧から攻撃者を退室させる。

上記を実施後、前述の対処方法 3「ミーティングをロックする」を実施し、攻撃者の再度の入室を制限する。

現在、Zoom のセキュリティについては現在様々な報道がなされておりますが、サービス提供元である Zoom Video Communications, Inc (以降、米 Zoom 社)はその主たる 2 件の事象について、アプリケーションのバージョンアップによる対策を完了しております。お客様各位におかれましては、お使いの Zoom アプリケーションを最新版 Ver.4.6.9 にアップデートして頂けますようお願いいたします。

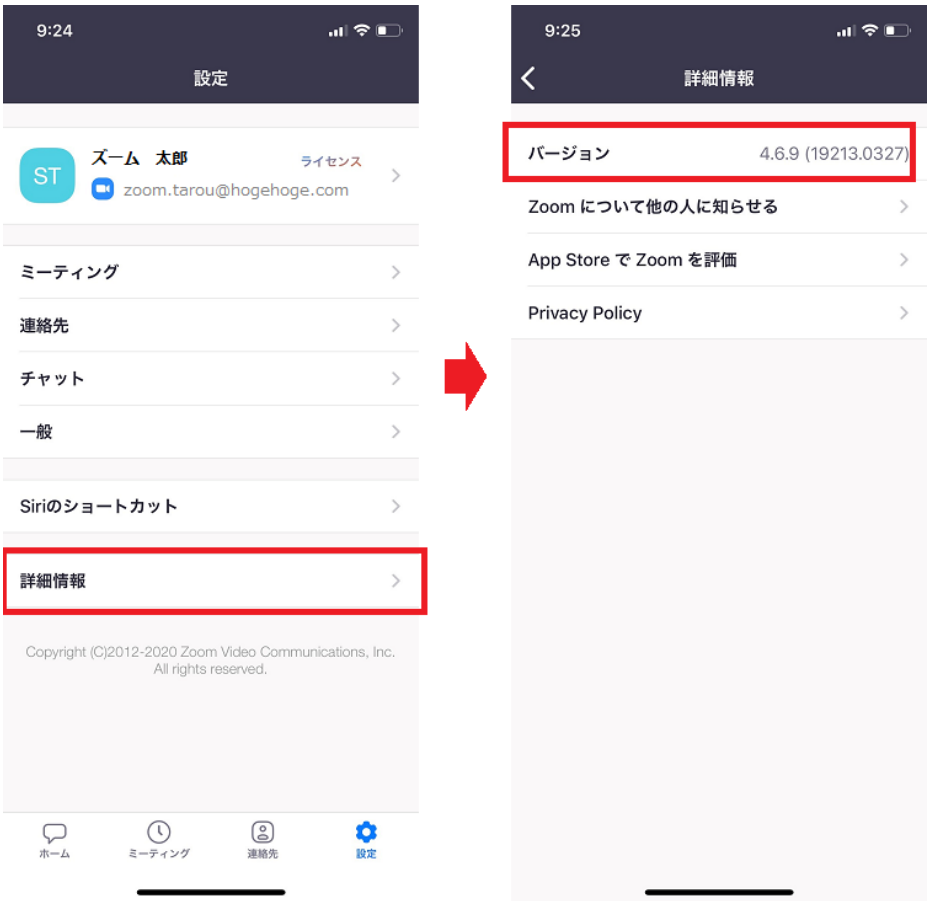
Zoom アプリケーションのバージョン確認方法

例）Windows の場合



※バージョンが 4.6.9 未満の場合は、「アップデートを確認」から更新が可能です。

例）iOS（iPhone）の場合



※バージョンが 4.6.9 未満の場合は、「App Store」から更新をお願いします。

ご参考：Zoom の iOS 及び Windows クライアントにおける脆弱性問題の対応について
https://symphonict.nesic.co.jp/zoom/notification-001/

なお、米 Zoom 社の Eric S. Yuan CEO は現地時間 2020 年 4 月 1 日、上記事象を含むセキュリティ上の懸念に対して声明を発表し、今後 90 日間は社内のリソースを集約しセキュリティ問題の修正に専念すると発表しています。

上記発表の詳細については、以下の URL をご参照ください。（英語）
https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/

また、最新のセキュリティポリシーについては、以下の URL をご参照ください。
https://zoom.us/jp-jp/privacy.html

弊社は今後も Zoom Video Communications, Inc 及び、その日本法人である ZVC Japan と連携し、より安全で快適なサービスをご提供できるよう努めてまいります。

以上