中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）関連資料

設定解説資料
（Zoom）

Ver2.2（2025.03）

本書は、総務省の調査研究事業により作成したものです。

本書に関する問い合わせ先（個別のシステムおよび環境に関する御質問については、製品の開発元にお問い合わせください。）
総務省 サイバーセキュリティ統括官室
Email telework-security@ml.soumu.go.jp
URL https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

目次

1 はじめに

(ア) 本書の目的

本書は、「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」の第 2 部に記載されているチェックリスト項目について、Zoom を利用しての具体的な作業内容の解説をすることで、管理者が実施すべき設定作業や利用者が利用時に実施すべき作業の理解を助けることを目的としています。

(イ) 前提条件

本製品（Zoom）のライセンス形態には「Basic（無償）」「Pro（有償）」「Business（有償）」「Enterprise（有償）」などが存在します。（2024 年 11 月 5 日現在）利用するライセンス形態により使用できる機能が異なります。**本資料は小規模チーム向けの「Pro」ライセンスの利用を前提としております。**

(ウ) 本書の活用方法

本書は、中小企業のセキュリティ管理担当者やシステム管理担当者（これらに準ずる役割を担っている方を含みます）を対象として、その方々がチェックリスト項目の具体的な対策を把握できるよう、第 2 章ではチェックリスト項目に紐づけて解説内容と解説ページを記載しています。本書では第 3 章にて管理者向けに、第 4 章では利用者向けに設定手順や注意事項を記載しています。

表 1. 本書の全体構成

章題	概要
1 はじめに	本書を活用するための、目的、本書の前提条件、活用方法、免責事項を説明しています。
2 チェックリスト項目と設定解説の対応表	本書で解説するチェックリスト項目と、その項目に対応する設定作業手順および注意事項の解説が記載されたページを記載しています。
3 管理者向け設定作業	対象のチェックリスト項目に対する管理者向けの設定手順や注意事項を解説しています。
4 利用者向け作業	対象のチェックリスト項目に対する利用者向けの設定手順や注意事項を解説しています。

(エ) 免責事項

本資料は現状有姿でご利用者様に提供するものであり、明示であると黙示であることを問わず、正確性、商品性、有用性、ご利用者様の特定の目的に対する適合性を含むその他の保証を一切行うものではありません。本資料に掲載されている情報は、2024 年 11 月 5 日時点の各製品の操作画面を基に作成しており、その後の製品仕様の更新、追加、変更、削除もしくは部分改廃により、画面表示等に差異が生じる可能性があります。本資料は、初期出荷状態の製品を単体動作させている環境を利用して設定手順を解説しています。本製品をご利用者様の業務環境で利用する際には、本資料に掲載している設定により業務環境システムに影響がないかをご利用者様の責任にて確認の上、実施するようにしてください。本資料に掲載されている製品仕様・設定方法について不明点がありましたら、製品提供元へお問い合わせください。

2 チェックリスト項目に対応する設定作業一覧

本書で解説しているチェックリスト項目、対応する設定作業解説および注意事項が記載されているページは下記のとおりです。

表 2. チェックリスト項目と管理者向け設定作業の紐づけ

チェックリスト項目	対応する設定作業	ページ
3-3 アクセス制御・認可 **オンライン会議の主催者は、会議に招集した参加者なのかどうか、名前や顔を確認してから会議への参加を許可するよう周知する。**	・ミーティングの入退室設定	P.6
3-4 アクセス制御・認可 **オンライン会議に参加するためのパスワードの設定は、原則必須とし、URL と合わせて必要なメンバーだけに伝えるよう周知する。**	・ミーティングのパスワードポリシーの設定 ・安全なミーティング URL の発行	P.10 P.12
3-5 アクセス制御・認可 **オンライン会議の主催者は、会議に招集した覚えのない参加者の参加を許可しないよう周知する。**	・待機室の有効化	P.14
8-5 データ保護 **オンライン会議のタイトルや議題には重要情報を記載せず、会議の録画ファイルに対してはパスワードの設定や期間指定の自動削除等を実施するよう周知する。また、上記ルールは可能な限り設定を強制する。**	・ミーティングの録画設定	P.16

表３．チェックリスト項目と利用者向け作業の紐づけ

チェックリスト項目	対応する設定作業	ページ
3-3　アクセス制御・認可 **オンライン会議の主催者は、会議に招集した参加者なのかどうか、名前や顔を確認してから会議への参加を許可するよう周知する。**	・ミーティング時の本人確認	P.20
3-5　アクセス制御・認可 **オンライン会議の主催者は、会議に招集した覚えのない参加者の参加を許可しないよう周知する。**	・不適切な参加者の強制退室	P.21
4-1　物理セキュリティ **テレワーク端末にのぞき見防止フィルタを貼り付けるよう周知する。**	・第三者からの盗聴・のぞき見の対策	P.22
5-2　脆弱性管理 **テレワーク端末の OS やアプリケーションに対して最新のセキュリティアップデートを適用するよう周知する。**	・アプリケーションの最新化	P.22
6-1　通信暗号化 **Web メール、チャット、オンライン会議、クラウドストレージ等のクラウドサービスを利用する場合（特に ID・パスワード等の入力を求められる場合）は、暗号化された HTTPS 通信であること、接続先の URL が正しいことを確認するよう周知する。**	・HTTPS 通信の確認 ・サービス接続先の確認	P.23 P.23
8-5　データ保護 **オンライン会議のタイトルや議題には重要情報を記載せず、会議の録画ファイルに対してはパスワードの設定や期間指定の自動削除等を実施するよう周知する。また、上記ルールは可能な限り設定を強制する。**	・ミーティング情報の件名に機密情報の記載禁止 ・ミーティング録画ファイルの削除	P.23 P.24

3 管理者向け設定作業

ここでは「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」の第 2 部に記載されているチェックリスト項目のうち、本製品の管理者が実施すべき対策の設定手順や注意事項を記載します。

3-1　チェックリスト 3-3 への対応

3-1-1　ミーティングの入退室設定

この項目では、主催者が参加者の入退室をコントロール及び認識するための設定を行います。会議の途中で**不正な参加者が参加したときに、情報漏洩するリスクを低減**することができます。

主催者より先の入室を禁止する

外部出席者が、主催者の同意なしにスケジュール済みミーティングに加わり、ミーティングを自由に操作できないようにします。

【手順①】

Zoom（https://zoom.us/）にログインし、左ペイン「管理者」の「アカウント管理」内の「アカウント設定」をクリックすると、ミーティングに関連する設定画面が表示されます。

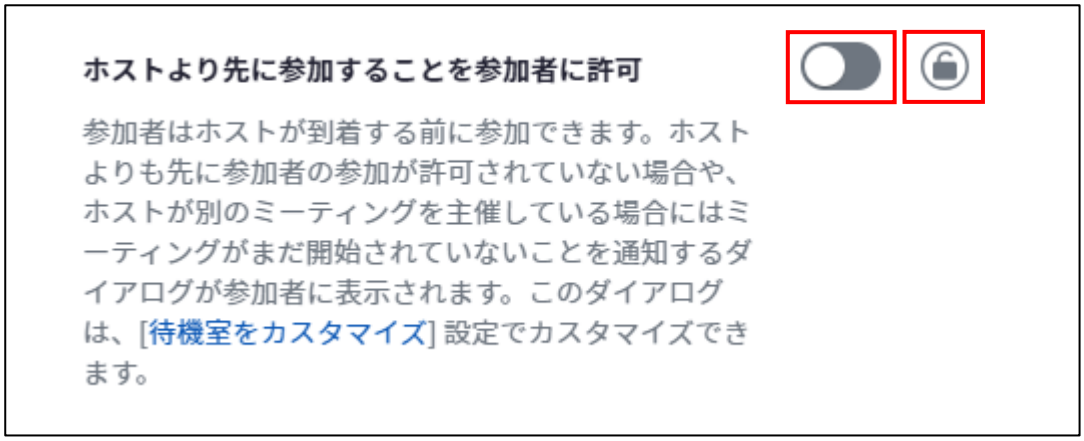
【手順②】

「ホストより先に参加することを参加者に許可」の項目まで下へスクロールします。

この設定はデフォルトで OFF になっていますが、ON になっていた場合は OFF へ変更します。

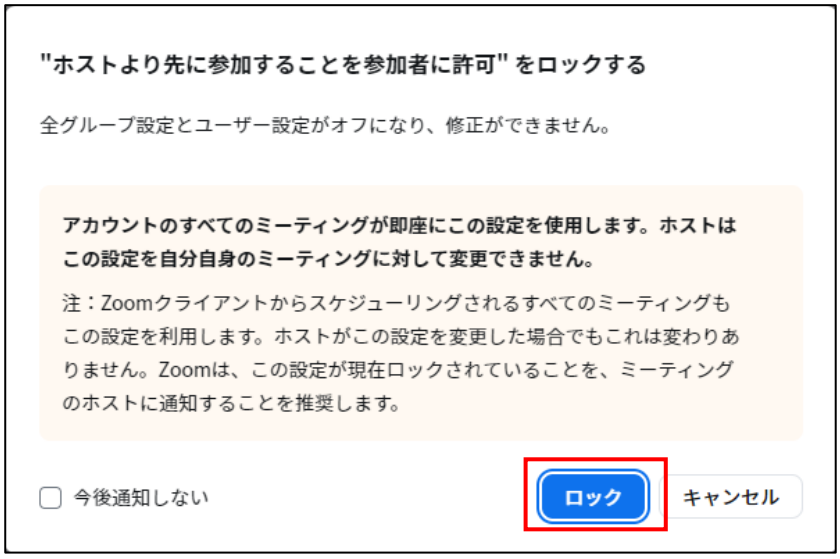
（以下の記載例は OFF の状態）

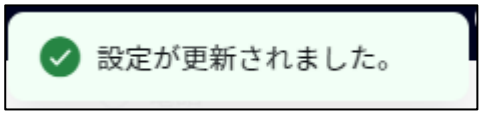
また、トグルボタンの右にある鍵マークをクリックしてロックすることで、管理者以外はこの設定の変更ができなくなります。



【手順③】

下記がポップアップされるため「ロック」をクリックします。





画面上部に「設定が更新されました」と表示されたら設定は完了です。

ユーザーの入退室通知の有効化

ミーティングに**不正ユーザーが参加した場合に気づくことができるように、ユーザーの入退室時の通知を有効化**します。この設定により、「不正ユーザー」に気付かず機密情報を漏洩してしまうリスクを低減させることができます。

【手順①】

Zoom（https://zoom.us/）にログインし、左ペイン「管理者」の「アカウント管理」内の「アカウント設定」をクリックすると、ミーティングに関連する設定画面が表示されます。

【手順②】

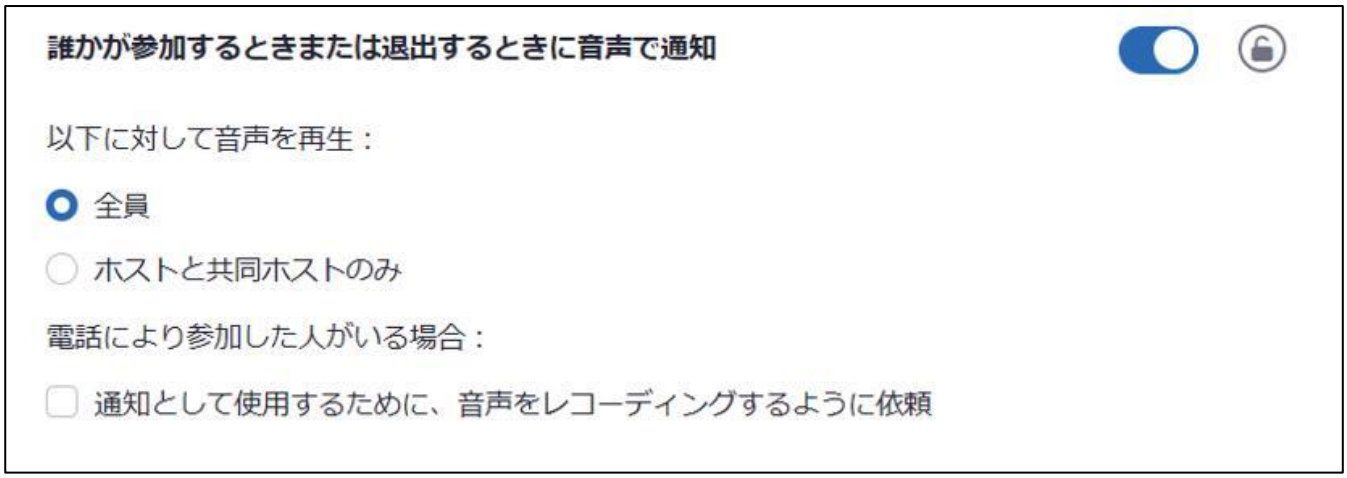
「誰かが参加するときまたは退出するときに音声で通知」の項目まで下へスクロールし、右側のトグルボタンをクリックし有効化します（デフォルトでこの機能はオフになっています。以下の記載例は OFF の状態）。

また、トグルボタンの右にある鍵マークをクリックしてロックすることで、管理者以外はこの設定の変更ができなくなります。

【手順③】

有効化すると、オプションの選択項目が表示され設定が完了します。

オプションは、参加者が少ない場合は「全員」に、参加者が多い場合は「ホストと共同ホストのみ」に設定することを推奨します。



3-2　チェックリスト 3-4 への対応

3-2-1　　ミーティングのパスワードポリシーの設定

ミーティングパスワードは**推測されにくい複雑なものを設定することにより、会議への不正アクセスを防止する有効な手段**となります。ここでは第三者に推測されにくいパスワードを設定するための設定方法を記載します。

より強力なパスワード設定（強度の設定）

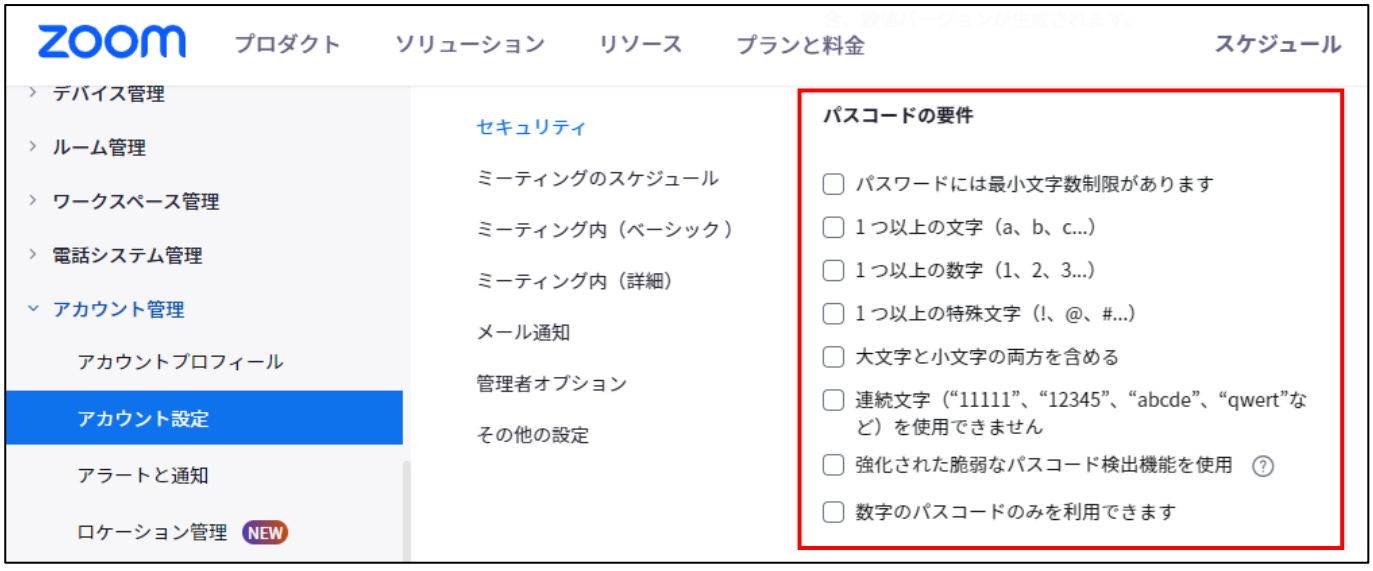
Zoom のミーティングで発行される、パスワードの設定条件を変更する方法を記載します。

【手順①】

Zoom（https://zoom.us/）にログインし、左ペイン「管理者」の「アカウント管理」内の「アカウント設定」をクリックするとミーティングに関連する設定画面が表示されます。

【手順②】

「パスコードの要件」の項目まで下へスクロールします。



【手順③】

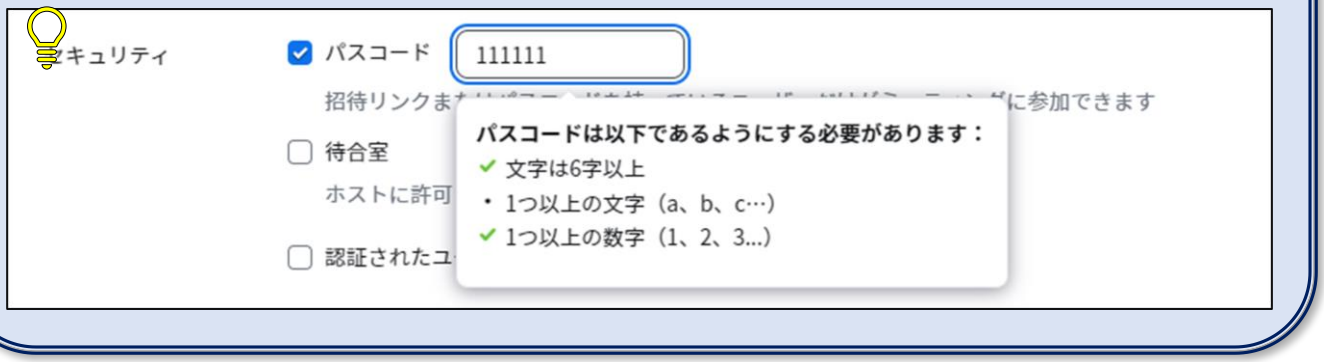
パスワードの設定条件にしたい項目のチェックボックスにチェックをし、最後に「保存」をクリックします。

（以下の記載例は、パスワードに６文字以上で１つ以上の文字と数字を含む条件を指定する設定）

画面上部に「設定が更新されました」と表示されたら設定は完了です。

参考　設定完了後の動作

ミーティングパスワードが設定した条件に当てはまらない場合は、以下のように会議が設定できなくなります



3-2-2　安全なミーティング URL の発行

Zoom では、ミーティングを設定する際にミーティング URL 内にパスワードを埋め込む機能がデフォルトで有効化されています。**ミーティング URL が流失してしまった場合に不正な利用者が参加してしまうリスクを低減するため、**この機能を **OFF** にします。

【手順①】

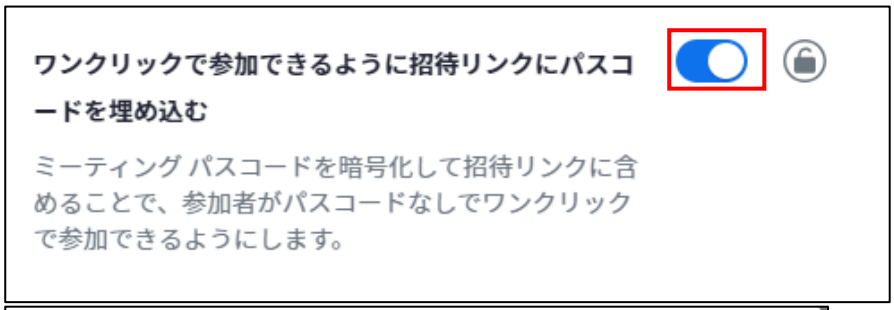
Zoom（https://zoom.us/）にログインし、左ペイン「管理者」の「アカウント管理」内の「アカウント設定」をクリックするとミーティングに関連する設定画面が表示されます。

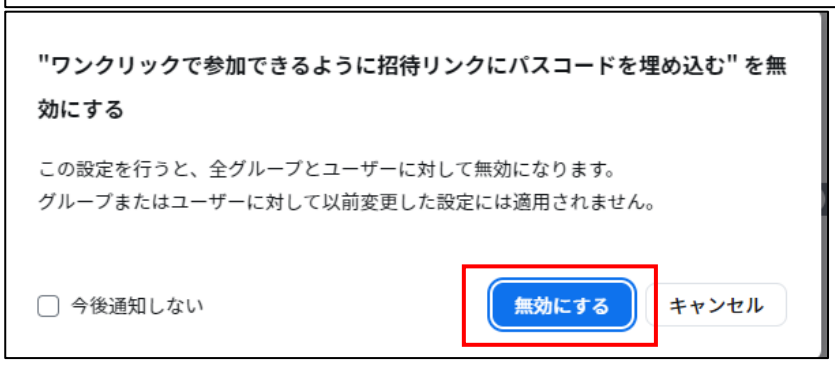
【手順②】

「ワンクリックで参加できるように招待リンクにパスコードを埋め込む」の項目まで下へスクロールします。

この設定は、デフォルトで有効化されているため、トグルボタンをクリックしオフにします。

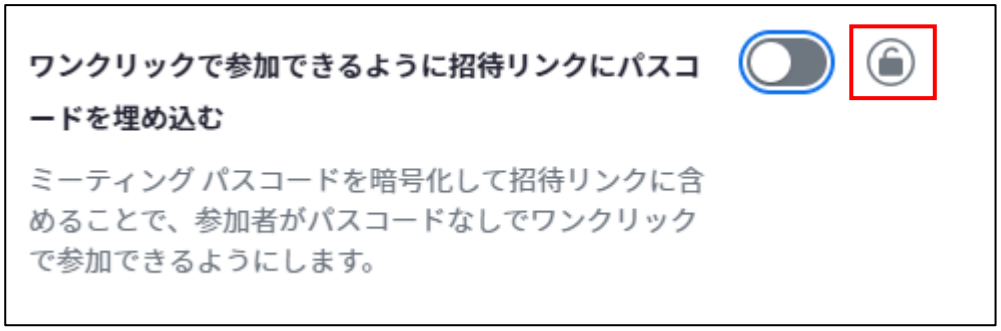
ポップアップされた内容から「無効にする」を選択します。



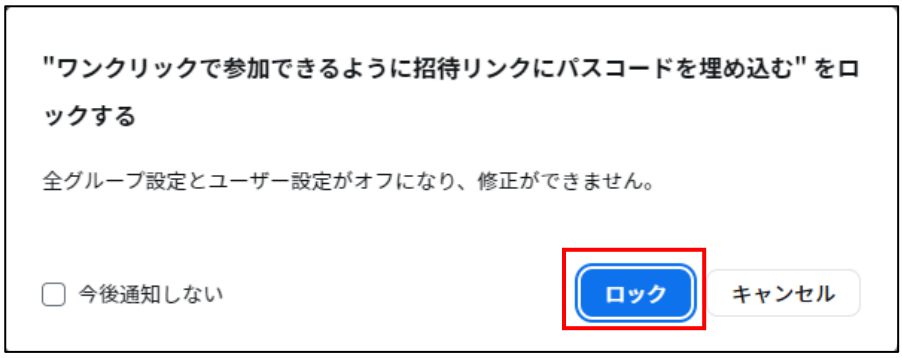


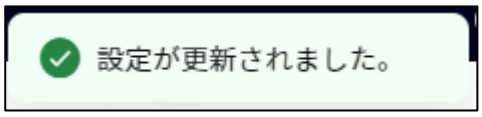
【手順③】

トグルボタンの右にある鍵マークをクリックし、設定をロックします。



下記がポップアップされるので「ロック」をクリックします。





画面上部に「設定が更新されました」と表示されたら設定は完了です。

3-3　チェックリスト 3-5 への対応

3-3-1　　待機室の有効化

待機室機能により、ホストはミーティングに参加する参加者を制御することができます。待機室は、参加者を直接会議に参加させず、一旦待機室に待機させ、主催者が参加を許可した場合にのみ、ミーティングに入室させる機能です。**想定していない参加者がミーティングに参加できないようにすることで、安全なミーティングを確保します**。

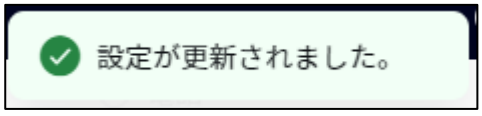
【手順①】

Zoom（https://zoom.us/）にログインし、左ペイン「管理者」の「アカウント管理」内の「アカウント設定」をクリックするとミーティングに関連する設定画面が表示されます。

【手順②】

「セキュリティ」の項目内に「待機室」という項目があります。右のトグルボタンをクリックし有効化します。

下記のようなポップアップが表示されるので「有効にする」を選択します。

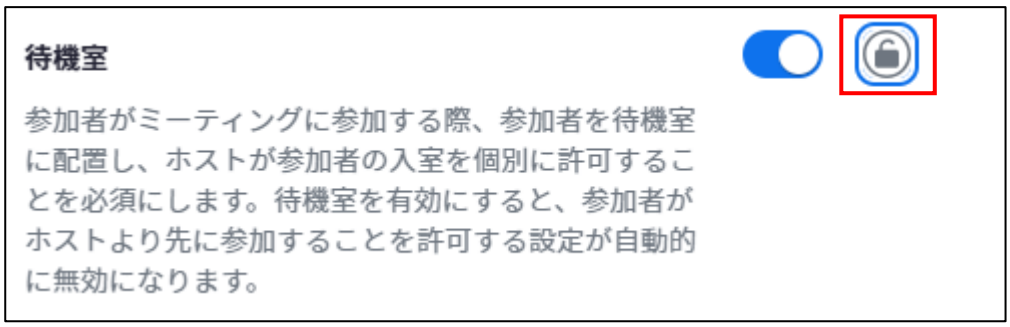


画面上部に「設定が更新されました」と表示されます。

【手順③】

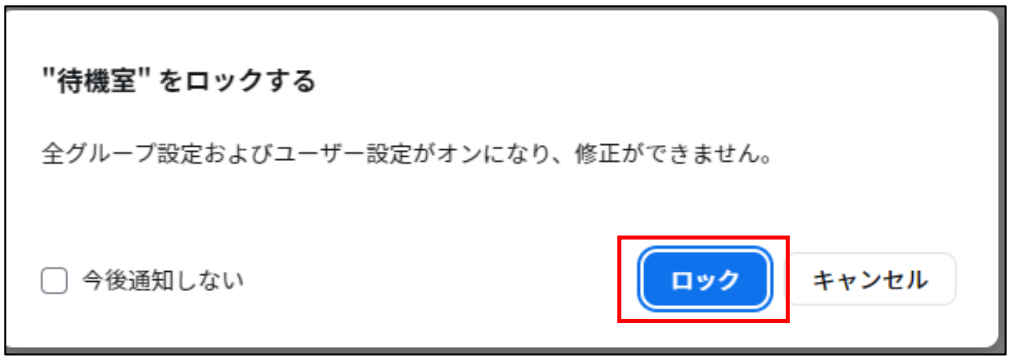
トグルボタンの右にある鍵マークをクリックし、設定をロックします。

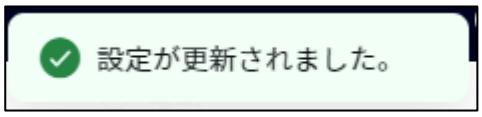
実行することで主催者は待機室を無効化できなくなります。



【手順④】

下記がポップアップされるので「ロック」をクリックします。





画面上部に再度「設定が更新されました」と表示されたら設定は完了です。

3-4　チェックリスト 8-5 への対応

3-4-1　　ミーティングの録画設定

ミーティングに参加していないメンバーが、録画データから**ミーティングの内容や目的等の情報を不正に取得するリスクを低減させる必要があります。**

録画ファイルのパスワード設定の強制

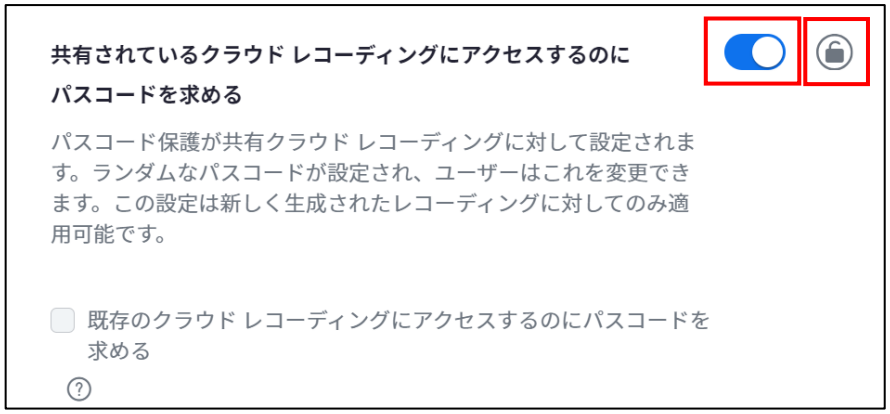
Zoom のクラウドに記録されたミーティングの動画に対してパスワード設定することを強制することで、ミーティングに参加していないメンバーが閲覧できないように設定します。

【手順①】

Zoom（https://zoom.us/）にログインし、左ペイン「管理者」の「アカウント管理」内の「アカウント設定」をクリック後、右ペイン上部の「レコーディングと文字起こし」タブをクリックします。

【手順②】

「共有されているクラウド レコーディングにアクセスするのにパスコードを求める」の項目まで下へスクロールします。
デフォルトで有効化されていますが、念のため設定が有効になっているかを確認します。　（以下、記載例は有効の状態）
また、右側にある鍵マークをクリックし、設定をロックします。

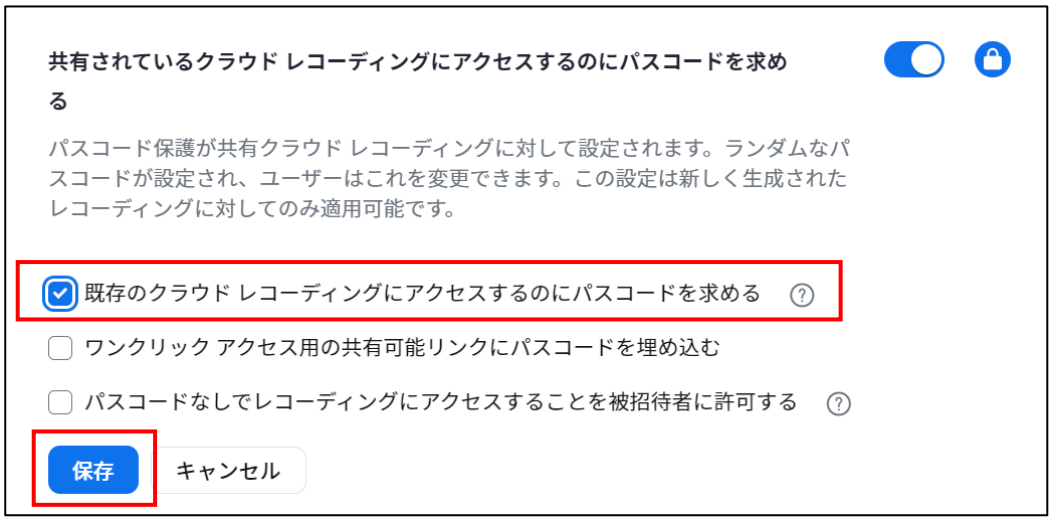


【手順③】ポップアップの「ロック」をクリック

下記がポップアップされるので「ロック」をクリックします。

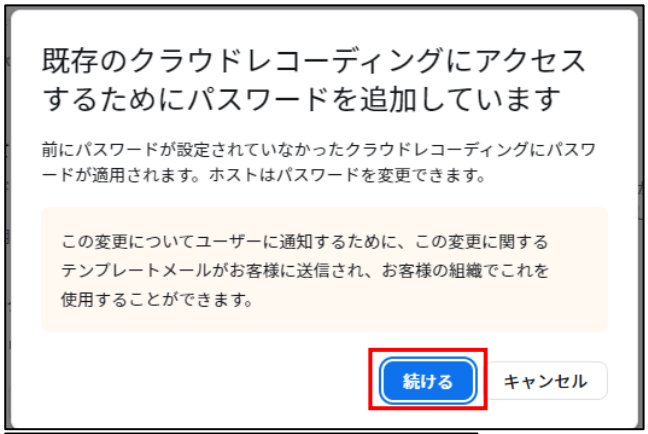
【手順④】

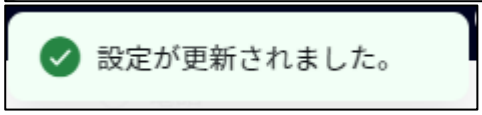
既にクラウドに記録されている録画ファイルにパスワードを付与する場合は、「既存のクラウドレコーディングにアクセスするにはパスコードが求める」という追加設定のチェックボックスにチェックを入れ、「保存」をクリックします。



【手順⑤】

下記がポップアップされるので「続ける」をクリックします。





画面上部に「設定が更新されました」と表示されたら設定は完了です。

録画ファイルの期日を指定した自動削除設定

不要になった機密情報が含まれるミーティング録画を自動削除するように設定することで、セキュリティリスクを低減することができます。

【手順①】

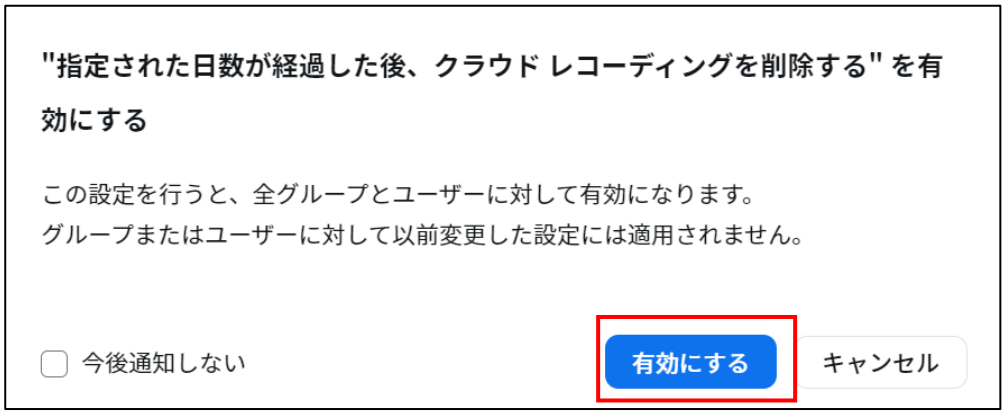
Zoom（https://zoom.us/）にログインし、左ペイン「管理者」の「アカウント管理」内の「アカウント設定」をクリック後、右ペイン上部の「レコーディングと文字起こし」タブをクリックします。

【手順②】

「指定された日数が経過された後、クラウドレコーディングを削除する」の項目まで下へスクロールします。
デフォルトはオフとなっているのでトグルボタンをクリックし有効化します。

【手順③】

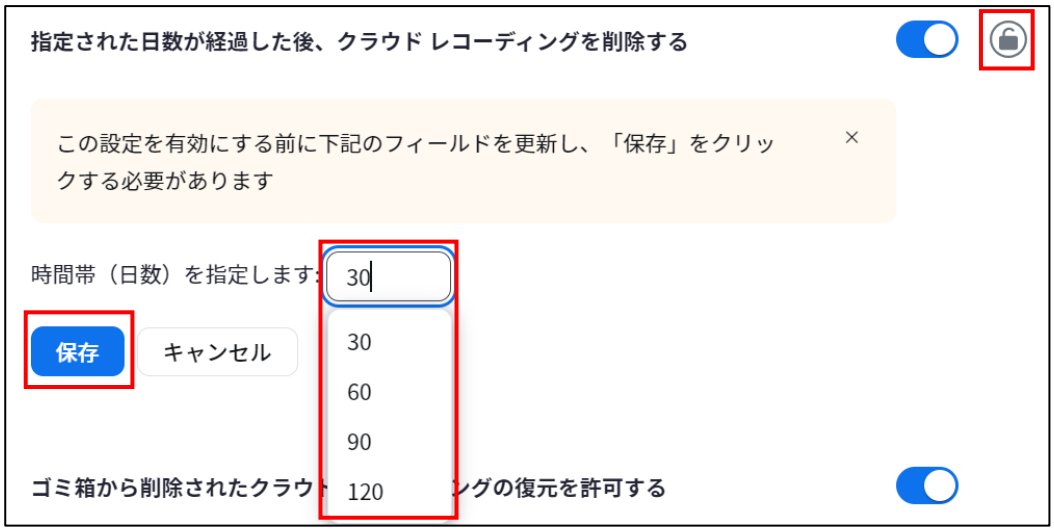
下記がポップアップされるので「有効にする」をクリックします。



【手順④】

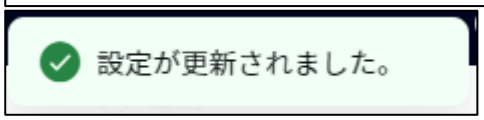
クラウド上に保管する日数を設定し、「保存」をクリックします。また、右側にある鍵マークをクリックし、設定をロックします。

（以下の記載例では 30 日後に削除）



【手順⑤】

下記がポップアップされたら「ロック」をクリックします。



画面上部に「設定が更新されました」と表示されたら設定は完了です。

４利用者向け作業

ここでは「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」の第２部に記載されているチェックリスト項目のうち、本製品の利用者が実施すべき対策の設定手順や注意事項を記載します。

４-１　チェックリスト 3-3 への対応

４-１-１　　ミーティング時の本人確認

ミーティングは、特別なアクセス制御を行わない限り**誰でも参加することができます**。また、ミーティング参加時の参加者としての表示名は、参加者側で自由に設定ができます。**なりすました不正ユーザー（※）が参加していないか確認するために、ミーティング開始時や途中参加者が入った場合はカメラの映像とマイクを有効化させ、映像と音声で本人確認することを推奨します**。

※　なりすましたユーザーによる機密情報の取得イメージ

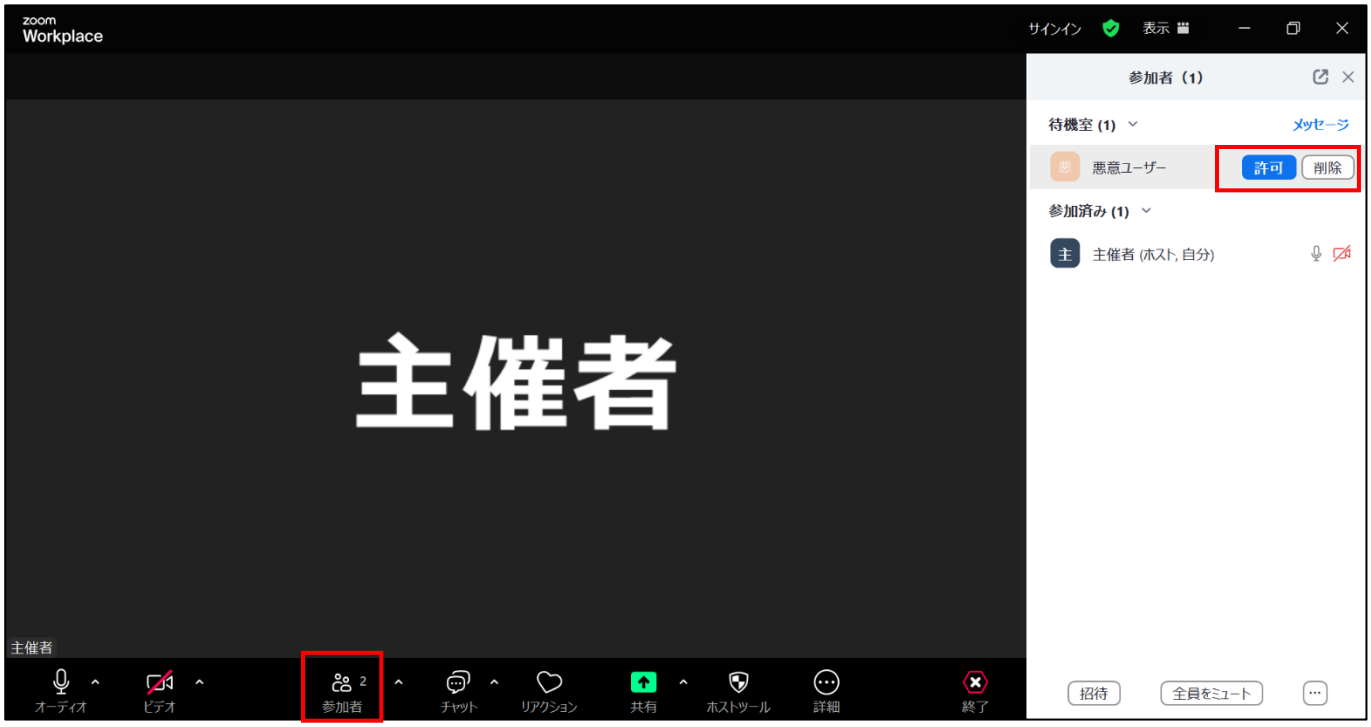
4-2　チェックリスト 3-5 への対応

4-2-1　　不適切な参加者の強制退室

Zoom の待機室には、URL やパスワードを知っていれば、**誰でも入室できてしまいます。**そのため主催者は、待機室内の参加者名を確認し、予め招待している参加者のみを許可するようにします。

【参加対象外メンバーの強制退室】

待機室の参加者を許可するにはミーティング画面の下部にある「参加者」をクリックします。
上部の「待機室」が待機しているユーザーの一覧で、下部の「参加済み」がミーティング参加者です。
待機室にいる参加者が参加対象であれば「許可」をクリックします。
対象メンバーでなければ「削除」をクリックすることで、待機室から強制退室させます。



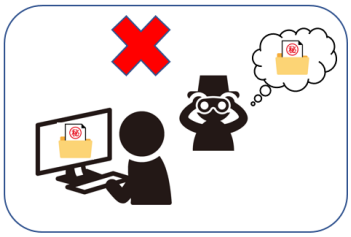
- **注意事項**

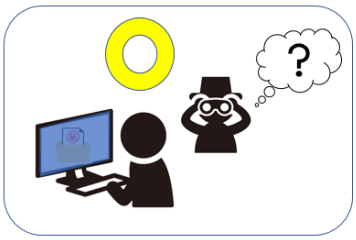
悪意のあるユーザーは名前をなりすまして参加する可能性があります。
可能であればミーティング冒頭で参加者のカメラ機能を有効化し、顔や音声で本人確認を実施することを推奨します。

4-3　チェックリスト 4-1 への対応

4-3-1　　第三者からの盗聴・のぞき見の対策

オフィス外で利用する場合は、第三者から盗聴・盗み見されないように注意する必要があります。端末上に投影されている会議資料などがのぞき見されないように**のぞき見防止フィルタを利用する**、会議音声が外部に漏れないようにイヤホンを利用する、など利用シーンにおいた対策が必要です。

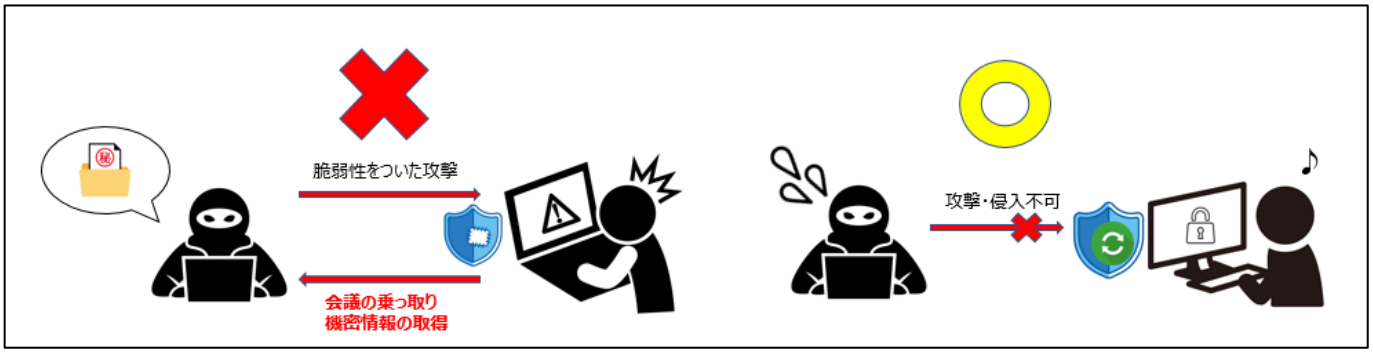




4-4　チェックリスト 5-2 への対応

4-4-1　　アプリケーションの最新化

製品提供元からリリースされている最新バージョンのアプリケーションを利用します。最新バージョンを利用することは、アプリケーションの**脆弱性をついたサイバー攻撃に対して有効な対策となる**ため、定期的にアップデートがないか確認をすることを推奨します。



Zoom の脆弱性について

Zoom は過去に脆弱性をついたサイバー攻撃の対象となった事例が報告されました。

既にアプリケーションのバージョンアップ対応にて解消しておりますが古いバージョンのままのユーザーがいない確認することを推奨します。

引用：IPA 情報処理推進機構 HP「Zoom の脆弱性対策について」より

URL: https://www.ipa.go.jp/archive/security/security-alert/2020/alert20200403.html

4-5　チェックリスト 6-1 への対応

4-5-1　　HTTPS 通信の確認

ユーザーがアクセスする Zoom での通信は基本的に HTTPS で暗号化されています。

4-5-2　　サービス接続先の確認

Zoom の URL として、第三者から共有されたものについては、**不正なアクセス先（Zoom のドメインではないケース等）でないことを確認する**ようにします。

また、**使用するアカウントが、個人アカウントではなく、業務利用アカウントを使用していることを確認し、Zoom にアクセスします。**

4-6　チェックリスト 8-5 への対応

ここでは、**ミーティング利用時に利用者（主催者）が注意すべき事項と設定**について記載します。

4-6-1　　ミーティング情報の件名に機密情報の記載禁止

会議名などに**機密情報が含まれている場合、間違った相手に招待メールを送信してしまうと情報漏洩してしまいます**。Zoom ではミーティングをスケジュールする際に、件名と議題を記載する項目がありますが、機密情報を記載せずに参加者同士が分かる内容で記載することを推奨します。

4-6-2　ミーティング録画ファイルの削除

不要になった録画ファイルは、適宜削除することを推奨します。不要になった録画ファイルを削除することで、**悪意のあるユーザーによる持ち出しやサイバー攻撃を受けた際の機密情報漏洩のリスクを低減することができます**。
「レコーディングと文字起こし」内の「クラウドレコーディング」から対象の会議を選択し、「その他（…）」のメニューから削除ができます。

【謝辞】

本設定解説資料の策定及び更新を行うにあたっては、ZVC JAPAN 株式会社の関係各所の方々に多大なるご協力をいただきました。この場をお借りして深く御礼申し上げます。