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）

ver1.0（2020.9.11）

本書は、総務省の令和２年度「テレワークセキュリティに係るチェックリスト策定に関する調査研究」事業（受託者：NRI セキュアテクノロジーズ株式会社）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を、Zoom を利用している環境で実現する際の具体的な作業内容の解説を行うことで、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する。

(イ) 前提条件

本製品のライセンス形態は「Basic（無償）」「Pro（有償）」「Business（有償）」「Enterprise（有償）」が存在します。（2020 年 8 月 1 日現在）

利用するライセンス種類により使用可能な機能が異なります。本資料で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(担当者ではないがこれらに準ずる役割を担っている方を含む)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することを助力するために、第 2 章にてチェックリスト項目に紐づく解説内容と解説ページを記載している。解説としては第 3 章にて管理者向けの設定手順を、第 4 章にて利用者向けの注意事項をそれぞれ記載している。

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、免責次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利用者向け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具体的な設定手順を解説しています。
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、2020 年 8 月 1 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

本書で解説するチェックリスト項目および対応する設定作業解説および利用者向け注意事項が記載されているページを示します。

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番号	対応する設定作業解説	ページ番号
3-3 アクセス制御（論理） **オンライン会議の主催者はミーティングの開始時および途中参加者が出た際に、参加者の本人確認を実施している。** **(クラウドサービス(オンライン会議)の利用がない場合は対象外)**	・ミーティングの入退室設定	P7
3-4 アクセス制御（論理） **オンライン会議にアクセスするための URL や会議参加のパスワードを不要なメンバーには伝えないようにしている。** **また、会議参加のパスワード設定を強制させることが可能な場合は、パスワード設定を強制している。** **(クラウドサービス(オンライン会議)の利用がない場合は対象外)**	・ミーティングのパスワードの設定と強度の強制	P10
3-5 アクセス制御（論理） **オンライン会議の主催者は必要に応じて不適切な参加者を退出させるなどし、会議を適切に進行している。** **(クラウドサービス(オンライン会議)の利用がない場合は対象外)**	・待機室の有効化	P14
8-5 データ保護 **オンライン会議を実施する際に、会議のタイトルや議題に重要情報を記載しないことや、会議の録画ファイルに対してパスワードの設定や期間指定の自動削除、等を実施している。上記のルールを強制することが可能な場合は、強制するように設定する。** **(クラウドサービス(オンライン会議)の利用がない場合は対象外)**	・ミーティングの録画設定	P16

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番号	対応する設定作業解説	ページ番号
3-3 アクセス制御（論理） **オンライン会議の主催者はミーティングの開始時および途中参加者が出た際に、参加者の本人確認を実施している。** **(クラウドサービス(オンライン会議)の利用がない場合は対象外)**	・ミーティング時の本人確認	P20
3-5 アクセス制御（論理） **オンライン会議の主催者は必要に応じて不適切な参加者を退出させるなどし、会議を適切に進行している。** **(クラウドサービス(オンライン会議)の利用がない場合は対象外)**	・不適切な参加者の強制退室	P21
4-1 アクセス制御（物理） **テレワーク端末に対して覗き見防止フィルタを貼付し、離席時にはスクリーンロックをかけるようルール化している。**	・第三者からの盗聴・覗き見の対策	P22
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ソフトウェアに対して最新のセキュリティアップデートを適用している。**	・アプリケーションの最新化	P22
8-5 データ保護 **オンライン会議を実施する際に、会議のタイトルや議題に重要情報を記載しないことや、会議の録画ファイルに対してパスワードの設定や期間指定の自動削除、等を実施している。上記のルールを強制することが可能な場合は、強制するように設定する。** **(クラウドサービス(オンライン会議)の利用がない場合は対象外)**	・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	P23

3 管理者向け設定作業

3-1 チェックリスト 3-3 に対応する設定作業

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します。
会議の途中で**不正な参加者が参加し情報漏洩するリスク低減**します。

主催者より先の入室を禁止する

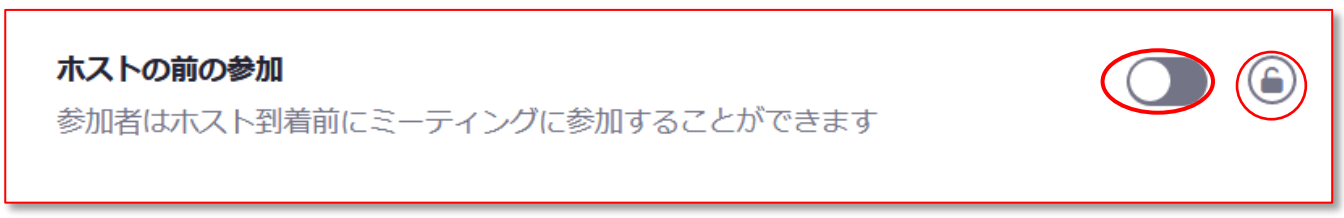
外部出席者が主催者の同意なしにスケジュール済みミーティングに加わりミーティングを自由に操作出来てしまうことを無効化します。

【手順①】

Zoom(https://zoom.us/)にログインし左ペインの「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】

「ホストの前の参加」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 になっているため ON になっていた場合は OFF へ変更**します。(以下、記載例は OFF の状態)
またトグルバーの右にある鍵マークをクリックしてロックします。



【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出来るように有効化**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します。

【手順①】Zoom のミーティング設定画面

Zoom(https://zoom.us/)にログインし左ペインの「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】

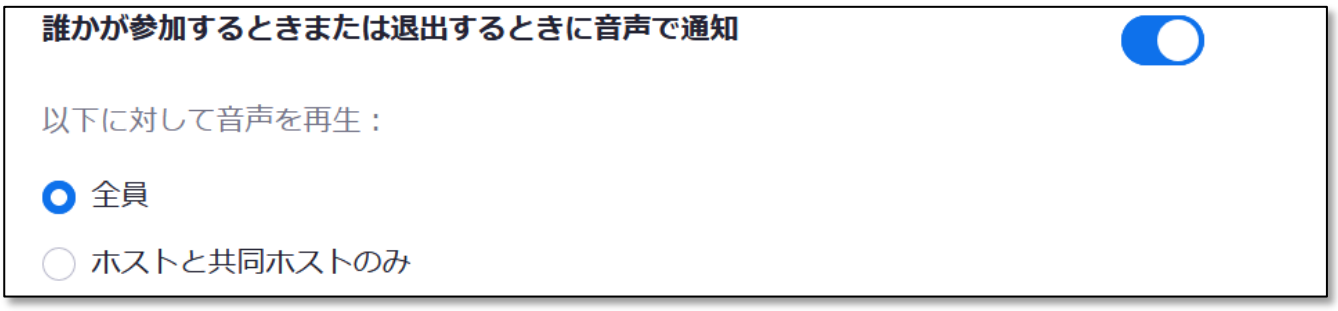
「誰かが参加するときまたは退出するときに音声で通知」の項目まで下へスクロールします。

デフォルトでこの機能はオフになっているためトグルボタンをクリックし有効化します。

【手順③】

有効化した際にオプションの選択項目が表示され設定が完了します。

参加者が少ない場合は全員に対して通知、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いたします。



3-2 チェックリスト 3-4 に対応する設定作業

3-2-1 ミーティングのパスワードの設定と強度の強制

ミーティングパスワードは**推測されな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**です。
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。

より安全なパスワード設定(強度の設定)

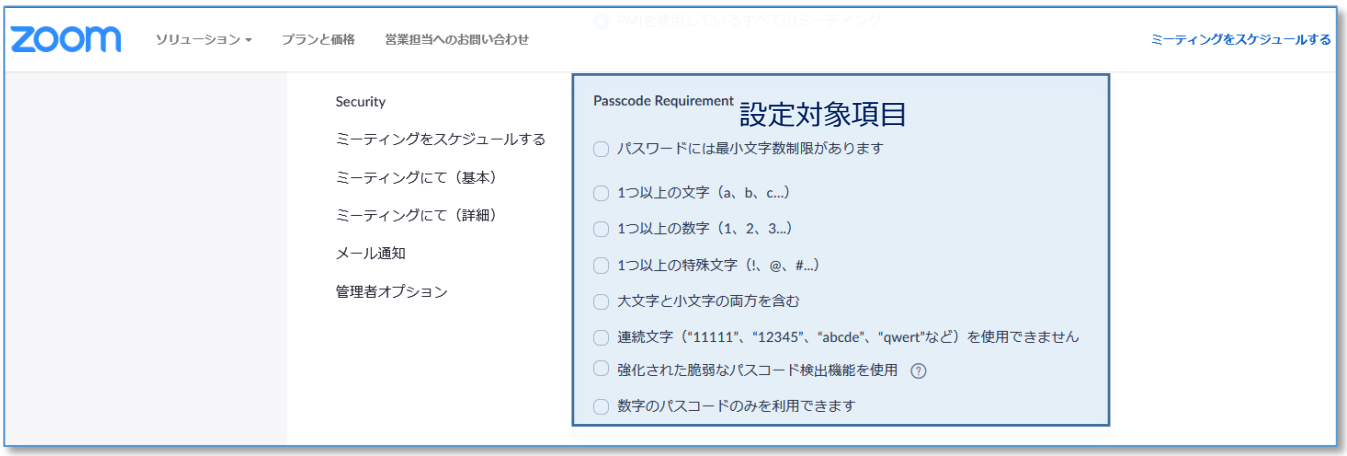
Zoom のミーティングで発行されるパスワードの設定条件について変更する方法を記載します。

【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】

「Passcode Requirement」の項目まで下へスクロールします。



【手順③】

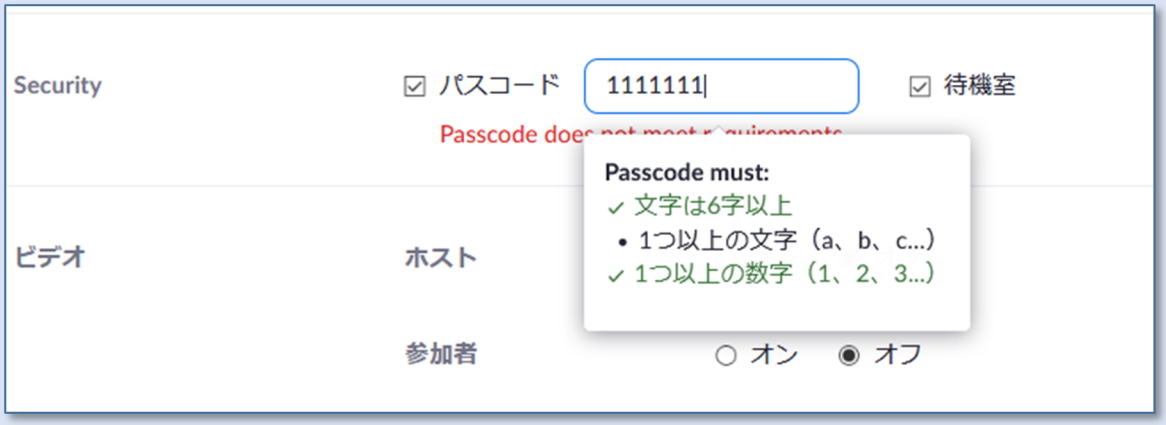
パスワード設定条件にしたい項目のチェックボックスにチェックをして最後に保存をクリックします。

以下、記載例は６文字以上で１つ以上の文字と数字を含む設定。

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条件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出来無くなります

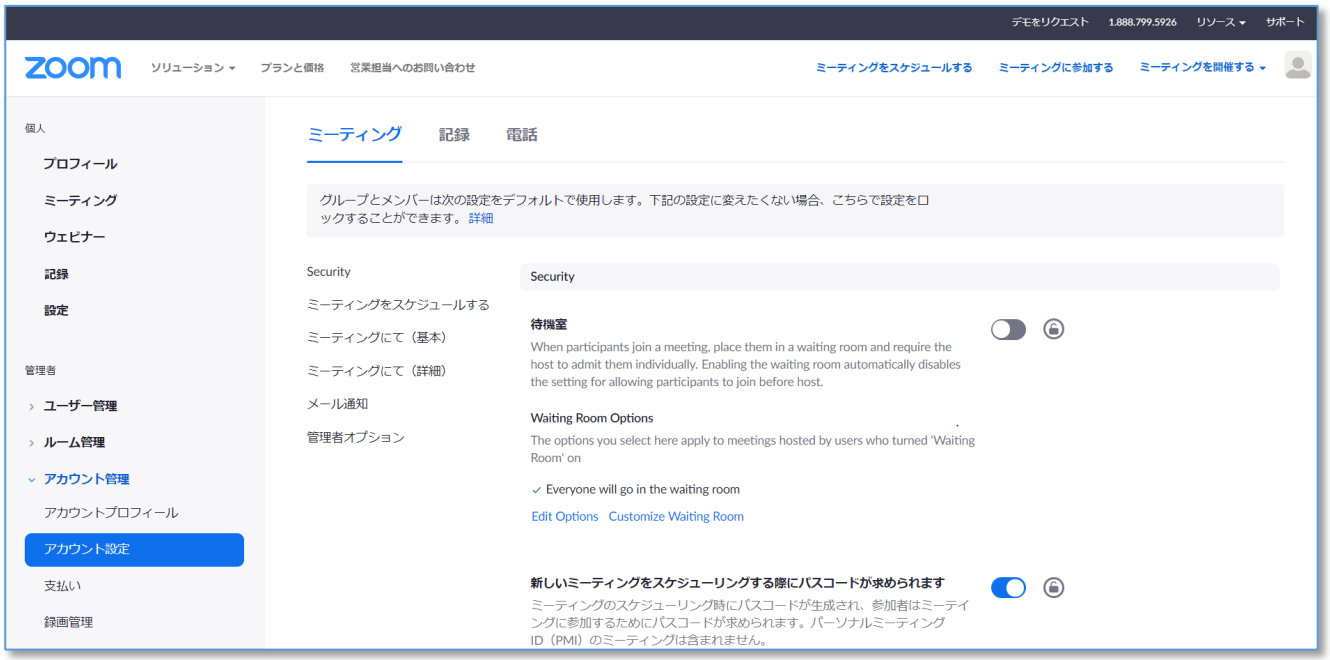


より安全なパスワード設定(パスワード埋め込みの禁止)

Zoom はデフォルトで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があるためこの機能を OFF します。

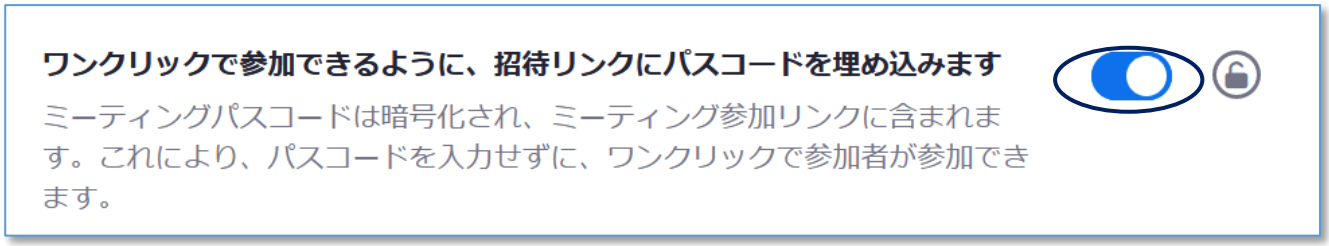
【手順①】Zoom のミーティング設定画面

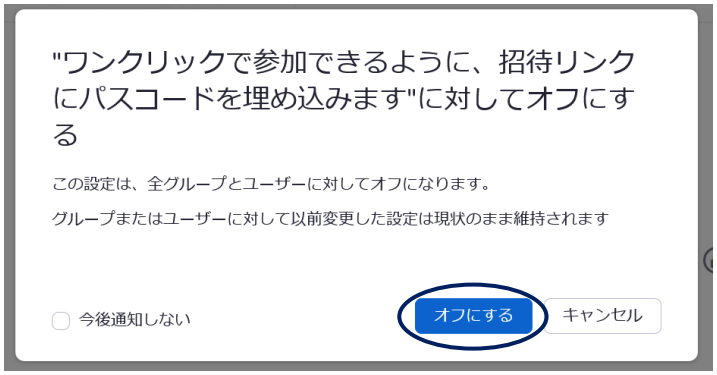
Zoom(https://zoom.us/)にログインし左ペインの「アカウント設定」をクリックするとミーティングに関連する設定画面が表示されます。



【手順②】

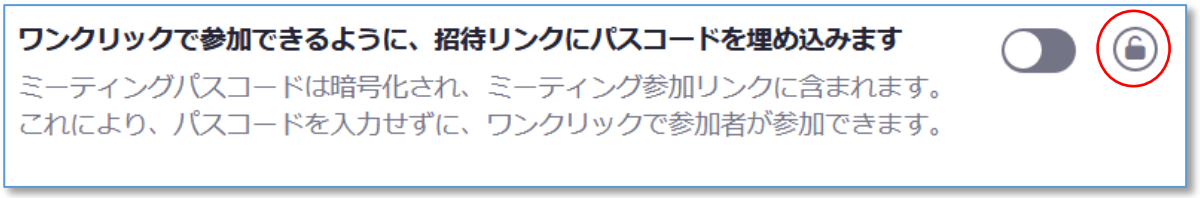
「ワンクリックで参加できるように、招待リンクにパスコードを埋め込みます」の項目まで下へスクロールします。
デフォルトで有効化されているのでトグルボタンをクリックし OFF します。
ポップアップされた内容から「オフにする」を選択します。





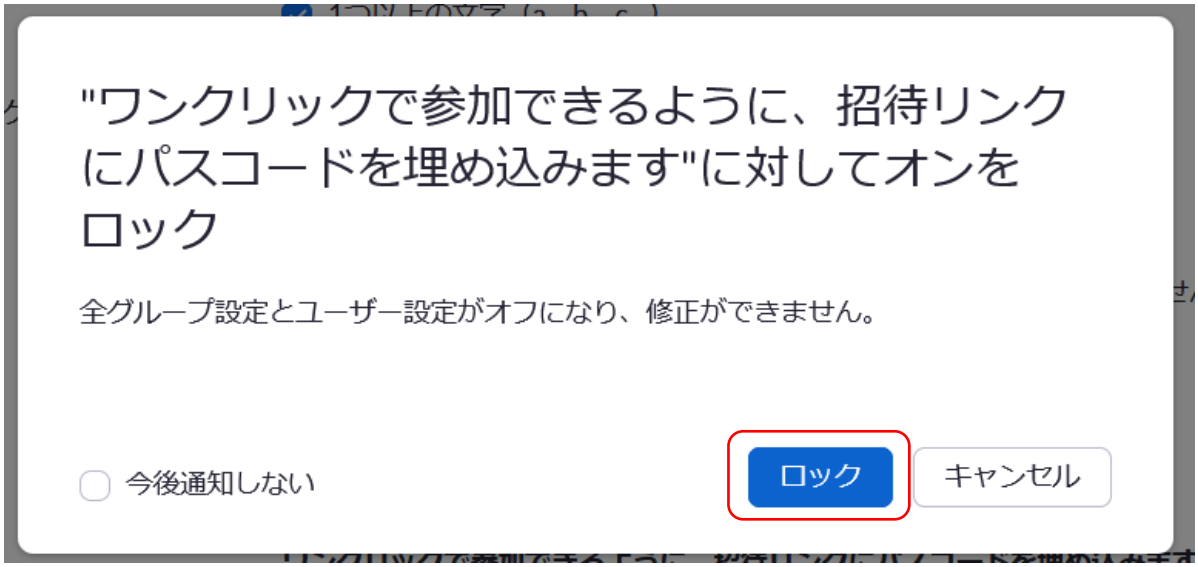
【手順③】

次に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。



【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「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 に対応する設定作業

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許可し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出来ないようにすることにより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】

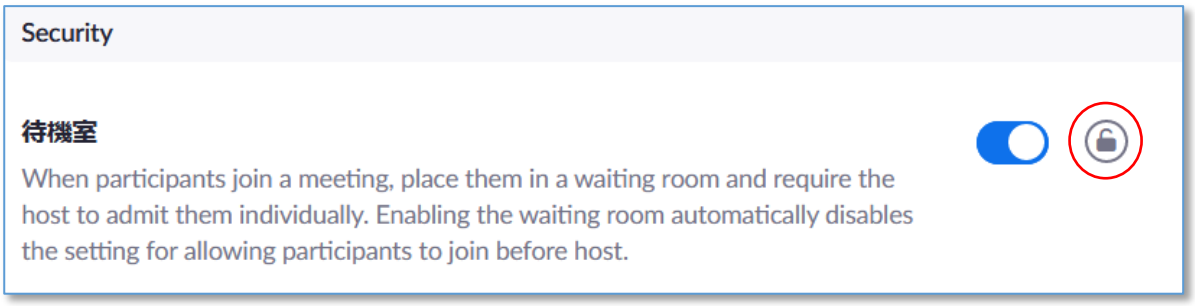
Security の項目の一番上に「待合室」という項目があります。右のトグルボタンをクリックし有効化します。
下記のようにポップアップが表示されますので「オンにする」を選択します。

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】

次に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。

実行することにより主催者は待機室を無効化することが不可となります。



【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 に対応する設定作業

3-4-1 ミーティングの録画設定

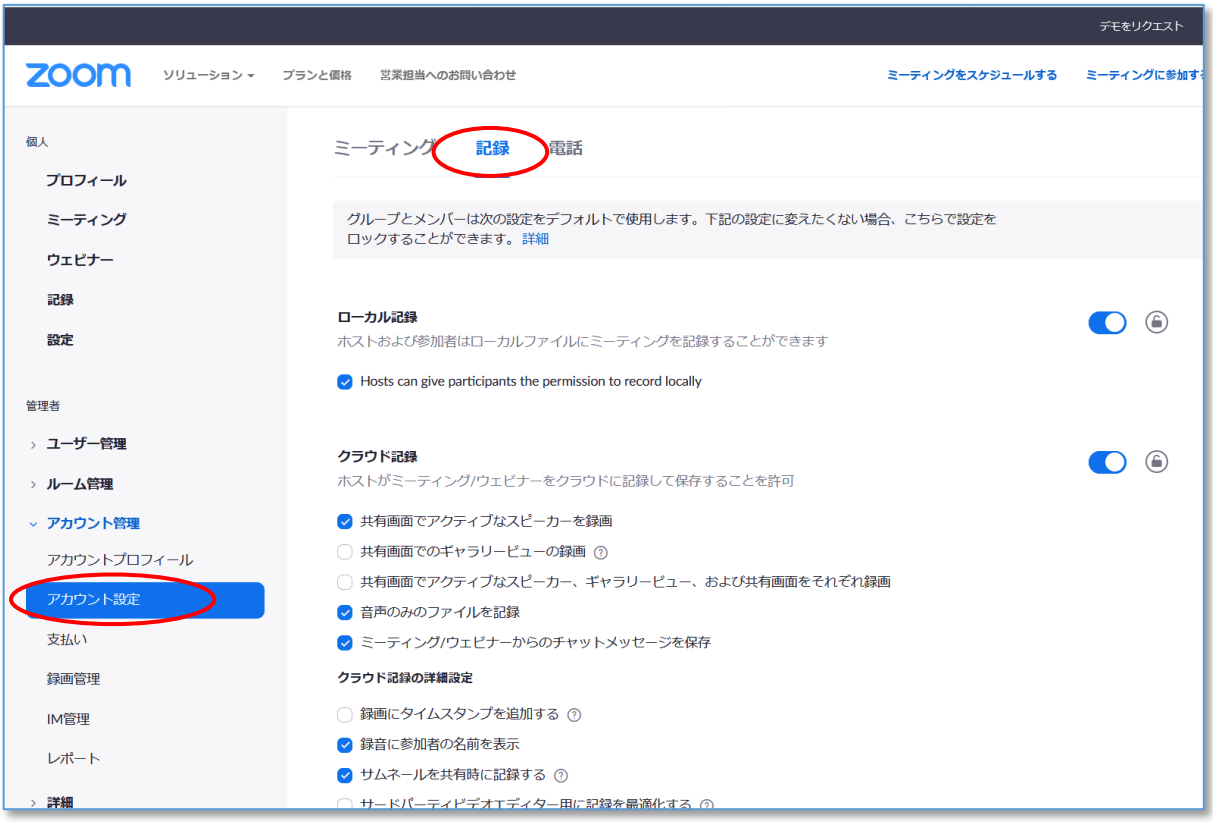
ミーティングに参加していないメンバーが、**ミーティングの内容や目的等の情報を不正に取得するリスクを低下**する必要があります。

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出来ないように設定します。

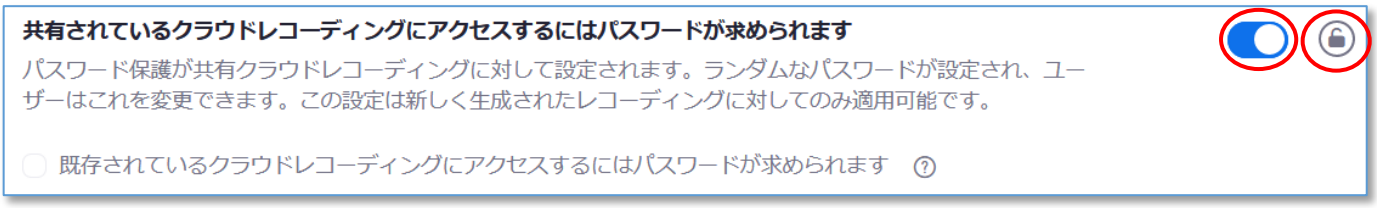
【手順①】

Zoom(https://zoom.us/)にログインし左ペインの「アカウント設定」をクリックし右ペイン上部の「記録」タブをクリックします。



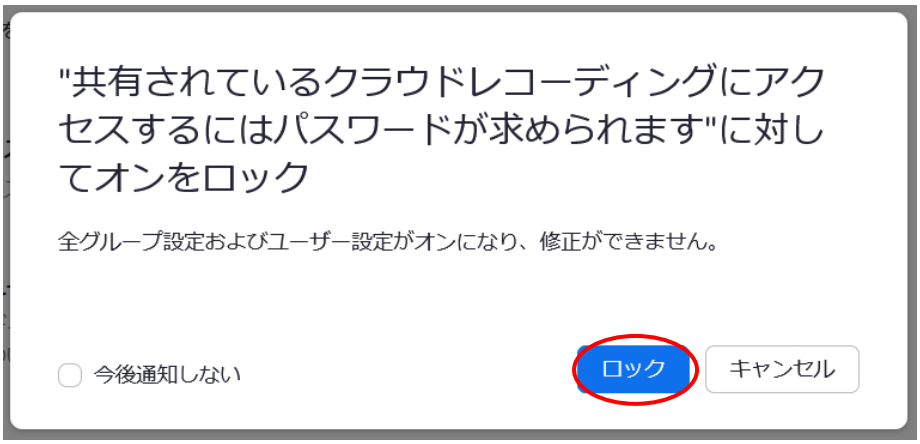
【手順②】

「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にはパスワードが求められます」の項目まで下へスクロールします。
デフォルトでオンのため設定が有効になっているか確認します。 (以下、記載例は有効の状態)
また右側にある施錠マークをクリックして設定にロックをかけます。



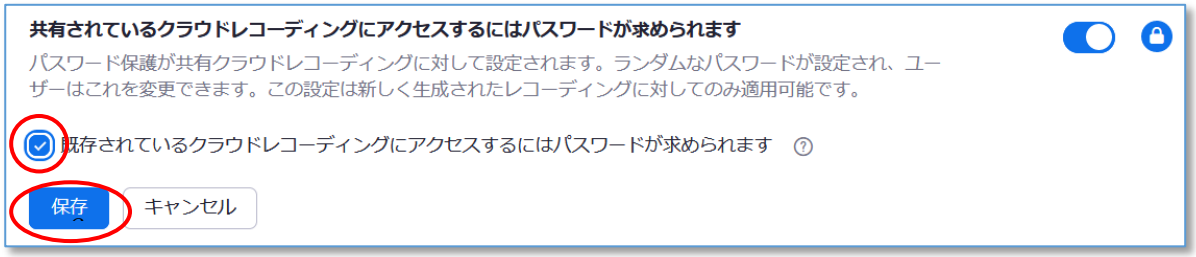
【手順③】

下記がポップアップされるので「ロック」をクリック。



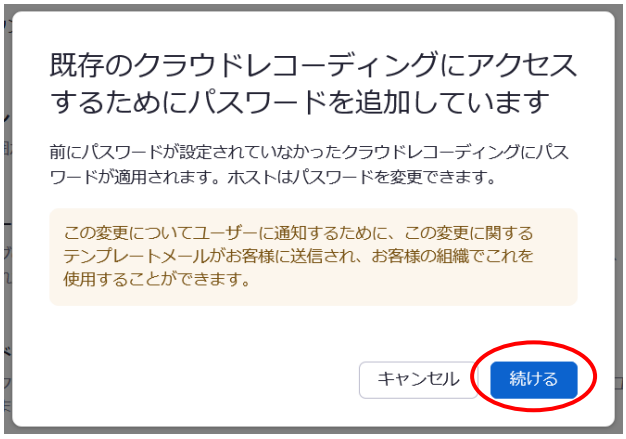
【手順④】

既にクラウドに記録されている録画ファイル対してパスワードを付与する場合は「既存されているクラウドレコーディングに～」という追加設定にチェックボックスにチェックを入れて「保存」をクリックします。(※1)



【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。



画面上部に上記が表示されましたら設定は完了です。

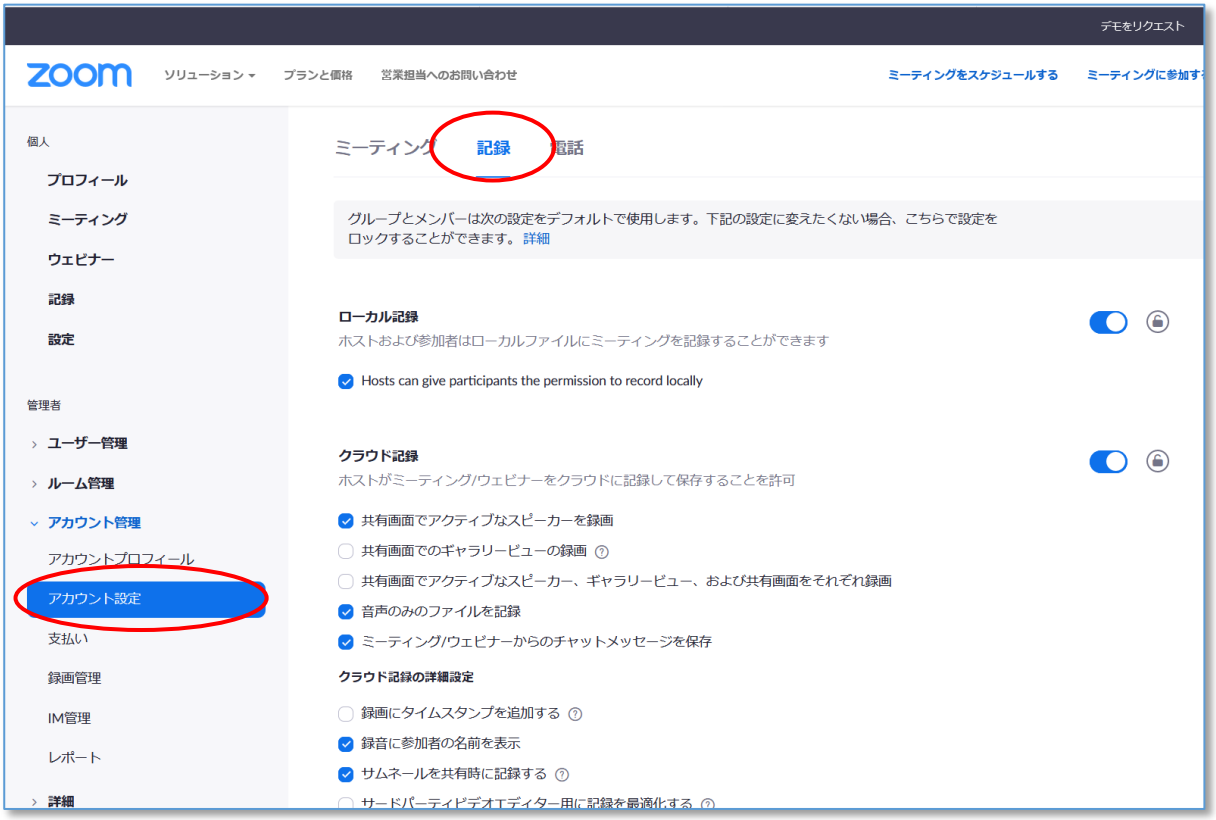
※１：既に録画されたファイルに対してのパスワード付与は必須としておりません。社内のルールで暗号化が必須となっていた場合はこの設定します。

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し録画保存の容量とセキュリティリスクを低減させます。

【手順①】

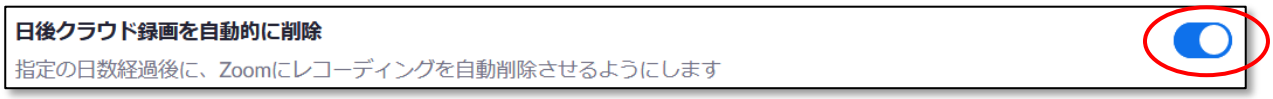
Zoom(https://zoom.us/)にログインし左ペインの「アカウント設定」をクリックし右ペイン上部の「記録」タブをクリックします。



【手順②】

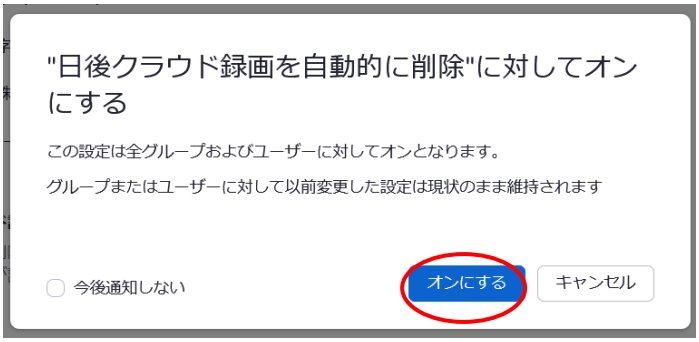
「日後クラウド録画を自動的に削除」の項目まで下へスクロールします。

デフォルトはオフとなっているのでスライドバーをクリックし有効化します。



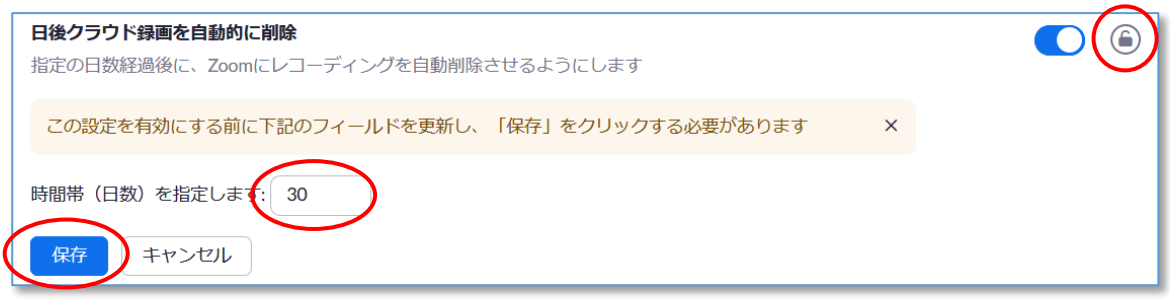
【手順③】

下記がポップアップされるので「オンにする」をクリックします。



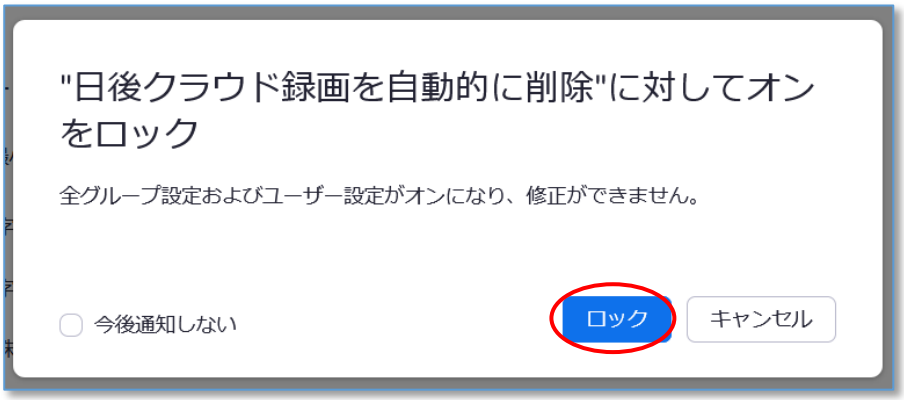
【手順④】

クラウド上に保管する日数を設定し保存と鍵マークをクリックします。 (以下、記載例は 30 日後に削除)



【手順⑤】

下記ポップアップがされたらロックをクリックします。



画面上部に上記が表示されましたら設定は完了です。

４利用者向け作業

ここでは本製品の利用者に対して、セキュリティ観点上、注意すべきことを記載致します。

４-１チェックリスト 3-3 に対する利用者向け作業

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可能**です。
またミーティング参加時の参加者名の入力は参加者側で自由に設定が出来ます。
なりすました不正ユーザー（※２）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。

※２：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 に対する利用者向け作業

4-2-1 不適切な参加者の強制退室

Zoom の待合室は**誰でも入室出来てしまいます。**

そのため主催者は待機室を利用し待機している参加者名を確認し予め招待している参加者のみ許可をします。

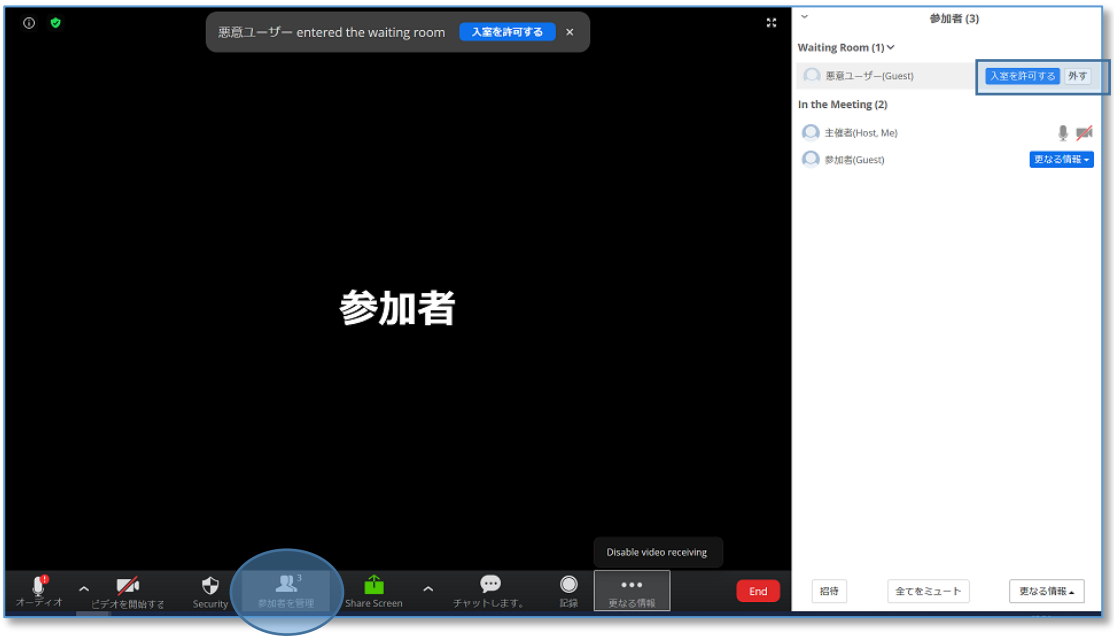
【手順】

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「参加者を管理」をクリックします。

上部が Waiting　Room(待機しているユーザー一覧)で下部が In the meeting(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「入室を許可する」をクリックします。

対象メンバーでなければ「外す」をクリックすると待機室から強制退場となります。

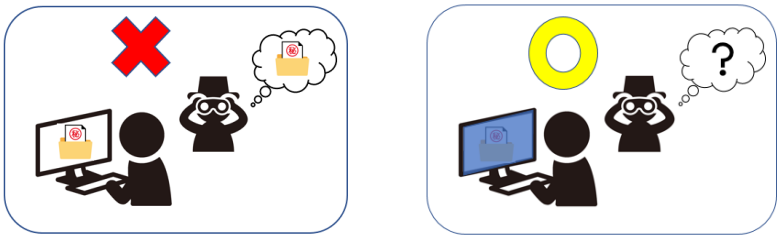


> ⚠ **注意事項**
>
> 悪意のあるユーザーは名前をなりすまして参加する可能性があります。
>
> 可能であればミーティング冒頭で参加者のカメラ機能を有効化して顔や音声で本人確認を実施することを推奨いたします。

4-3 チェックリスト 4-1 に対する利用者向け作業

4-3-1 第三者からの盗聴・覗き見の対策

オフィス外で利用する場合は第三者からの盗聴・盗み見に配慮する必要があります。
端末上に投影されている会議資料がのぞき見されないように**のぞき見防止フィルタの利用**や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 に対する利用者向け作業

4-4-1 アプリケーションの最新化

利用されるアプリケーションに関しては製品提供元からリリースされる最新バージョンアプリケーションを利用します。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手段となりますので定期的なアップデート確認をすることを推奨いたします。

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いたします。

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/security/ciadr/vul/alert20200403.html

4-5チェックリスト 8-5 に対する利用者向け作業

ミーティング利用時に**利用者（主催者）が利用中に注意すべき事項があります**。ここでは各デバイスでの Zoom の操作について詳細を記載します。

4-5-1ミーティング情報の件名に機密情報の記載禁止

会議名に**機密情報を含まれている場合、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。

機密情報を記載せずに参加者同士が分かる内容で記載をすることを推奨します。

4-5-2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。

悪意のあるユーザーによる持ち出し、またはサイバー攻撃を受けた際の機密情報漏洩のリスク低減になります。

記録→クラウド記録から対象の会議を選択して「その他」のメニューから削除が可能です。