

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	3
2 チェックリスト項目に対応する設定作業一覧.....	4
3 管理者向け設定作業.....	6
3-1 チェックリスト 3-3 への対応	6
3-1-1 ミーティングの入退室設定.....	6
3-2 チェックリスト 3-4 への対応	10
3-2-1 ミーティングのパスワードポリシーの設定	10
3-2-2 安全なミーティング URL の発行	12
3-3 チェックリスト 3-5 への対応	14
3-3-1 待機室の有効化	14
3-4 チェックリスト 8-5 への対応	16
3-4-1 ミーティングの録画設定	16
4 利用者向け作業	20
4-1 チェックリスト 3-3 への対応	20
4-1-1 ミーティング時の本人確認.....	20
4-2 チェックリスト 3-5 への対応	21
4-2-1 不適切な参加者の強制退室.....	21
4-3 チェックリスト 4-1 への対応	22
4-3-1 第三者からの盗聴・のぞき見の対策	22
4-4 チェックリスト 5-2 への対応	22
4-4-1 アプリケーションの最新化	22
4-5 チェックリスト 6-1 への対応	23
4-5-1 HTTPS 通信の確認	23
4-5-2 サービス接続先の確認	23
4-6 チェックリスト 8-5 への対応	23
4-6-1 ミーティング情報の件名に機密情報の記載禁止	23
4-6-2 ミーティング録画ファイルの削除	24

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、明示であると默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/) (<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。

The screenshot shows the Zoom account settings interface. The top navigation bar includes links for Product, Solutions, Resources, Plans & Pricing, Schedule, Participants, Host, and Web Apps. On the left, a sidebar lists management categories like Plan & Request, User Management, Team Chat Management, Device Management, Room Management, Workspaces Management, Phone System Management, and Account Management. Under Account Management, 'Account Settings' is highlighted with a red box. The main content area has tabs for AI Companion, General, Meetings, Recording and Transcription, Mail & Calendar, and Audio Conferencing. The 'Meetings' tab is active. Below the tabs, a note states: 'Groups and members will use the following settings by default. If you want to change these settings, click here.' It then shows the 'General' settings for meetings, including the 'Meeting Host Control' toggle switch, which is turned on (blue). Other options include 'Each participant's "Present" status' (checked), 'Meeting chat links and attachments' (checked), 'Recording' (checked), and 'Always share with participants' (radio button selected). The bottom right corner features a blue circular icon with a white 'Q'.

【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。

ホストより先に参加することを参加者に許可



参加者はホストが到着する前に参加できます。ホストよりも先に参加者の参加が許可されていない場合や、ホストが別のミーティングを主催している場合にはミーティングがまだ開始されていないことを通知するダイアログが参加者に表示されます。このダイアログは、[待機室をカスタマイズ] 設定でカスタマイズできます。

【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。

"ホストより先に参加することを参加者に許可" をロックする

全グループ設定とユーザー設定がオフになり、修正ができません。

アカウントのすべてのミーティングが即座にこの設定を使用します。ホストはこの設定を自分自身のミーティングに対して変更できません。

注：Zoomクライアントからスケジューリングされるすべてのミーティングもこの設定を利用します。ホストがこの設定を変更した場合でもこれは変わりありません。Zoomは、この設定が現在ロックされていることを、ミーティングのホストに通知することを推奨します。

今後通知しない

 ロック

キャンセル

 設定が更新されました。

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、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 \(https://zoom.us/\)](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。

The screenshot shows the Zoom account settings interface. On the left sidebar, under 'Account Management', 'Account Settings' is selected. In the main content area, the 'Meetings' tab is active. Under the 'General' section, there's a heading 'Meeting Assets'. To its right is a toggle switch that is turned on (blue), with a lock icon next to it, indicating it's locked. Below the toggle switch are several checkboxes for meeting features: 'Participants who have joined' (checked), 'Meeting chat links and attachments' (checked), 'Recording' (checked), 'Always share with participants' (unchecked), and 'Host only can view and share' (unchecked).

【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。

誰かが参加するときまたは退出するときに音声で通知



以下に対して音声を再生：

- 全員
- ホストと共同ホストのみ

電話により参加した人がいる場合：

- 通知として使用するために、音声をレコーディングするように依頼

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 \(https://zoom.us/\)](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。

The screenshot shows the Zoom account settings interface. The left sidebar is titled '管理者' and lists various management options. The 'アカウント設定' link is highlighted with a red box. The main content area has tabs for 'AI Companion', '一般', 'ミーティング' (which is selected), 'レコーディングと文字起こし', 'Mail & Calendar', and 'オーディオ カンフ'. Below these tabs, there's a note about group and member settings. The 'セキュリティ' section contains several checkboxes for meeting recording and sharing options. A blue lock icon is visible next to some settings.

【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。

The screenshot shows the Zoom account settings interface again, with the 'アカウント設定' link highlighted in the sidebar. The right side of the page features a 'セキュリティ' section with links to 'ミーティングのスケジュール', 'ミーティング内 (ベーシック)', 'ミーティング内 (詳細)', 'メール通知', '管理者オプション', and 'その他の設定'. To the right of these, a large red box encloses the 'パスコードの要件' section, which lists ten requirements for password strength, each preceded by a checkbox. The requirements include: 'パスワードには最小文字数制限があります', '1つ以上の文字 (a, b, c...)', '1つ以上の数字 (1, 2, 3...)', '1つ以上の特殊文字 (!, @, #...)', '大文字と小文字の両方を含める', '連続文字 ("11111", "12345", "abcde", "qwert"など) を使用できません', '強化された脆弱なパスコード検出機能を使用', and '数字のパスコードのみを利用できます'.

【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)

The screenshot shows the Zoom account settings interface. On the left sidebar, under 'アカウント管理' (Account Management), 'アカウント設定' (Account Settings) is selected. In the main content area, under 'セキュリティ' (Security), there is a section titled 'パスコードの要件' (Password Requirements). This section contains several checkboxes:

- パスワードには最小文字数制限があります
パスワードの長さを指定する: 6
- 1つ以上の文字 (a, b, c...)
- 1つ以上の数字 (1, 2, 3...)
- 1つ以上の特殊文字 (!, @, #...)
- 大文字と小文字の両方を含める
- 連続文字 ("11111", "12345", "abcde", "qwert"など) を使用できません
- 強化された脆弱なパスコード検出機能を使用 (?)
- 数字のパスコードのみを利用できます

At the bottom right of the 'パスコードの要件' section are two buttons: '保存' (Save) and 'キャンセル' (Cancel), with '保存' highlighted by a red box.

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

This screenshot shows a meeting setup dialog box. On the left, there are several checkboxes:

- パスコード (Password) is checked, and the input field contains '111111'.
- 招待リンクまでは (Invitation link only) is unchecked.
- 待合室 (Waiting room) is unchecked.
- ホストに許可 (Host permission) is unchecked.
- 認証されたユーザー (Authenticated users) is unchecked.

 A callout bubble points to the password input field with the text: 'パスコードは以下であるようにする必要があります:' (The password must be set as follows):

- ✓ 文字は6字以上 (6 or more characters)
- 1つ以上の文字 (a, b, c...)
- ✓ 1つ以上の数字 (1, 2, 3...)

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 内にパスコ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。

The screenshot shows the Zoom account settings interface. The left sidebar lists various management categories. The 'Account Settings' link is highlighted with a red box. The main content area shows the 'Meeting' tab selected. On the right, there's a section titled 'Meeting Passcode' with a toggle switch set to 'On' (blue) and a lock icon. Below this, there are several checkboxes for meeting options.

【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。

The pop-up window contains the following text:

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

ミーティングパスコードを暗号化して招待リンクに含めることで、参加者がパスコードなしでワンクリックで参加できるようにします。

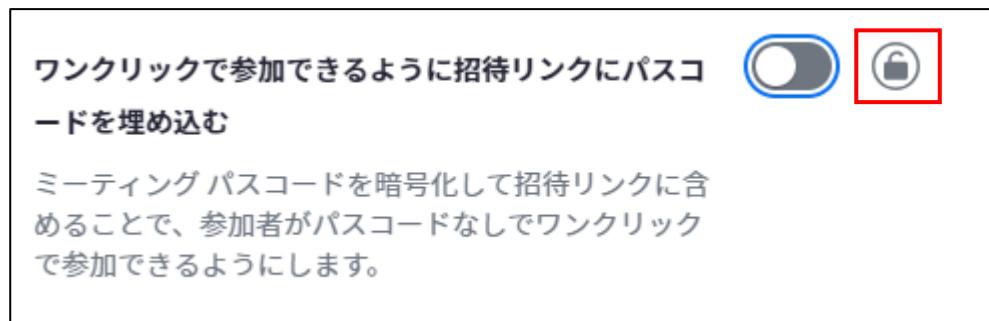
"ワンクリックで参加できるように招待リンクにパスコードを埋め込む" を無効にする

この設定を行うと、全グループとユーザーに対して無効になります。
グループまたはユーザーに対して以前変更した設定には適用されません。

今後通知しない **無効にする** キャンセル

【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する設定画面が表示されます。

The screenshot shows the Zoom account settings interface. The top navigation bar includes links for Product, Solutions, Resources, Plans & Pricing, Schedule, Participants, Host, and Web App. The left sidebar under 'Manager' has sections for Plan & Billing, User Management, Team Chat Management, Device Management, Room Management, Work Space Management, Phone System Management, Account Management (which is expanded), Account Profile, Alerts & Notifications, and Log Management. A red box highlights the 'Account Settings' link under 'Account Management'. The main content area shows tabs for AI Companion, General, Meeting (which is selected and highlighted in blue), Recording and Transcription, Mail & Calendar, and Audio & Video Calls. Below the tabs is a note about group and member settings. The 'Meeting' tab contains sections for Security (Meeting in Schedule, Meeting in Basic, Meeting in Detailed), Notifications (Meeting Chat Link and Attachment, Recording), and Other Settings. A lock icon is present next to the recording options.

【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。

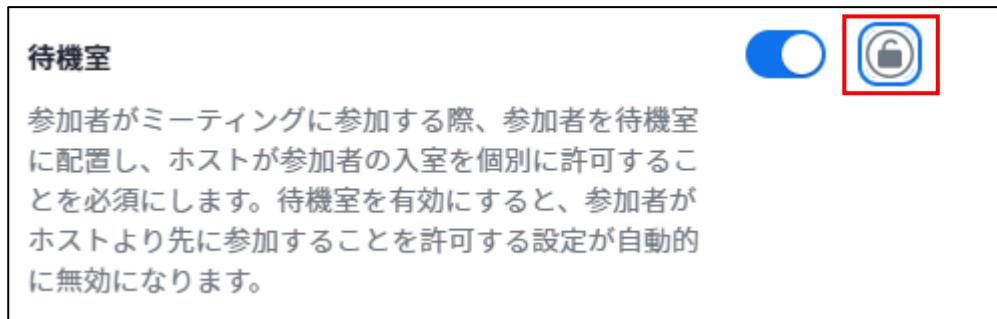
The screenshot shows a modal dialog box titled "待機室". It contains a toggle switch that is turned on, indicated by a blue circle and a lock icon. The text next to the switch says "参加者がミーティングに参加する際、参加者を待機室に配置し、ホストが参加者の入室を個別に許可することができます。" Below the switch is a section titled "待機室" with the sub-section "ミーティングのスケジュール". A message states "この設定を行うと、全グループとユーザーに対して有効になります。グループまたはユーザーに対して以前変更した設定には適用されません。". At the bottom of the dialog are two buttons: "今後通知しない" (Do not notify me again) and a red-bordered "有効にする" (Enable) button. Below the dialog is a footer with "オプションを編集する" and "待機室をカスタマイズ".

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】

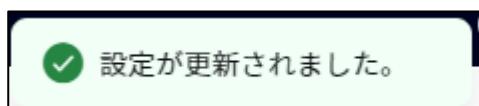
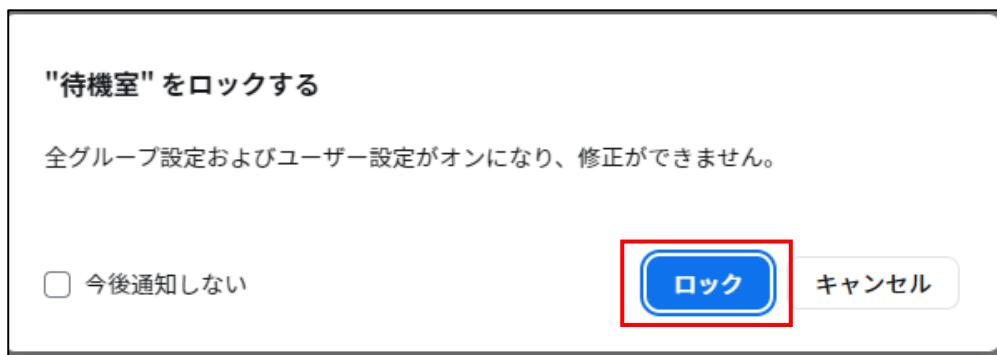
トグルボタンの右にある鍵マークをクリックし、設定をロックします。

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。

The screenshot shows the Zoom account settings interface. On the left sidebar, 'アカウント設定' (Account Settings) is highlighted with a red box. At the top right, the 'Recording and Transcription' tab is selected, also highlighted with a red box. In the main content area, there are two tabs: 'Recording' and 'Transcription'. Under 'Recording', there is a section titled 'Computer files are recorded' with a toggle switch and a lock icon. Below it, there are two checkboxes: 'Host requests recording permission from users' (unchecked) and 'Internal meeting participants' (checked). A blue circular icon with a white question mark is located at the bottom right.

【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。

This screenshot shows a specific configuration for cloud recordings. It includes a toggle switch and a lock icon, both of which are highlighted with red boxes. Below this, there is a checkbox for 'Existing cloud recordings require a password' (unchecked) and a help icon (a question mark inside a circle).

【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。

"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" をロックする

全グループ設定およびユーザー設定がオンになり、修正ができません。

今後通知しない

ロック

キャンセル

【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。

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



パスコード保護が共有クラウド レコーディングに対して設定されます。ランダムなパスコードが設定され、ユーザーはこれを変更できます。この設定は新しく生成されたレコーディングに対してのみ適用可能です。

既存のクラウド 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 [?](#)

ワンクリック アクセス用の共有可能リンクにパスコードを埋め込む

パスコードなしでレコーディングにアクセスすることを被招待者に許可する [?](#)

保存

キャンセル

【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。

既存のクラウドレコーディングにアクセスするためにはパスワードを追加しています

前にパスワードが設定されていなかったクラウドレコーディングにパスワードが適用されます。ホストはパスワードを変更できます。

この変更についてユーザーに通知するために、この変更に関するテンプレートメールがお客様に送信され、お客様の組織でこれを使用することができます。

続ける

キャンセル

設定が更新されました。

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。

The screenshot shows the Zoom web interface. On the left, there's a sidebar with '管理者' (Administrator) and various management options like 'プランと請求' (Plans & Billing), 'ユーザー管理' (User Management), 'チームチャット管理' (Team Chat Management), 'デバイス管理' (Device Management), 'ルーム管理' (Room Management), 'ワークスペース管理' (Workspace Management), '電話システム管理' (Phone System Management), 'アカウント管理' (Account Management), 'アカウントプロフィール' (Account Profile), and 'アカウント設定' (Account Settings). The 'アカウント設定' option is highlighted with a red box. On the right, the main content area has tabs at the top: 'AI Companion', '一般' (General), 'ミーティング' (Meetings), 'レコーディングと文字起こし' (Recording and Transcription), 'Mail & Calendar', 'オーディオ カンフ' (Audio Conference). The 'レコーディングと文字起こし' tab is also highlighted with a red box. Below the tabs, there are two sections: 'レコーディング' (Recording) and '文字起こし' (Transcription). Under 'レコーディング', there's a toggle switch labeled 'コンピュータ ファイルにレコーディングする' (Record to computer file) which is turned on (blue). To its right is a lock icon. A note below says 'ミーティングをコンピュータにレコーディングすることをホストと参加者に許可します。レコーディングには、レコーダーの表示オプションに一致するビデオや共有コンテンツ、オーディオのみのファイルなどが含まれます。' Under '文字起こし', there are two checkboxes: '内部のミーティング参加者' (Internal meeting participants) which is checked, and '権限リクエストを自動承認する' (Automatically approve permission requests) which is unchecked. At the bottom right of the main content area is a blue circular icon with a white phone receiver symbol.

【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。
デフォルトはオフに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。

This screenshot shows a specific setting within the 'Recording and Transcription' tab. It features a text input field containing the text '指定された日数が経過した後、クラウド レコーディングを削除する' (Delete cloud recordings after the specified number of days have passed) and a toggle switch to its right. The toggle switch is currently off (gray), but it is highlighted with a red box, indicating it needs to be clicked to enable the feature.

【手順③】

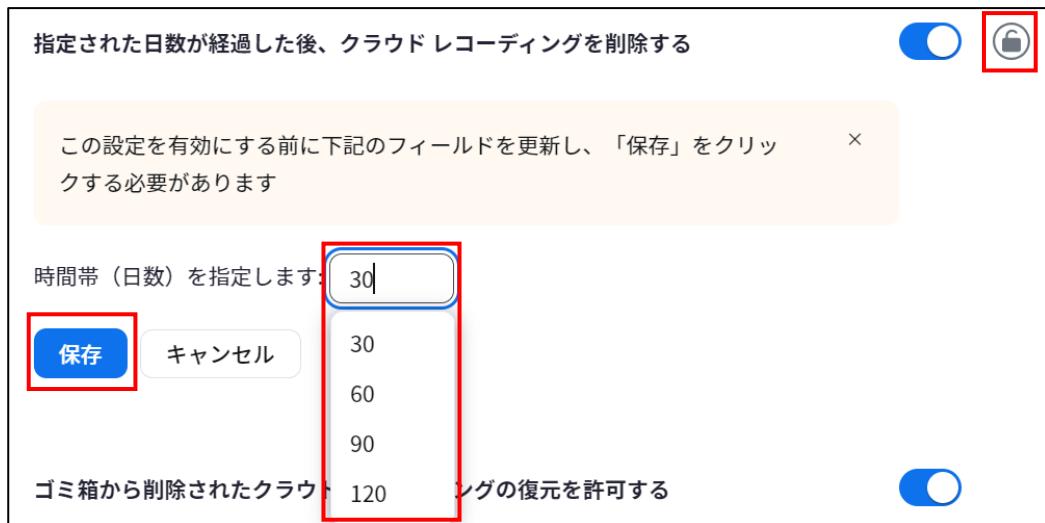
下記がポップアップされるので「有効にする」をクリックします。

This screenshot shows a confirmation dialog box. The text inside reads: "'指定された日数が経過した後、クラウド レコーディングを削除する'を有効にする" (Enable 'Delete cloud recordings after the specified number of days have passed'). Below this, a note states: 'この設定を行うと、全グループとユーザーに対して有効になります。グループまたはユーザーに対して以前変更した設定には適用されません。' (This setting will be effective for all groups and users. Changes made to individual groups or users will not apply). At the bottom of the dialog are three buttons: a checkbox labeled '今後通知しない' (Do not notify me again), a blue button labeled '有効にする' (Enable) which is highlighted with a red box, and a white button labeled 'キャンセル' (Cancel).

【手順④】

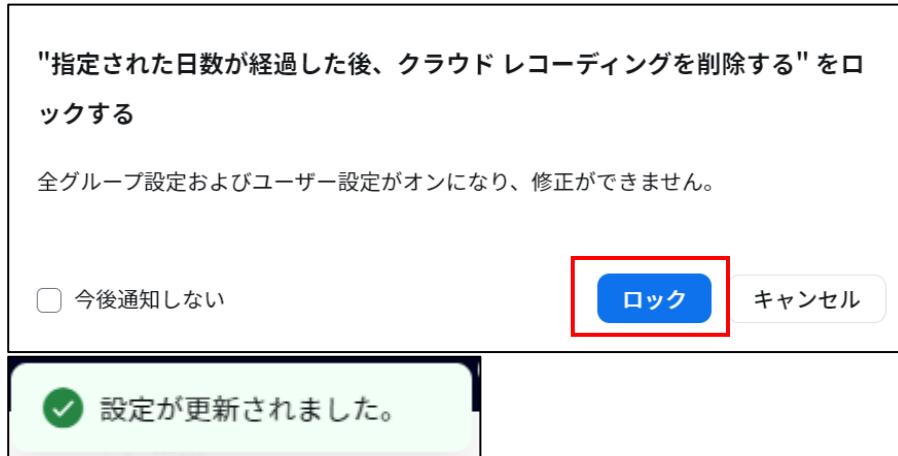
クラウド上に保管する日数を設定し、「保存」をクリックします。また、右側にある鍵マークをクリックし、設定をロックします。

（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



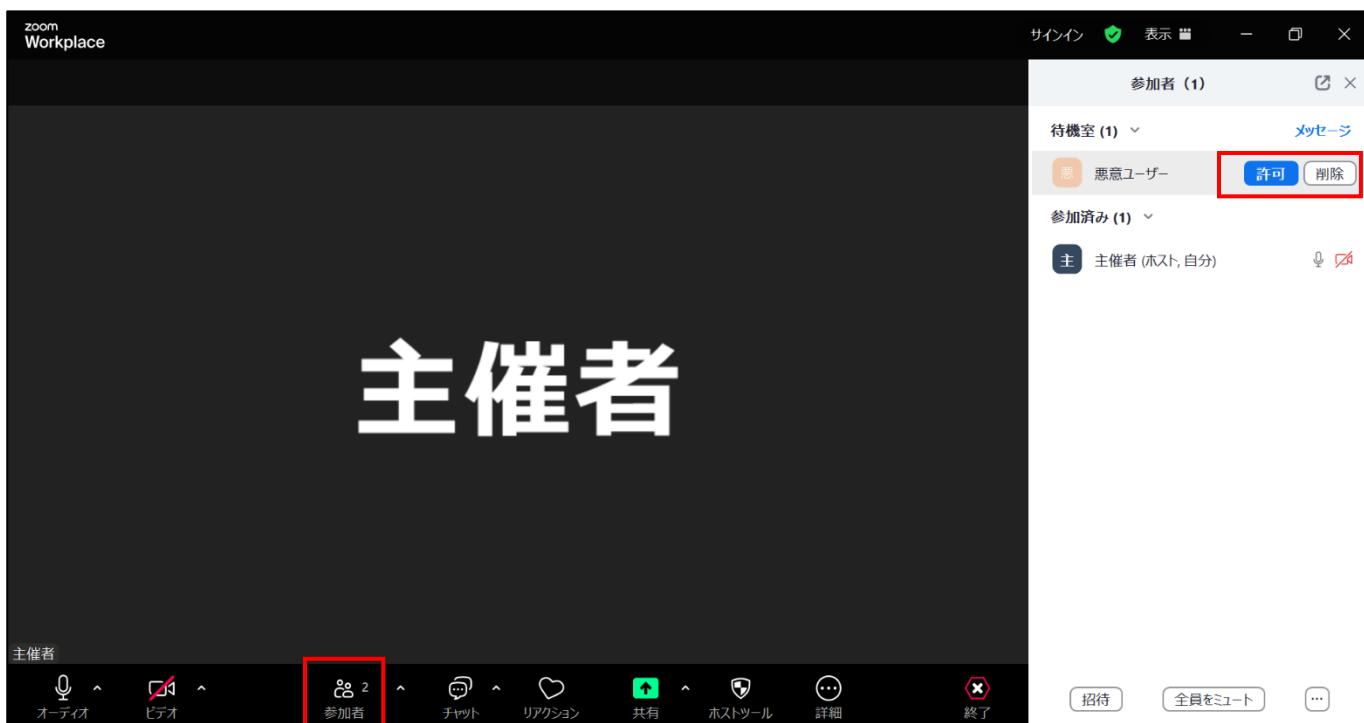
4-2 チェックリスト3-5への対応

4-2-1 不適切な参加者の強制退室

Zoomの待機室には、URLやパスワードを知つていれば、**誰でも入室できてしまします。**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

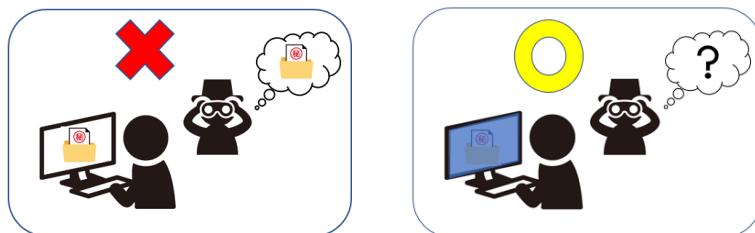
悪意のあるユーザーは名前をなりすまして参加する可能性があります。

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

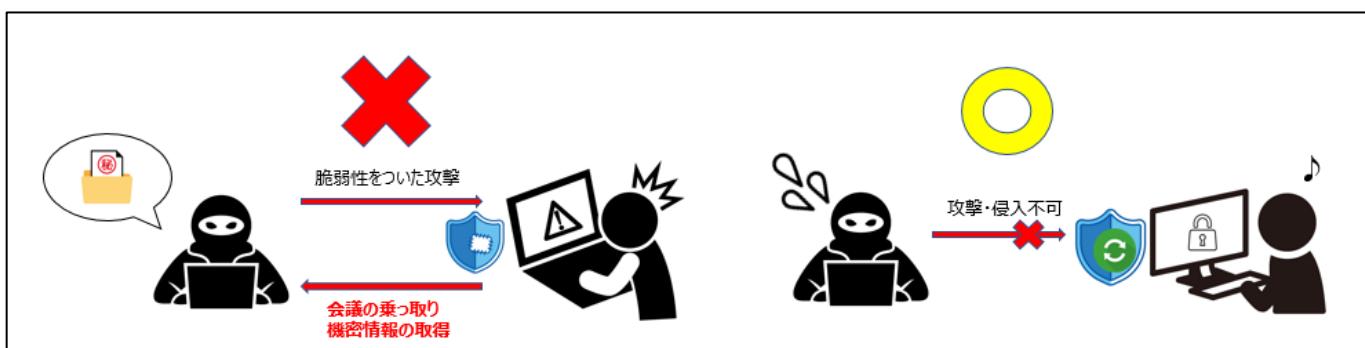
オフィス外で利用する場合は、第三者から盗聴・盗み見されないように注意する必要があります。端末上に投影されている会議資料などがのぞき見されないように**のぞき見防止フィルタを利用する**、会議音声が外部に漏れないようにイヤホンを利用する、など利用シーンにおいて対策が必要です。



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-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ことを推奨します。

The screenshot shows the Zoom web interface for scheduling a meeting. On the left, a sidebar menu has 'ミーティング' selected. The main area is titled 'ミーティングをスケジュールする'. It includes fields for 'トピック' (Topic) containing 'マイミーティング' and '社外秘の新商品「○○」について進捗報告をいたします。' (Confidential internal new product '○○' progress report), both of which are highlighted with a large red box. Below these are fields for '開催日時' (Schedule Date & Time) set to '2024/11/27 7:00 PM', '期間' (Duration) set to '1 時 0 分', and 'タイムゾーン' (Time Zone) set to '(GMT+9:00) 大阪、札幌、東京'. At the bottom are '保存' (Save) and 'キャンセル' (Cancel) buttons.

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。

レコーディングと文字起こし □ ドキュメント

クラウド レコーディング コンピュータ レコーディング 文字起こし

クラウド レコーディングは、30日間保存された後、自動的に削除されます。 X

トピックまたはミーティング ID で検索 オーディオ文字起こし内のテキスト 詳細検索 エクスポート

トピック	ID	開始時刻	ファイルサイズ	最大
マイミーティング	937 2302 8504	2024年11月28日 03:08 PM	4件のファイル (599 KB)	30日

共有 ...

4件のファイルをダウンロード
自動削除の無効化
削除

1件の結果

◀ ▶

Q

【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。