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

中小企業向け設定解説資料
（Cisco Webex Meetings）

Ver 2.0（2023.07）

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、Cisco Webex Meetings（以後、Webex と記載）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

本製品のライセンス形態は「個人（無償）」「Starter（有償）」「Business（有償）」が存在します。（2022 年 11 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「Starter」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、2022 年 11 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の設定と強度の強制	P.8
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。**	・ロビー機能の有効化	P.10
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.12

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.16
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.16
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.18
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.18
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.19 P.19
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.19 P.20

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

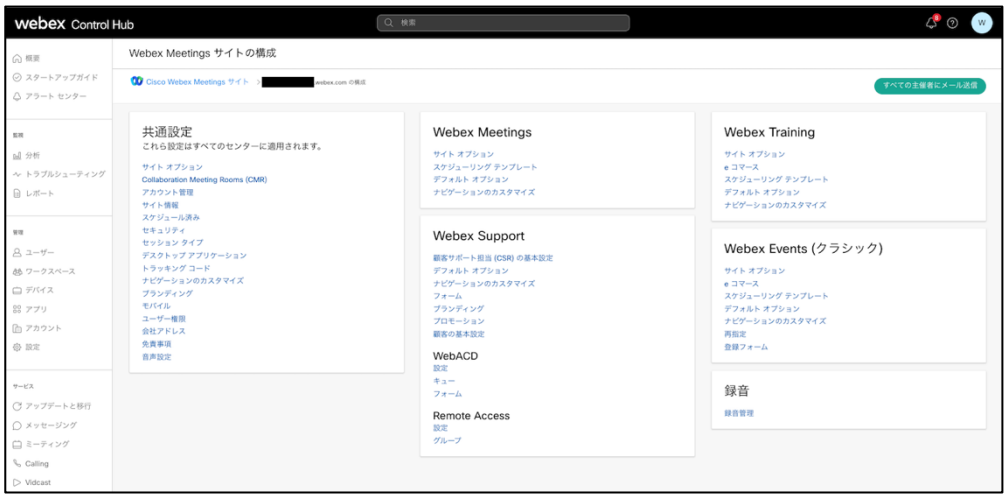
外部出席者が、主催者の同意なしにスケジュール済みミーティングに加わり、ミーティングを自由に操作できないようにします。

【手順①】

Webex サイト（https://@@@.webex.com）にログイン後、右ペインの「サイト管理」をクリックし、ミーティングに関連する設定が可能な Control Hub の画面に遷移します（@@@の部分はお使いの環境によって異なります）。

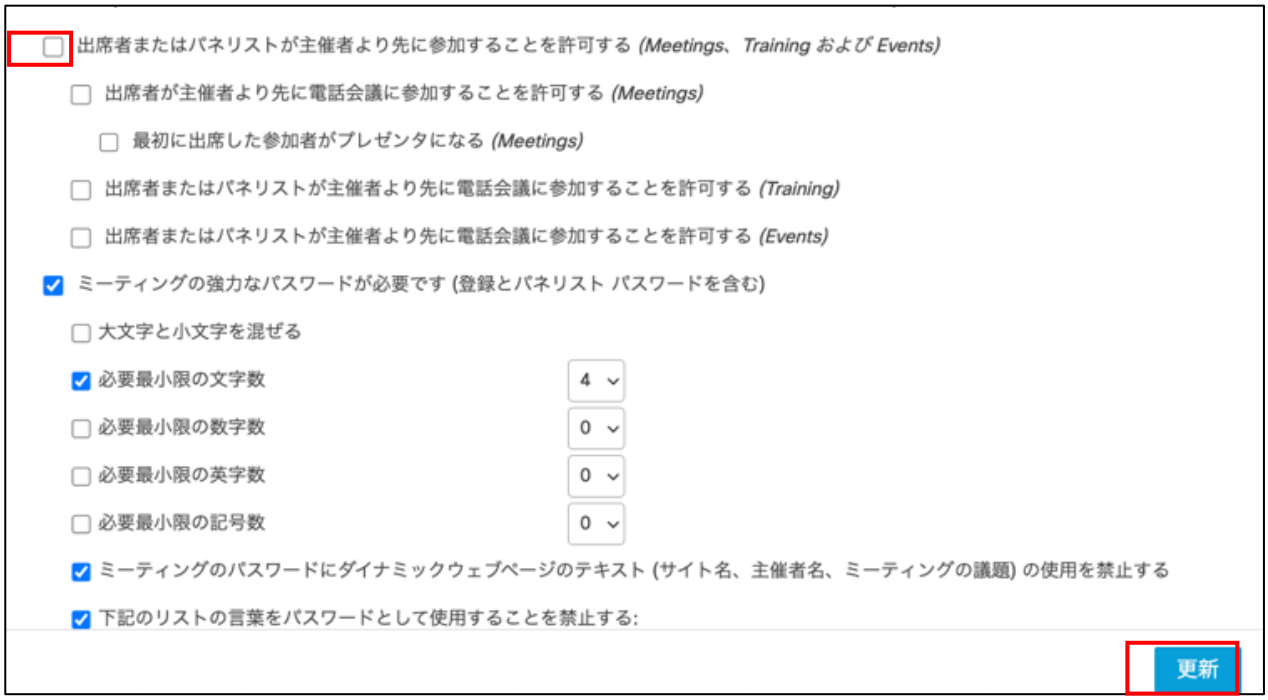
以下は遷移後の Control Hub 画面

※　直接 Control Hub（https://admin.webex.com）にアクセスすることもできます。



【手順②】

共通設定のサイトオプションをクリックし、「出席者またはパネリストが主催者より先に参加することを許可する」を確認します。チェックボックスにチェックがされていた場合はチェックを外し、「更新」ボタンを押します。（この設定はデフォルトではチェックされていません。）



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。

より安全なパスワード設定（強度の設定）

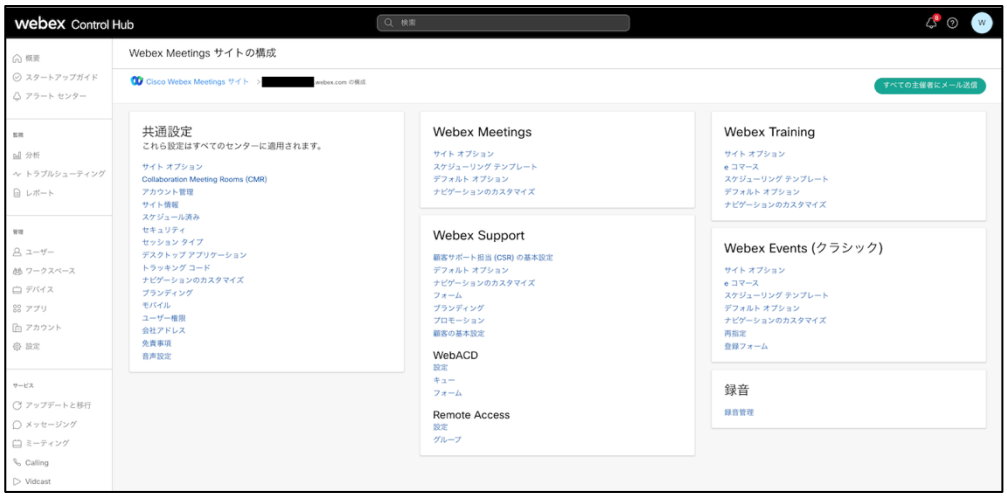
Webex のミーティングで発行されるパスワードの設定条件を変更する方法を記載します。

【手順①】

Webex サイト（https://@@@.webex.com）にログイン後、右ペインの「サイト管理」をクリックし、ミーティングに関連する設定が可能な Control Hub の画面に遷移します（@@@の部分はお使いの環境によって異なります）。

以下は遷移後の Control Hub 画面

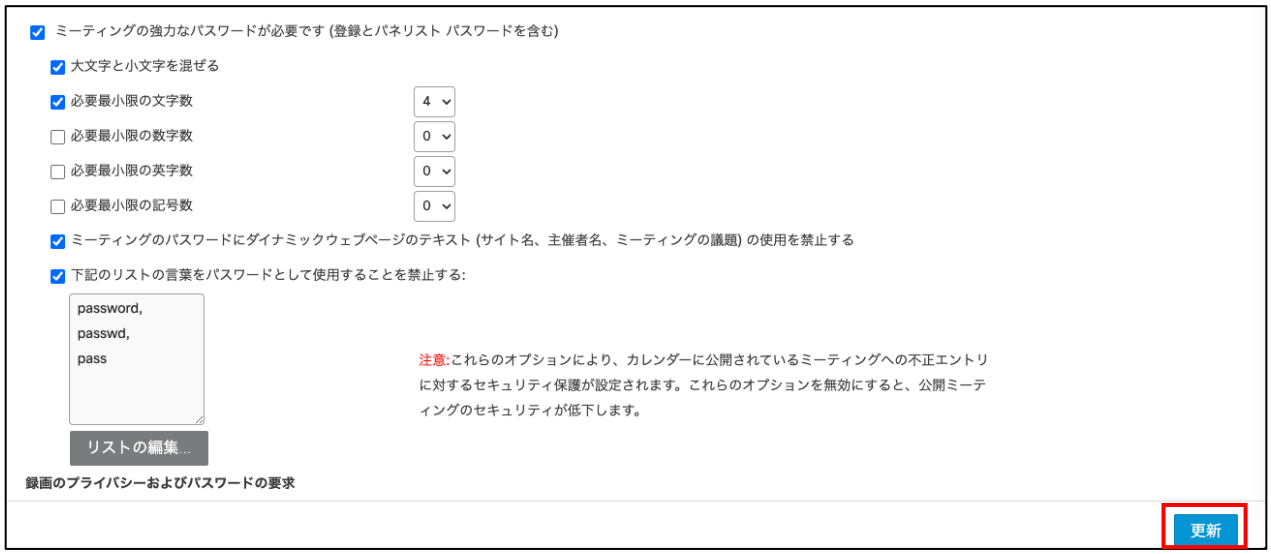
※　直接 Control Hub（https://admin.webex.com）にアクセスすることもできます。



【手順②】

共通設定のサイトオプションをクリックし、「ミーティングの強力なパスワードが必要です　（登録とパネリスト パスワードを含む）」にチェックを入れます。その後パスワードの設定条件を設定し、「更新」ボタンを押します。

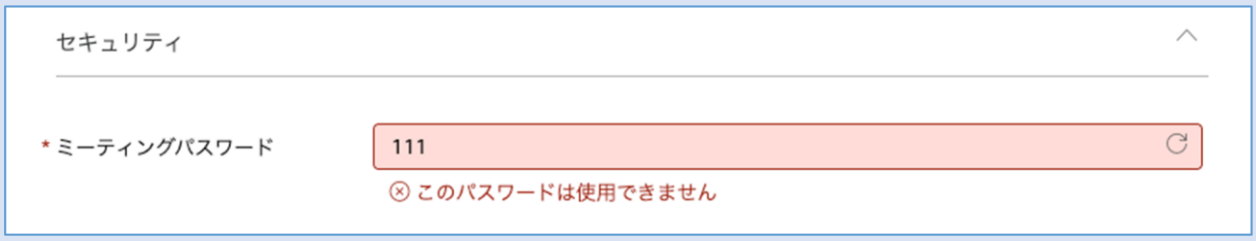
（以下、記載例は 4 文字以上で大文字小文字を含むパスワードの設定）



この際、更新完了メッセージは表示されませんが設定は完了です。

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できなくなります



3-3　チェックリスト 3-5 への対応

3-3-1　　ロビー機能の有効化

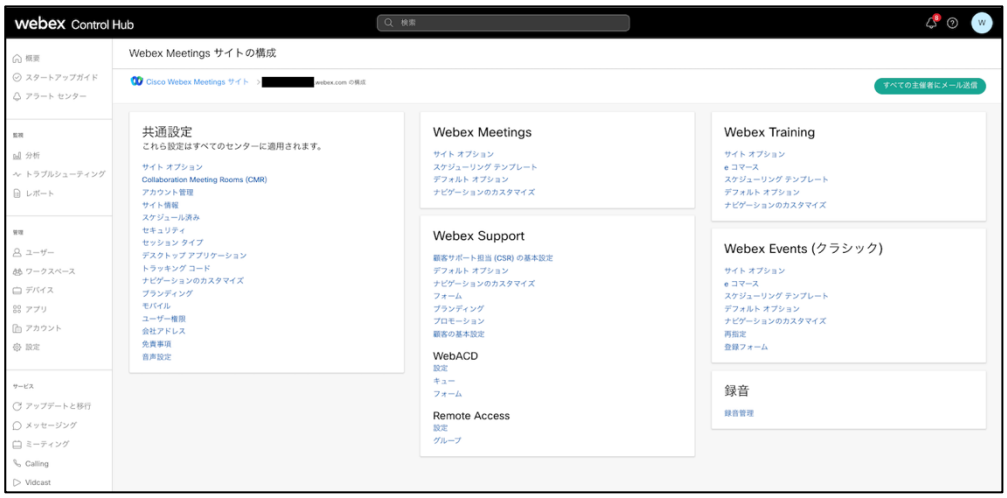
ロビー機能により、ホストはミーティングに参加する参加者を制御することができます。ロビー機能は参加者を直接会議に参加させず、一旦ロビーに待機させ主催者が許可し入室させる機能です。**想定していない参加者がミーティングに参加できないようにすることで、安全なミーティングを確保します**。

【手順①】

遷移 Webex サイト（https://@@@.webex.com）にログイン後、右ペインの「サイト管理」をクリックし、ミーティングに関連する設定が可能な Control Hub の画面に遷移します（@@@の部分はお使いの環境によって異なります）。

以下は遷移後の Control Hub 画面

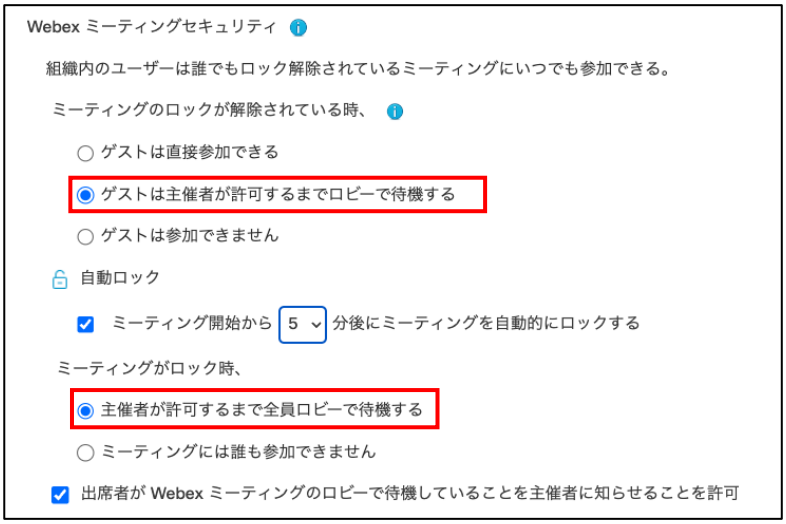
直接 Control Hub（https://admin.webex.com）にアクセスすることも可能です。

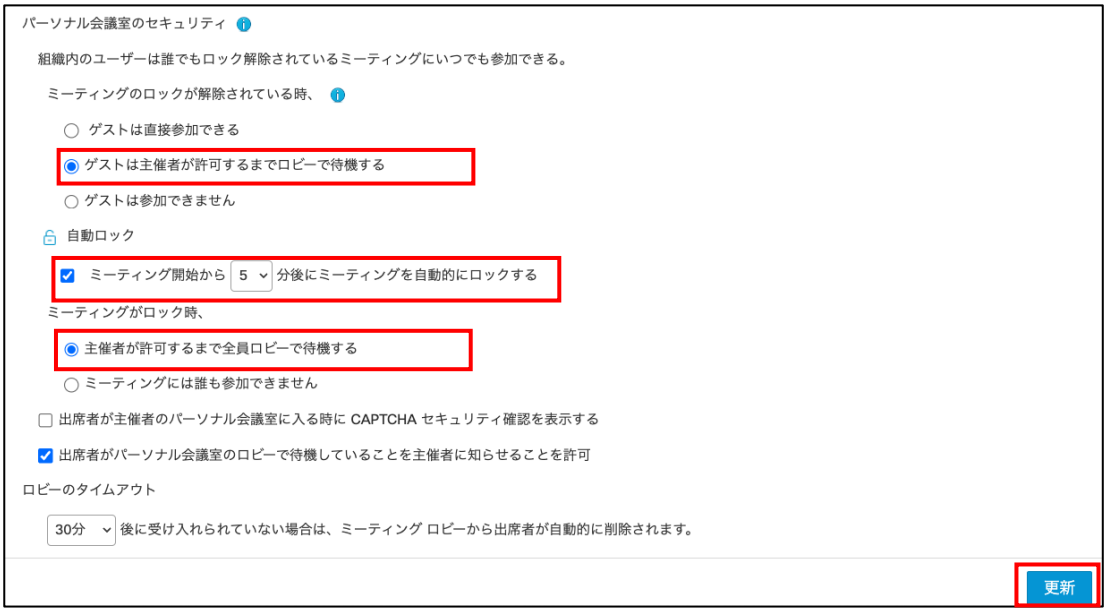


【手順②】

共通設定のサイトオプションをクリックし「Webex ミーティングセキュリティ」まで下へスクロールします。

Webex ミーティングセキュリティおよびパーソナル会議室のセキュリティのそれぞれについて、「ゲストは主催者が許可するまでロビーで待機する」を選択します。その後、「更新」ボタンを押します。





この際、更新完了メッセージは表示されませんが設定は完了です。

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、**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ことができます。**

録画ファイルのパスワード設定の強制

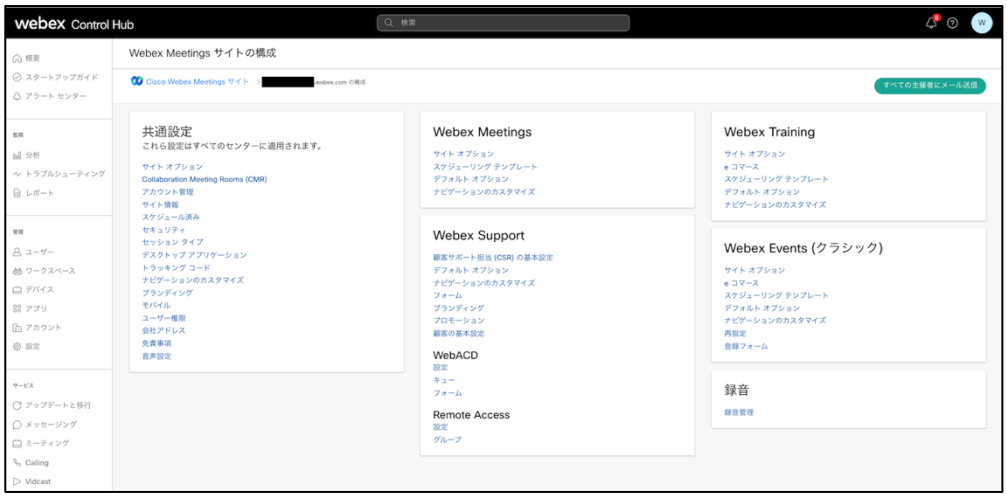
Webex のクラウドに記録されたミーティングの動画に対し、パスワード設定を強制することでミーティングに参加していないメンバーが録画ファイルを閲覧できないように設定します。

【手順①】

遷移 Webex サイト（https://@@@.webex.com）にログイン後、右ペインの「サイト管理」をクリックし、ミーティングに関連する設定が可能な Control Hub の画面に遷移します。（@@@の部分はお使いの環境によって異なります。）

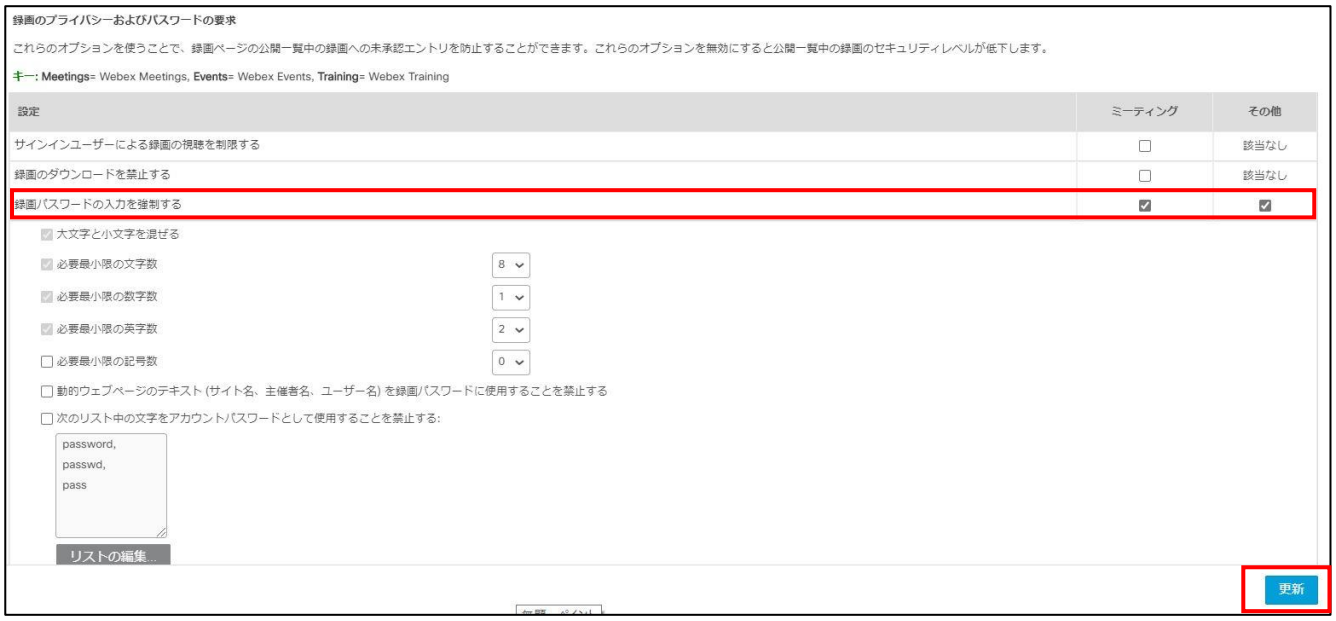
以下は遷移後の Control Hub 画面

※　直接 Control Hub（https://admin.webex.com）にアクセスすることもできます。。



【手順②】

共通設定のサイトオプションをクリックし「録画のプライバシー及びパスワードの要求」まで下へスクロールします。
パスワード設定条件を入力し「録画パスワードの入力を強制する」にチェックが入っていることを確認し、「更新」ボタンをクリックします。



この際、更新完了メッセージは表示されませんが設定は完了です。

録画ファイルの期日を指定した自動削除設定

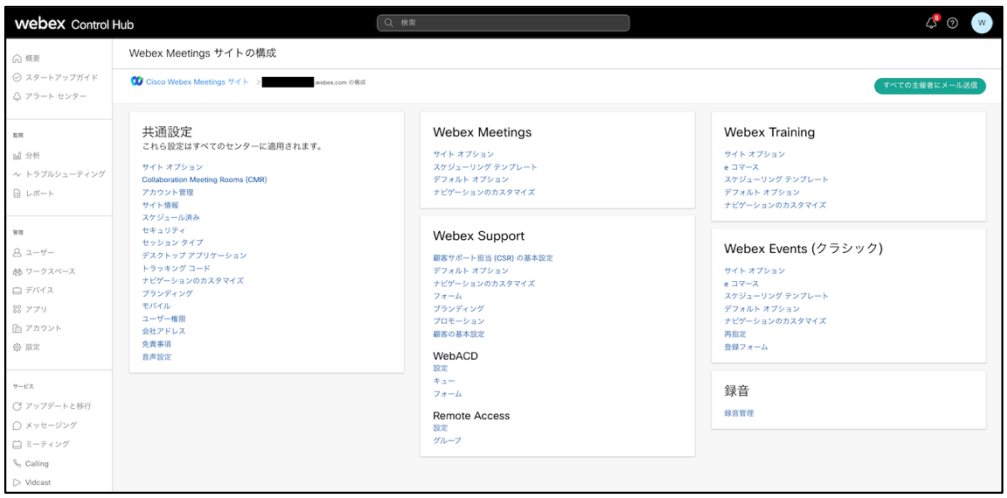
不要になった機密情報が含まれるミーティング録画を自動削除するように設定することでセキュリティリスクを低減させることができます。

【手順①】

遷移 Webex サイト（https://@@@.webex.com）にログイン後、右ペインの「サイト管理」をクリックし、ミーティングに関連する設定が可能な Control Hub の画面に遷移します。（@@@の部分はお使いの環境によって異なります。）

以下は遷移後の Control Hub 画面

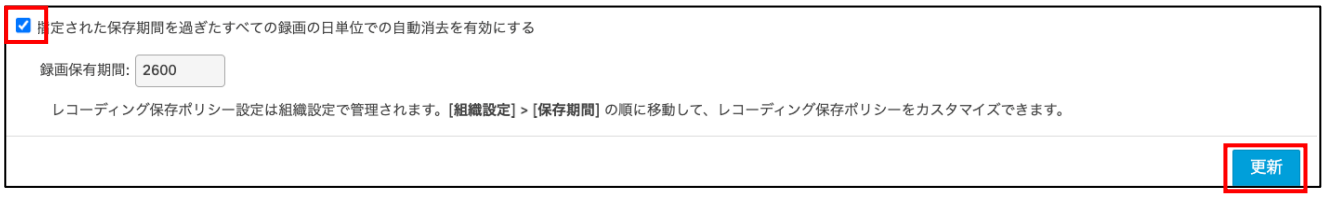
直接 Control Hub（https://admin.webex.com）にアクセスすることもできます。



【手順②】

共通設定のサイトオプションをクリックし「指定された保存期間を過ぎたすべての録画の日単位での自動消去を有効にする」まで下へスクロールします。チェックボックスにチェック後、保管期間（日数）を入力し、「更新」ボタンをクリックします。

以下記載例は、2600 日保管後に削除する設定です。この設定はデフォルトでは有効になっていため、必ず設定を行ってください。



この際、更新完了メッセージは表示されませんが設定は完了です。

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名の入力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

Webex の待合室は特別な設定をしない限り**誰でも入室できてしまいます。**そのため、主催者はロビー機能を利用して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を許可するようにします。

【手順①】

ロビーに参加者が入ると主催者画面の上部に待機しているユーザー名が表示されます。

【手順②】

下部中央にある参加者ボタンを押し、ロビーで待機しているユーザーの一覧を表示します。

予定していた参加者であれば参加者名のチェックボックスにチェックし、「参加を許可」をクリックします。

対象メンバーでなければ「削除」をクリックすると、待機室から削除します。

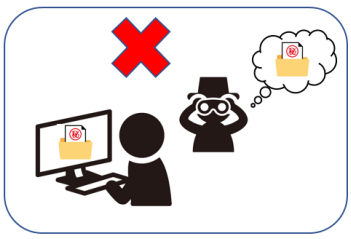
- **注意事項**

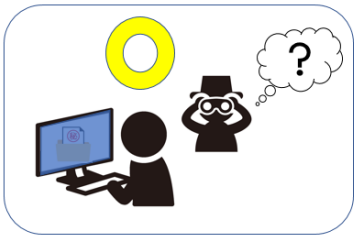
悪意のあるユーザーは、名前をなりすまして参加する可能性があります。可能であればミーティング冒頭で参加者のカメラ機能を有効化し、顔や音声で本人確認を実施することを推奨します。

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・のぞき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。





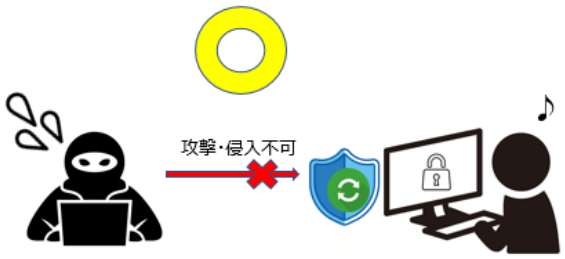
4-4　チェックリスト 5-2 への対応

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です。**

Webex アプリの場合、自動的にアップデートがかかるため、利用者がアップデートの作業を行う必要はありません。

【参考】Webex Meetings アプリのインストール・アップデート詳解 - Cisco Community



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 Webex への通信は基本的に HTTPS で暗号化されています。

4-5-2　　サービス接続先の確認

Webex 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（Webex 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、Webex 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**。Webex ではミーティングをスケジュールする際、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は、**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低減になります**。

「録画」から対象の会議を選択して「ゴミ箱」アイコンをクリックすることで削除することができます。