セキュアな Cisco WebEx ミーティング開催のための管理者および主催者用ベストプラクティス

初版：2016 年 03 月 15 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

WebEx プライバシーの概要

Cisco WebEx のオンラインソリューションなら、グローバル社員やバーチャルチームがまるで会議室にいるかのようなリアルタイム共同作業を可能にします。世界中二点在する事業、学会、政府の組織はCisco WebEx ソリューションを使って業務プロセスを簡素化し、営業、トレーニング、プロジェクト管理、サポートチームに優れた結果をもたらします。

すべての組織およびユーザーにとってプライバシーはとても重要です。オンラインコラボレーションでは、ミーティングのスケジューリングから参加者によるコンテンツ共有の許可まで多層レベルのセキュリティを提供します。

Cisco WebEx は誰にでも開かれたコラボレーションスペースに最適化されたこれまでで最も安全な環境を提供します。サイト管理者としてプライバシー機能を理解することで、エンドユーザーはあなたのビジネスニーズに合った形で WebEx を使用します。

詳細については、WebEx セキュリティのホワイトペーパーを参照してください。

管理者のベストプラクティス

プライバシーの基礎はWebExサイト管理者によって指定されます。管理者は主催者とプレゼンタの権限のプライバシーポリシーの管理と強制を行うことができます。例えば、承認済み管理者はセッション設定のカスタマイズを行い、プレゼンタのアプリケーション共有やサイトまたはユーザーレベルでのファイル転送を無効にすることができます。

ミーティング保護に次の機能を使用することをお薦めします。

すべてのミーティングを非公開にする

ミーティングの議題だけでも繊細な情報を明かすには十分です。例えば、A社の買収を検討する、というミーティングの議題だけで株価への影響は大きなものになります。非公開ミーティングにしておくことで繊細な情報の機密性を保持することができます。

公開ミーティングだと議題およびその他の一部情報がお使いのサイトに表示され、認証ユーザーだけでなく未認証ユーザーも見ることができます。特に議題を表示しておく必要が無い場合は、すべてのミーティングを非公開にしておくことをお薦めします。

手順

ステップ 1 WebEx サイト管理ツールにサインインする。

ステップ 2 [設定 > 共通のサイト設定 > オプション > セキュリティオプション] の順に移動します。

ステップ 3 [すべてのミーティングを非公開ミーティングとする (MC、TC、および EC)。

すべてのミーティング、イベント、セッションでパスワード入力を要求する

あなたのすべてのミーティング、イベント、トレーニングセッションの安全性を高めるために最も効果がある方法はパスワードを設定することです。パスワードがあれば未承認の出席者が参加

することはありません。パスワードを知っている招待者だけがあなたのセッションに参加できます。パスワード要求の手順に従い設定することでミーティング、イベント、トレーニングセッションはかなり安全なものになります。

パスワードには複雑なパターンが組み合わされた強力なものを使用してください。強力なパスワードには、大文字小文字、数字、特殊文字が組み合わされ、使用されているべきです。例えば $Tu0psrOx! です。

（注） ミーティング、イベント、トレーニングセッションにパスワードを追加しても承認済み出席者による参加体験には影響しません。参加者は招待状中の URL または WebEx サイトから簡単に参加できます。

手順

ステップ 1 WebEx サイト管理ツールにサインインする。

ステップ 2 [設定 > 共通のサイト設定 > オプション > セキュリティオプション] の順に移動します。

ステップ 3 Meeting Center セクションで [すべてのミーティングでパスワードを必須にする] にチェックを入れます。

ステップ 4 Event Center セクションで [すべてのイベントでパスワードを必須にする] にチェックを入れます。

ステップ 5 Training Center セクションで [すべてのトレーニングでパスワードを必須にする] にチェックを入れます。

ステップ 6 強力なパスワードを必須にするには、ミーティングの複雑なパスワードを要求する] にチェックを入れます。

ステップ 7 次のボックスにチェックを入れ指定します。

- 大文字と小文字を混ぜる
- 最小文字数
- 最小数字数
- 最小アルファベット文字数
- 最小特殊文字数
- 同じ文字を 3 回以上使用することはできない
- ミーティングパスワードに動的ウェブページのテキスト (サイト名、主催者名、ユーザー名) の使用を禁止する
- このリスト中の言葉をアカウントパスワードとして使用することはできない

電話およびビデオ会議システムからの参加者にミーティングパスワード入力を強制する (WBS30)

ミーティングアプリケーション (Windows または Mac など) からの参加者にパスワードを要求すると共に、さらに電話およびビデオ会議システムからの参加者にもパスワードの入力を強制することができます。この機能はWBS30以降で利用できます。このオプションが有効な場合、システムにより電話及び会議システム用に自動的に 8 桁のパスワード番号が生成され、ミーティングの招待状に記載されます。これにより、電話またはビデオ会議システムの使用時に招待状が届いたユーザーのみがミーティングに参加できます。

手順

ステップ 1 WebEx サイト管理ツールにサインインする。

ステップ 2 [設定 > 共通のサイト設定 > オプション > セキュリティオプション] の順に移動します。

ステップ 3 Meeting Centerセクションで[電話で参加する場合にミーティングパスワードが必要] にチェックを入れます。

ステップ 4 Event Centerセクションで[電話で参加する場合にイベントパスワードが必要] にチェックを入れます。

ステップ 5 Training Center セクションで [電話で参加する場合にトレーニングパスワードが必要] にチェックを入れます。

ステップ 6 Meeting Center セクションで [ビデオ会議システムで参加する場合にミーティングパスワードが必要] にチェックを入れます。

ミーティング、イベント、トレーニングセッション参加時にサインインを要求する (WBS30)

機密性の高いミーティング、イベント、トレーニングセッションを開催する場合は、すべてのユーザーにWebExサイトのユーザー認証を要求してください。この場合には、主催者だけでなく出席者にもミーティング、イベント、トレーニングセッション参加時にアカウント情報の入力が求められます。

WBS30からの向上で、サイトへのサインインの他に、出席者は電話から参加する場合もサインインすることを必須にしてください。こうすることで、アカウント情報を持たないユーザーはミーティングおよびトレーニングセッションには参加することができません。

（注） Meeting Center または Training Center アプリケーションを使って参加する参加者はユーザー認証する必要がありますが、これにより、音声接続時に証明を求められることはありません。こうすることでこの制限は電話でのみ参加するユーザーにだけ影響します。

さらに、ビデオ会議システムで出席者によるサインインが必要なミーティングにダイヤルインすることを考えないといけません。なぜならユーザーはビデオ会議システムからはサインインできないからです。ビデオ会議システムからの参加を許可すると、未認証ユーザーによる参加が可能になってしまいます。

手順

ステップ 1 WebEx サイト管理ツールにサインインする。

ステップ 2 [設定 > 共通のサイト設定 > オプション > セキュリティオプション] の順に移動します。

ステップ 3 WebEx ミーティング、イベント、トレーニングセッションを開催する、または参加するすべてのユーザーに WebEx サイトへのサインインを要求するには、[サイトへのアクセスの前にログインが必要] (Meeting Center、Event Center、および Training Center のみ) にチェックを入れます。

ステップ 4 電話からミーティングまたはトレーニングセッションに参加するユーザーにサインインを要求するには、[電話から参加する場合にユーザーはアカウントが必要] (Meeting Center および Training Center のみ) にチェックを入れます。
これが有効な状態で、主催者がサインインを要求する場合、出席者は電話からサインインする必要があります。出席者はプロファイル設定で電話番号と PIN を追加しておく必要があります。

ステップ 5 ミーティングへの参加にサインインが求められる場合にビデオ会議システムからの参加を防ぐには、[ブロック中] を選択します(Meeting Center のみ)。
ブロックされている場合に、ビデオ会議システムのユーザーはサインインが求められているミーティングの開始および参加はできません。これにはサインインが求められるパーソナル会議室も含まれます。

主催者より先の参加を許可しない

安全面への影響を理解していない間、またはこの機能が求められる場合を除き、すべてのミーティングで出席者が主催者より先に参加することを許可しないでください。

お使いのサイトの主催者より先に参加するオプションを無効にすることをお薦めします。公開ミーティングではこれらのオプションを無効にしてください。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、好き放題なことができてしまいます。

出席者による主催者より先の参加を許可した場合でも、音声には主催者より先には参加させないようにしてください。あなたの公開ミーティングがパスワードで保護されていない場合、不正アクセスユーザーが勝手に費用が発生する通話を始めてしまう可能性もあります。

パーソナル会議のミーティング (PCN ミーティング) では主催者より先に音声に参加するオプションを無効にすることをお薦めします。主催者は出席者がミーティングに参加できるよう、先に音声ブリッジの WebEx アクセス番号にダイヤルし、主催者アクセスコードと主催者 PIN を入力しておく必要があります。

手順

ステップ 1 WebEx サイト管理ツールにサインインする。

ステップ 2 [設定 > 共通のサイト設定 > オプション > セキュリティオプション] の順に移動します。

ステップ 3 出席者が主催者より先に参加することを防ぐには、次のボックスにチェックを入れます:

- 出席者が主催者より先に参加することを許可する (MC、TC および EC)
- 最初に参加した出席者がプレゼンタになる (MC のみ)
- 出席者が主催者より先に電話会議に参加することを許可する (MC、TC および EC)
- 出席者が主催者より先にパーソナル会議に参加することを許可する (PCN ミーティング)

アカウント管理

サイト上のすべてのユーザーのポリシー設定を管理するには、WebEx サイト管理で次の機能も利用できます:

主催者アカウント管理

- ログインに指定回数以上失敗するとアカウントがロックアウトされる

アカウント作成

- 新規ユーザーに画面に表示される文字認証の入力を求めます
- 新規アカウントのメール確認を要求します
- 新規アカウントのセルフ登録ルールを設定します

アカウントのパスワード

- パスワード形式、文字数、再使用の各規定を指定します
- 一定期間後にパスワードの変更を要求します
- 簡単に推測できるパスワードを禁止します (例えば password など)
- パスワードの強制変更までの期間を指定します

主催者のベストプラクティス

主催者はミーティングのセキュリティ設定を行う最後の意思決定者です。主催者は、ミーティングの開始と終了の日時を含む、ほぼすべての要素を指定することができます。

ミーティングのスケジューリングではセキュリティのベストプラクティスを参照し、またビジネスニーズに合わせてミーティングと情報を保護してください。

パーソナル会議室を使用する (WBS30)

パーソナル会議室の自動ロック

WBS30以降、ミーティングが開始されるとパーソナル会議室が自動的にロックされる機能が追加されました。この機能は、WebExサイトの [マイ WebEx > 基本設定 > マイパーソナル会議室] からアクセスできます。会議室を0分でロックすることをお薦めします。つまりあなたが参加した時点で会議室がロックされるということです。こうすることで、ロビーにいる出席者が自由に会議室に入ることを防ぐことができます。ミーティング中、出席者がロビーで待機しているかどうか常に確認する必要があります。これで適切な出席者だけがあなたのミーティングに加わることができます。

（注） サイト管理者によりパーソナル会議室がログインユーザーだけに使用できるように設定されていない場合に、あなたのパーソナル会議室URLは公開URLであり、誰でもロビーで待つことができます。出席者を会議室に通す前に常に名前を確認してください。

ミーティング前のパーソナル会議室の通知

ユーザーがあなたのパーソナル会議室のロビーに入る前に、ユーザーはあなたにミーティングの開始を待っていることを知らせる通知を出すことができます。不正ユーザーであってもあなたのパーソナル会議室のロビーに入って通知を出すことができます。

ミーティングを開始する前にメール通知に目を通し、不正ユーザーを監視するようにしてください。パーソナル会議室の自動ロックを0分で設定していない場合、ミーティングが開始されると、

パーソナル会議室のロビーで待機しているすべての出席者がミーティングに加わります。参加者リストを確認し、不正ユーザーはすぐに強制退出するようにしてください。

パーソナル会議室を自動ロックしている状態で、不正ユーザーから届く通知メールが大量にある場合、通知を無効にすることができます。[マイ WebEx > 基本設定] に移動し、[退席中に誰かがパーソナル会議室のロビーに入ったらメールで知らせる]のチェックを解除してパーソナル会議室の通知をオフにすることができます。

ミーティング中のパーソナル会議室の通知

パーソナル会議室をロックしている場合、ロビーで待機しているユーザーを監視することができます。あなたがミーティングに参加した後、誰かがロビーに入ってきたら通知が届きます。あなたはそのユーザーを入れるか入れないか決めることができます。パーソナル会議室のロビーに複数の出席者が待機している場合、名前の一覧を確認し、個々またはすべてのユーザーを選択してミーティングに加えることができます。

ミーティングのスケジューリング

非公開ミーティングのスケジュール

ミーティングのプライバシーを強化するため、主催者はミーティングカレンダーにミーティングを記載しないようにすることができます。こうするには、このオプションからチェックを外してミーティングへの不正アクセスを防ぎます。また、主催者、議題、開始日時などのミーティング情報を非表示にします。

- 非公開ミーティングは、[ミーティング一覧]ページのミーティングカレンダーにも、[パーソナル会議室] ページにも表示されません。
- 非公開ミーティングに参加するには、固有のミーティング番号を入力する必要があります。
- 非公開ミーティングの場合、出席者は招待状メールで出席者にリンクを送信するか、または主催者がミーティングに参加ページでミーティング番号を入力する必要があります。

（注） ミーティングを公開するとミーティングの議題と一部情報が公開されてしまいます。ミーティングがパスワードで保護されていない場合、誰でも参加することができます。

ヒント ミーティングの目的に応じて、セキュリティレベルを選択してください。例えば、社内ピクニックの話し合いのためにミーティングを実施するのであれば、ミーティングのパスワードを設定するだけで十分と言えます。一方、社外秘の財務情報に関するミーティングを行うような場合は、ミーティングカレンダーでミーティングを非公開にします。すべての出席者がミーティングに参加したら、以降のアクセスを制限することもできます。

使用する議題を注意して選ぶ

公開ミーティングまたは送信される招待状では不正なユーザーに議題が見られてしまいます。議題によって故意なくプライベートな情報が漏れてしまうことがあるため、会社名やイベントなどの繊細な情報が表に出ないよう議題決めには細心の注意を払う必要があります。

複雑なパスワードでミーティングの安全性を高める

セッションに複雑なミーティングパスワードを指定することであなたのミーティングを保護してください。稀なケースですが、サイト管理者はパスワードなしのミーティング作成を許可している場合があります。通常ではすべてのミーティングで強力なパスワードを指定して保護することをお薦めします。

複雑で簡単に推測できないパスワードを与えることがとても大事です。強力なパスワードには、大文字小文字、数字、特殊文字が組み合わされ、使用されているべきです。例えば$Tu0psrOx! です。パスワードがあれば未承認の出席者がミーティングに参加することはありません。パスワードを知っている招待者だけがあなたのセッションに参加できます。

ミーティングに同じパスワードを再使用しないようにしてください。毎回同じパスワードを使用することで脆弱性が高まります。

（注） ミーティングにパスワードを追加しても承認済み出席者による参加体験には影響しません。参加者はミーティングへの招待状に含まれる URL をクリックすることで簡単に参加できます。これは WebEx モバイルアプリケーションでも Cisco Jabber でも同じです。

招待状にミーティングパスワードを記載しない

出席者をミーティングに招待する場合、出席者が受け取る招待メールにはミーティングパスワードが記載されません。電話などの別の手段で出席者にパスワードを知らせる必要があります。

機密性の高いミーティングの場合は、パスワードを招待状に含めないでください。こうすることで、未承認ユーザーが招待状を受け取ったとしても、ミーティングの情報への不正アクセスを防ぐことができます。

出席者にサイトのアカウント所有を要求する

この設定が有効な場合、出席者はミーティングに出席するためにサイトのユーザーアカウントを持っている必要があります。出席者がユーザーアカウントを取得する方法の詳細については、サイト管理者にお問い合わせください。

Meeting Center のアドバンストスケジューラで [出席者がこのミーティングに参加するにはウェブサイトのアカウントを必要とする] にチェックを入れます。

入退室のサウンドを使用または名前をアナウンスする機能

この機能を使用することで、音声から参加するユーザーがいつの間にかミーティングに参加していることを防ぎます。

この機能はMeeting CenterおよびTraining Centerで既定で有効になっています。この設定を調整するには、[音声会議の設定 > 入退室のサウンド] を選択肢ます。

使用できる機能を制限する

出席者に主催者より先の参加を許可する場合に、チャットや音声などの使用できる機能を制限します。

招待状を転送しないよう要求する

機密性の高いミーティングの場合には、招待者に招待状を他のユーザーに転送しないよう要求することができます。

代理主催者を指名する

ミーティングを開始して進行するための代理主催者を指名します。これを指定しておくことで、万一あなたがミーティングとの接続を切断してしまった場合でも、主催者権限が未承認ユーザーに渡ることを防ぐことができ、安全性がさらに高まります。

（注） スケジュール済みミーティングに出席者を招待する場合、1人または複数の出席者を代理のミーティング主催者として指名することができます。代理主催者は、ミーティングを開始して、主催者としての役割を担うことができます。代理主催者になるには、Meeting Centerサイトのユーザーアカウントが必要です。

ミーティング中

ミーティングへのアクセスを制限する

すべての出席者がミーティングに参加したら、ミーティングをロックします。こうすることで不要な出席者が参加してくることを防ぎます。主催者はセッション中であればいつでもミーティングをロックおよびロック解除できます。ミーティングをロックするには、[ミーティング>アクセスを制限] の順に選択します。

ヒント ミーティングへのアクセスを制限すると、ミーティング招待者でまだ参加していない参加者も含めミーティングに参加できなくなります。ミーティングをロック解除するには、[ミーティング > アクセス制限を解除] の順に選択します。

通話に参加するユーザーの認証確認

点呼をすることですべての出席者の確認を行うことで安全性が高まります。出席者にビデオをオンにさせるか、または名前を読み上げさせることで認証確認を行います。

（注）
- 発呼者が正しい WebEx ダイヤルイン番号と 9 桁のミーティング ID がわかってさえいれば、ミーティングに電話から参加できます。ミーティングパスワードは WebEx の音声会議から参加する出席者には有効ではありません。
- アカウントを持たない出席者がミーティングへの参加に許可されている場合、不正ユーザーは適当な名前を名乗ることでミーティングに参加できてしまいます。

ミーティングから参加者を排除する

ミーティング中いつでも参加者を強制退出させることができます。

排除したい参加者の名前を選択し、[参加者 > 退出させる] を選択します。

画面共有ではなくアプリケーション共有を行う

[共有 > 画面] ではなく、[共有 > アプリケーション] を使って特定のアプリケーションを共有することで、画面上にある繊細な情報の漏れを防ぐことができます。

ミーティング後

録画のパスワードを指定する

録画への不正アクセスを防ぐ最善の方法は録画を作成しないことです。

録画が作成された場合、ミーティング録画の共有を開始する前に、録画を編集し、パスワードを追加することで安全性を高めることができます。パスワード保護された録画ではユーザーが閲覧する際にパスワードの入力が求められます。

録画を削除する

一定期間が過ぎたら録画を削除してください。

主催者のパーソナル会議

WebEx サイトのマイ WebEx 基本設定セクションで強固な音声 PIN を作成して保護してください。

この PIN があなたのパーソナル会議アカウントへの不正アクセスを防ぐ最後の砦となります。パーソナル会議のミーティング (PCN ミーティング) の主催者アクセスコードへの不正アクセスがあったとしても、音声 PIN が無ければ会議を開始することはできません。音声 PIN は絶対に共有しないでください。