Webexのしくみを理解して
安全、快適にWebexを使おう

シスコシステムズ合同会社

2020年3月

アジェンダ

1. 主催者向けのベストプラクティス
2. 管理者向けのベストプラクティス
3. Webex Meetingsのネットワーク要件に適応するための
   セキュリティ対策
4. シングルサインオンと多要素認証

補足

- Webexのバージョン (WBS 40.xなど) が変更される際にユーザインタフェース、設定方法、操作方法などが変更される可能性があります。
- 本資料では WBS 40.1 の環境にてユーザインタフェースのスクリーンショットなどを取得しております。
- Webexサイトのユーザインタフェースはモダンビューでご説明いたします。(クラシックビューは長期的にはなくなる予定です。)

参考資料：ぜひご一読下さい

- ミーティングをセキュアなものにするための Cisco Webex ベストプラクティス: 主催者
  https://help.webex.com/ja-jp/8zi8tq/Cisco-Webex-Best-Practices-for-Secure-Meetings-Hosts
- ミーティングをセキュアなものにするための Cisco Webex ベストプラクティス: サイト管理
  https://help.webex.com/ja-jp/v5rgi1/Cisco-Webex-Best-Practices-for-Secure-Meetings-Site-Administration

- Cisco Webex Meetings Security White Paper
  https://www.cisco.com/c/dam/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.pdf?dtid=osscdc000283
- Cisco Webex Meetings プライバシー データ シート
  https://www.cisco.com/c/dam/global/ja_jp/about/doing-business/trust-center/docs/cisco-webex-privacy-data-sheet.pdf

スケジュールされたミーティング vs PMR

- これからご説明するセキュリティ関連の各種機能は会議のタイプによって利用できないものもあります。また利用できるとしても設定方法が異なる（会議毎に都度設定可能 vs ポータルにて基本設定で変更が必要であり多数の会議に影響がある など）ことがあります。
- 管理者設定または主催者の基本設定はあまり変更しないことを前提として本資料を作成しております。

機能	スケジュールされたミーティング	パーソナルミーティングルーム (PMR)
代理の主催者を事前に指名	○	×
他の認証済みユーザに開催を許可することが可能	○	○
主催者が参加する前に会議の開催を許可することが可能	○	× (※1)
参加者を登録ユーザのみに制限することが可能	○	×
ミーティングのロック	○	○

※1：PMRについては基本設定で特定のライセンス割り当て済みユーザを代理主催者として事前に指定することも可能。

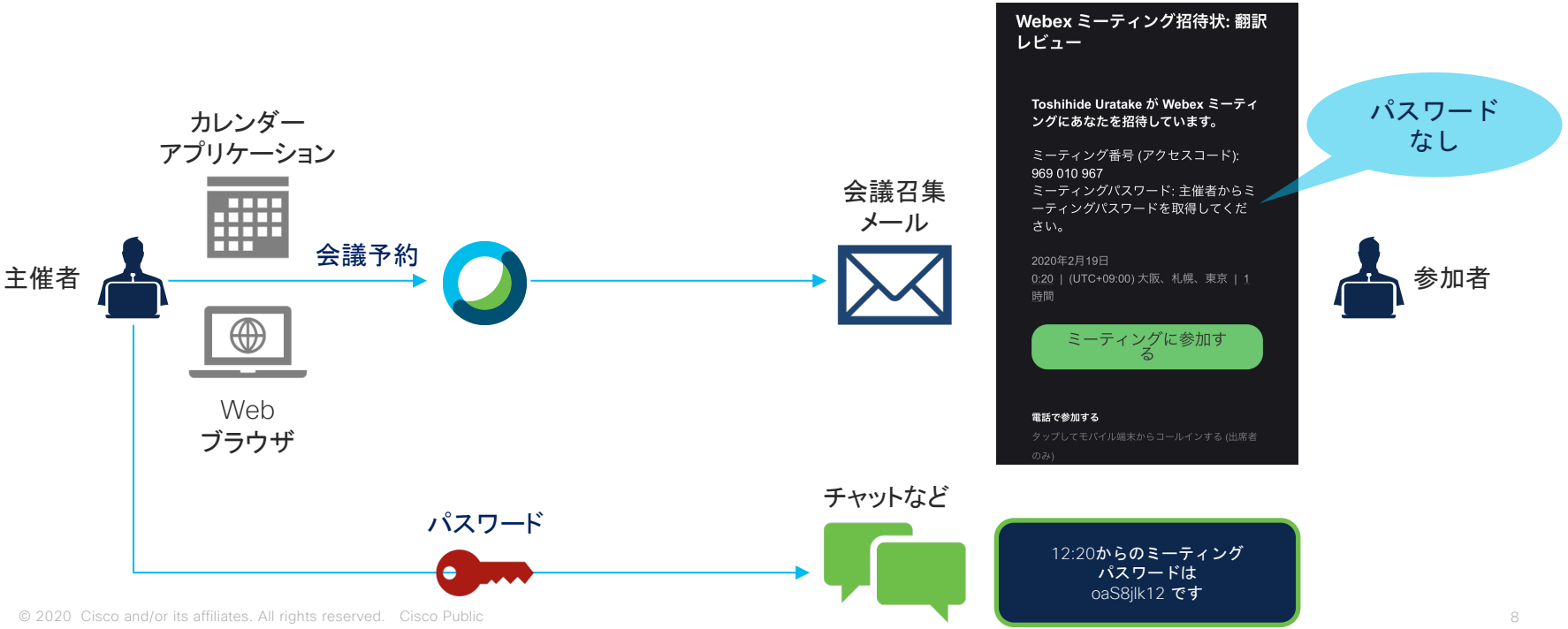
主催者向けの
ベストプラクティス

主催者

機密性の高いミーティングではパスワードを招待状に記載しない

パスワードを別の手段で参加者に伝達する

メールへの不正アクセスがあった場合でもミーティングへの不正な参加を防止できます



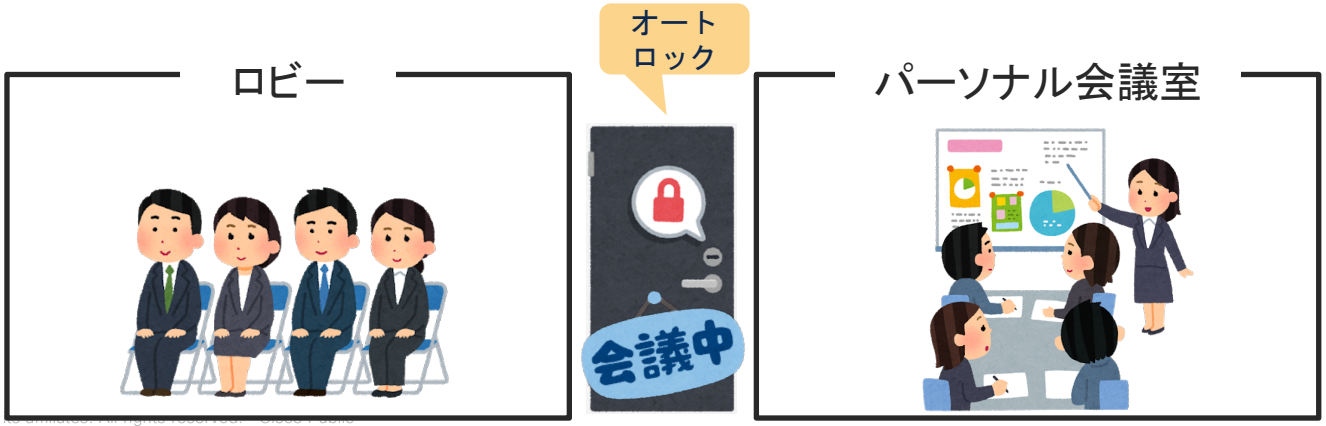
主催者

会議予約時の設定方法

ミーティングをロックする

パーソーナル会議室とロビー

- パーソナル会議室はWebex Meetingsにおいて会議を主催する権限を持ったユーザがそれぞれ持つことができる個人用の会議室です。
- 会議室のオーナーによって会議室をロックまたはロック解除することが可能です。
- 会議室がロックされている場合に参加者が会議に参加を試みた場合はロビーにて待機することになります。
- 会議開始後から一定時間経過後に自動的にロックする設定を行うことが可能です。



主催者が自分で自動ロックを有効化する方法

管理者が自動ロックのデフォルトを設定する方法

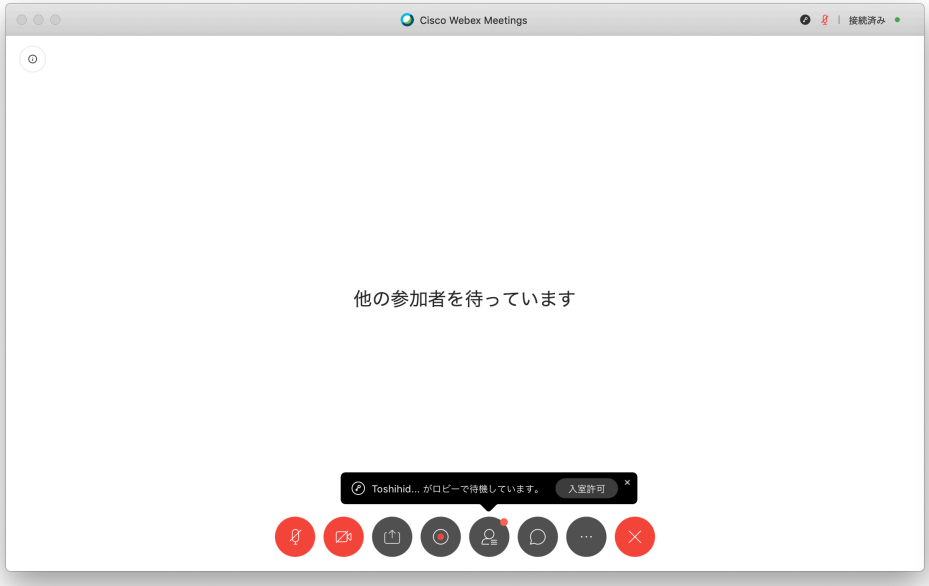
管理者は自動ロックを有効化していないユーザに対して自動ロックを有効化することが可能です

主催者

ロックされた会議へ参加者を追加する方法

[入室許可] ボタンを押して会議室への入室を許可します

参加者パネル非表示の場合の通知方法

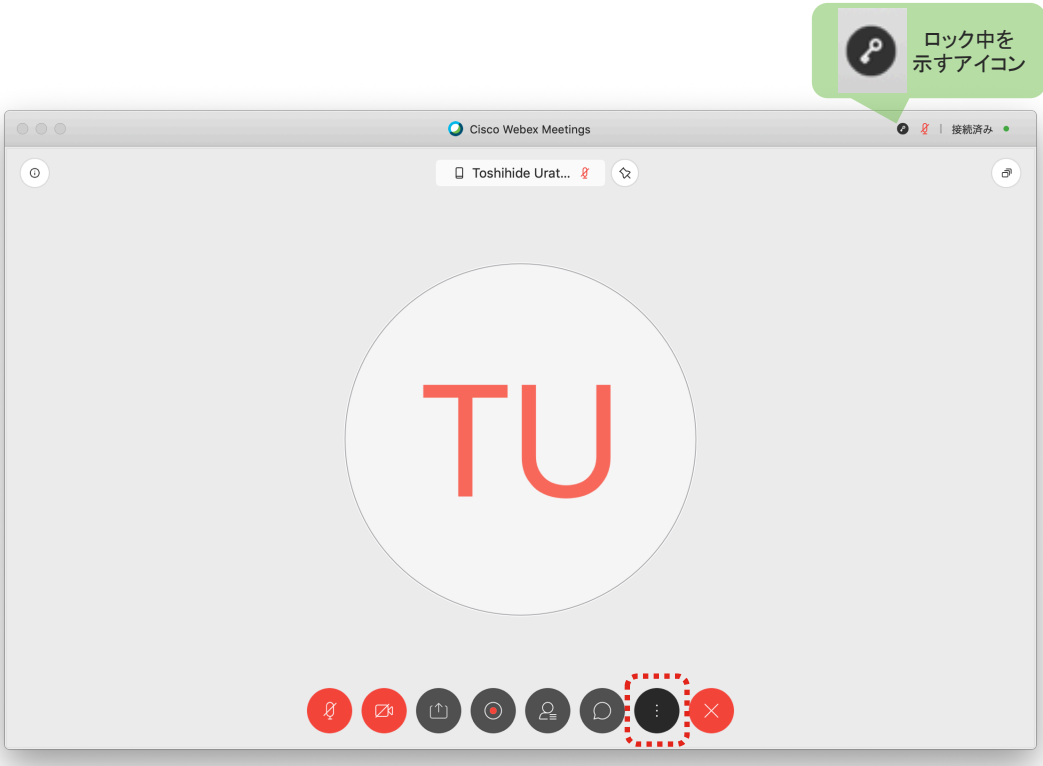


参加者パネル表示中の場合の通知方法

Cisco Webex パーソナル会議室をロックまたはロック解除する
https://help.webex.com/ja-jp/vjfafi/Lock-or-Unlock-Your-Cisco-Webex-Personal-Room

主催者

明示的に会議室をロックまたはロック解除する



会議がロック中の場合

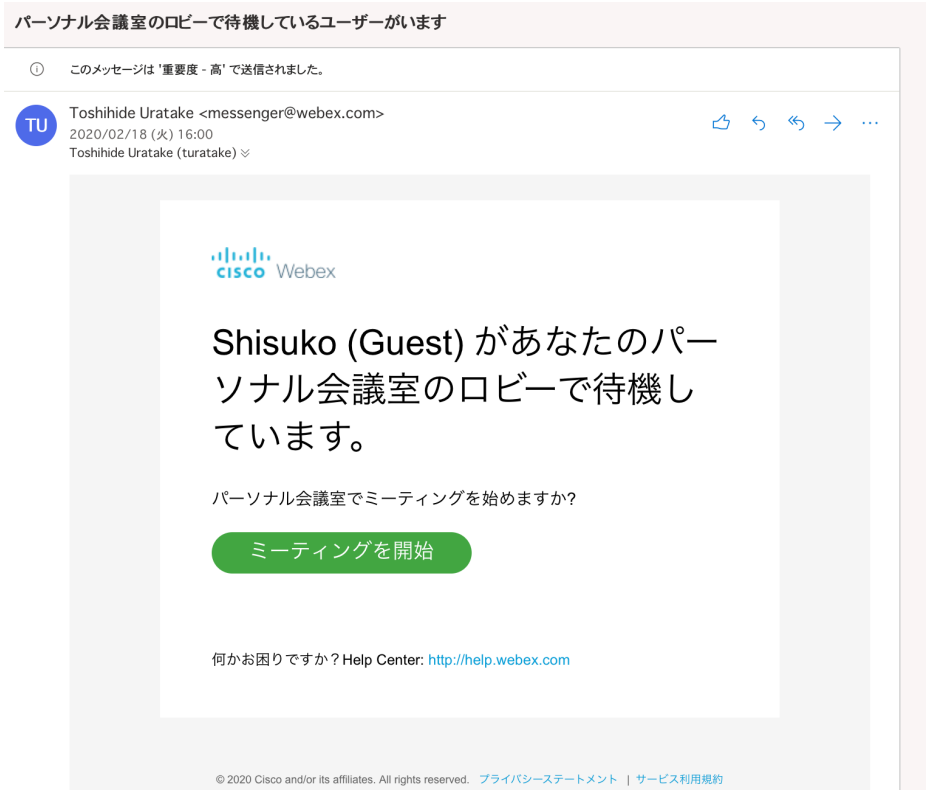
会議がロック解除中の場合

ロックされた会議に参加し、ロビーで待機する場合のユーザ体験

CAPTCHの入力が必要な場合があります

通知機能は無効に
することも可能です

[参考] 主催者への通知メールのサンプル

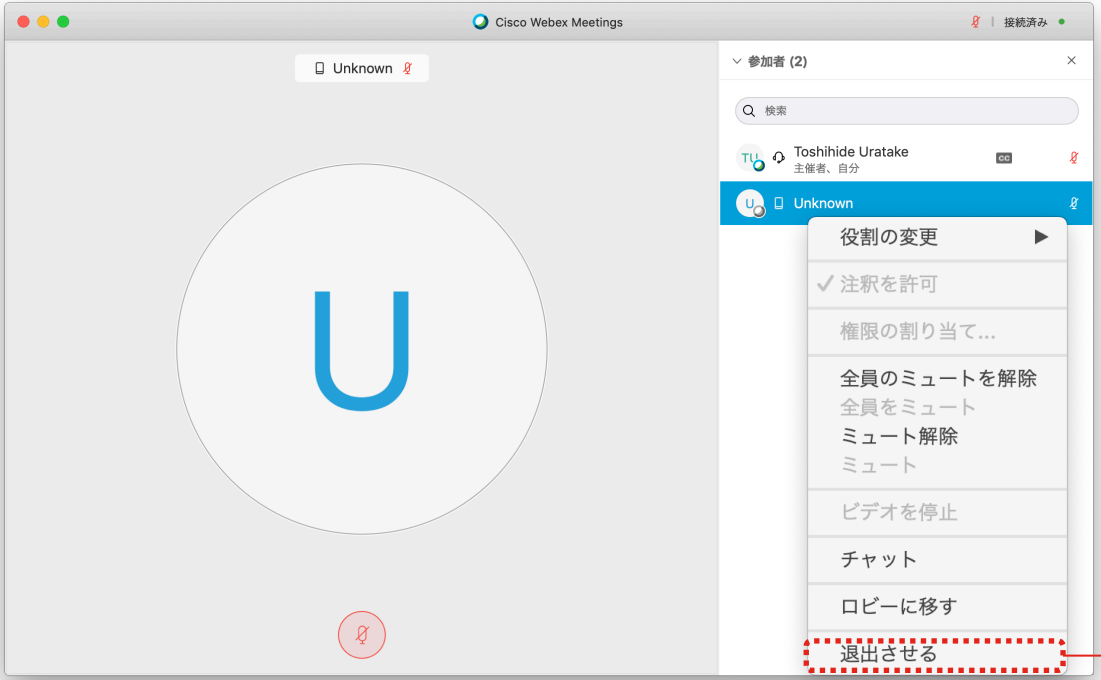


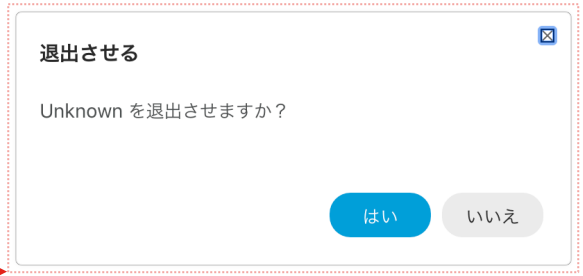
[参考] 主催者への通知を許可する設定方法

不明な参加者を会議室から排除する

正体不明な参加者を退出させる

参加者リストを確認しましょう。不明な参加者は退出させましょう。





会議の参加者をサインイン済みのユーザのみに制限する

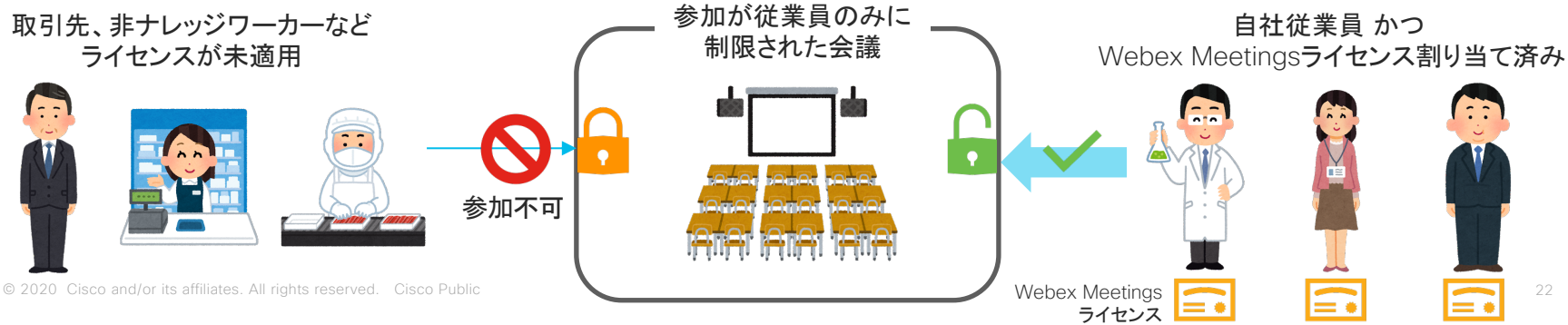
主催者

機密性の高いミーティング、イベント、トレーニングで Webex サイトのユーザー認証を要求する

会議の内容が社内の経営計画や人事異動などである場合に、(主催者だけではなく)参加者を社内の従業員のみに制限することが望ましいケースがあります。

その場合は会議のスケジュールを行う際に次の条件を満たすようにする必要があります。

- スケジュール会議として会議を予約する
- スケジューリングオプションにおいて [アカウントの要求] を有効にする



主催者

会議予約時にミーティングをアカウントの要求を設定する

管理者向けの
ベストプラクティス

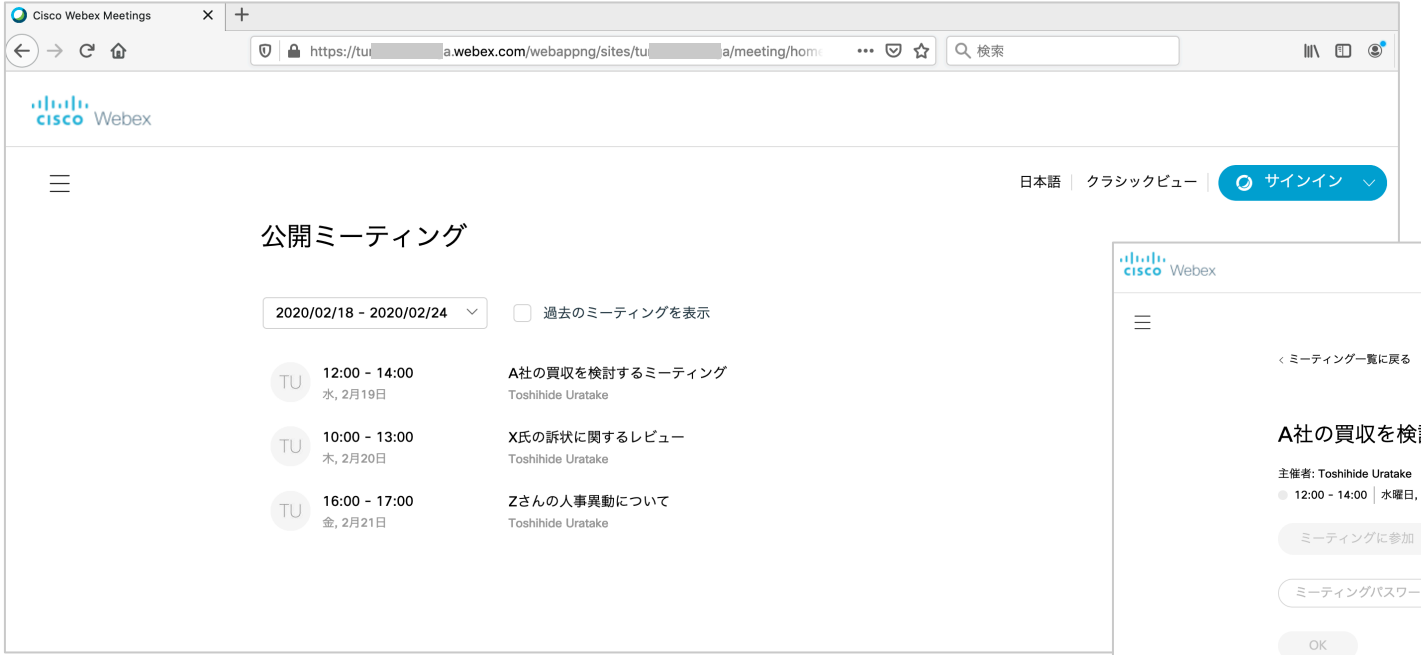
管理者

ミーティングの一覧表示を行わないようにする

管理者

会議の題名から重要な機密情報が。。。

未認証のユーザ (全く関係のない第三者など) も公開ミーティングを閲覧することが可能です。



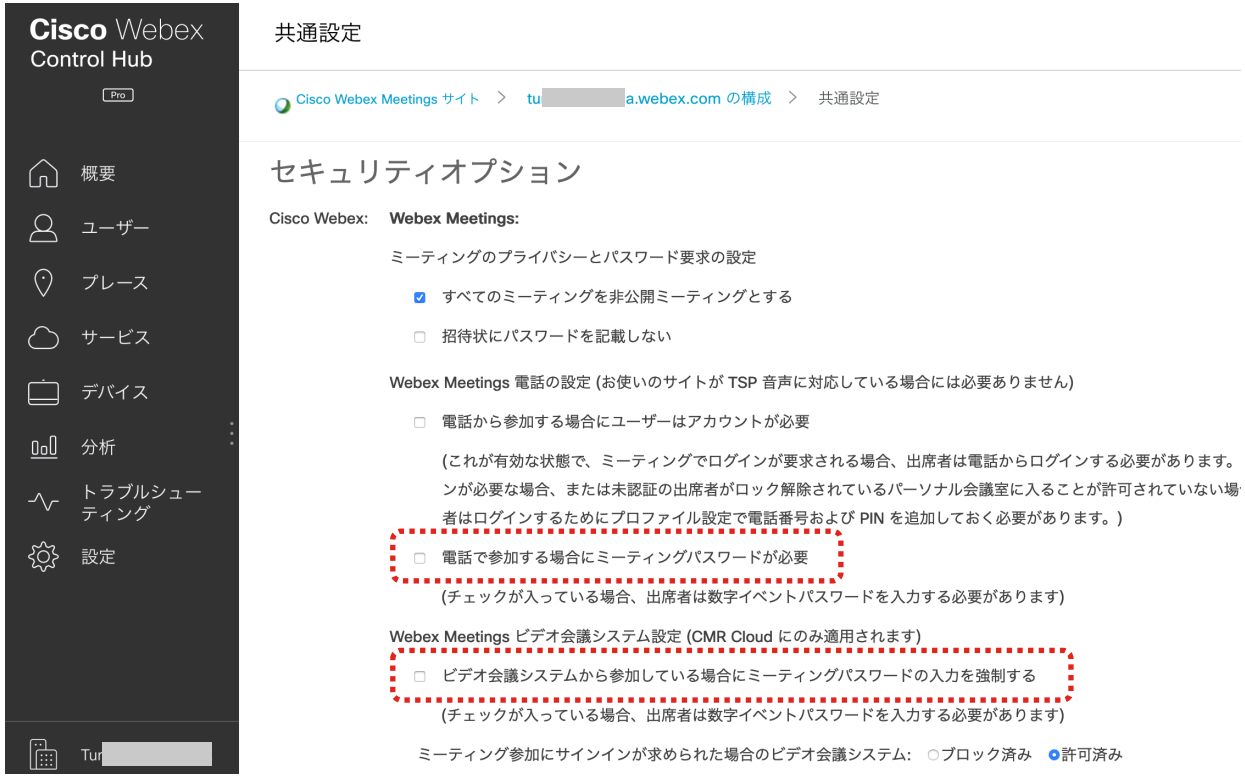
設定方法

管理者

ビデオ会議端末からの参加時にパスワードの入力を求めるようにする

管理者

設定方法

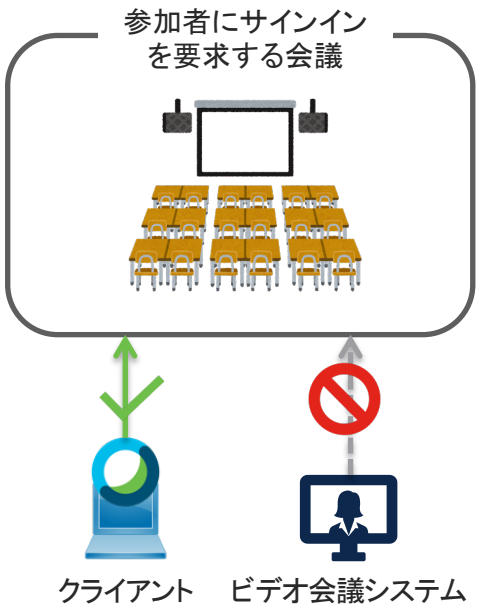


管理者

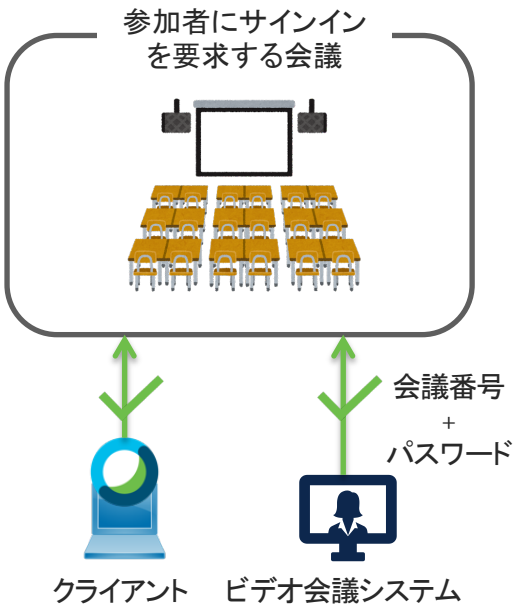
サインインが必要な場合にビデオ会議システムがミーティングに参加することを許可する

会議端末からサインインが要求される会議への参加を許可する

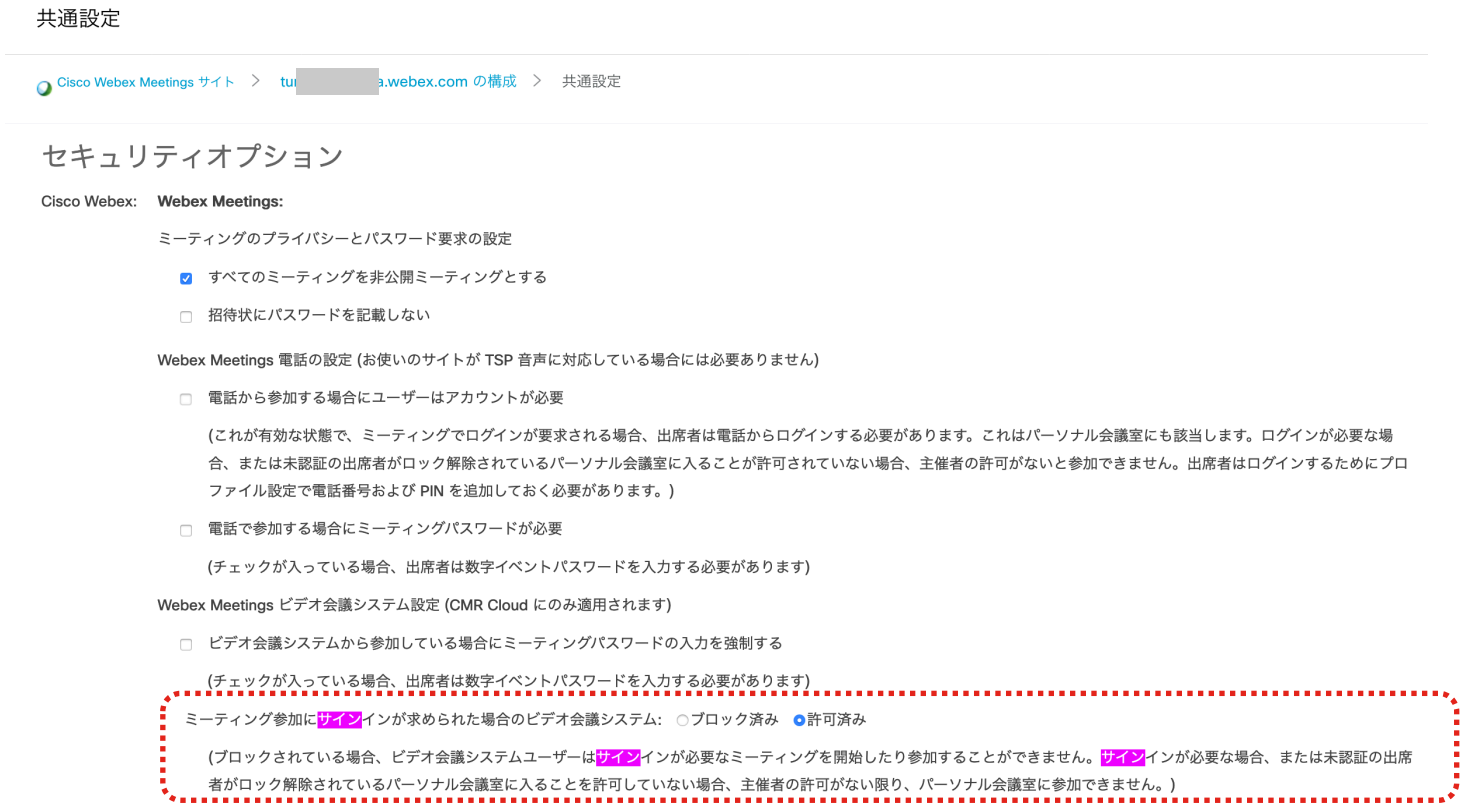
管理者によって参加を**ブロック**



管理者によって参加を**許可**



サインインを要求する会議にビデオ会議端末からの接続を許可する設定



管理者

ミーティングパスワードの複雑さを設定する

複雑なミーティングのパスワードを要求する

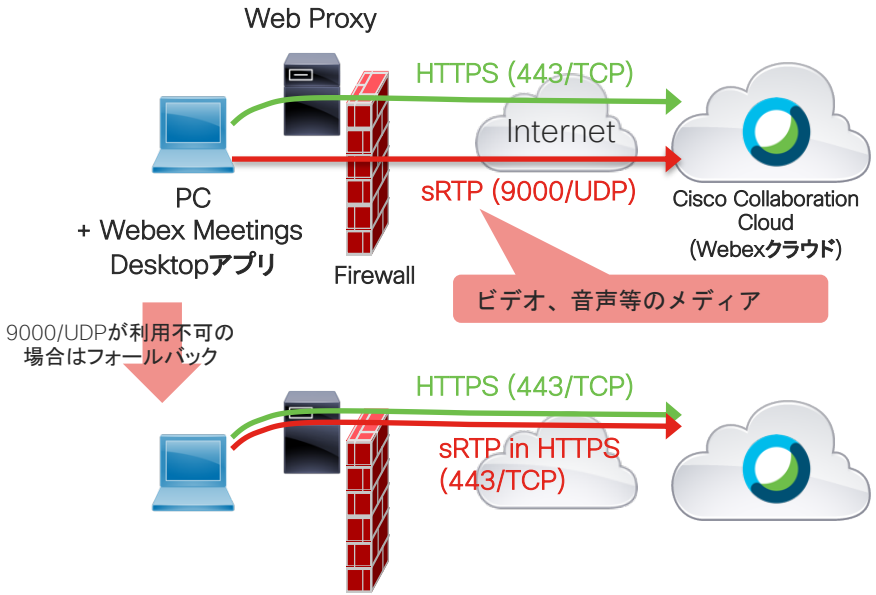
- ミーティングパスワードは主催者ユーザがそれぞれ設定します。
- 管理者はミーティングパスワードの複雑さを設定することが可能です。
- 会社名や製品名などをパスワードに含めることを禁止することも可能です。

Webex Meetingsの
ネットワーク要件に適応する
ためのセキュリティ対策

PCおよびモバイル機器のネットワーク要件 (概要)

https://help.webex.com/en-us/WBX264/Network-Requirements

- PCおよびモバイルデバイスなどWebex Meetingsのクライアントから Webex Meetingsへ接続する場合の要件です。
- 音声やビデオなどのメディアは9000/UDP, 443/TCPなどを利用して送受信されます。
- ネットワーク側の対応：
  - FWは内側 (LAN/WAN) から外側 (Internet) という方向にのみトラフィックを許可するだけでOK
  - RTPは9000/UDPが利用できない場合は443/TCPへとフォールバックします。(品質が大幅に劣化します。)
- 443/TCPを利用する場合、つまりProxyを通過する場合は音質および画質が大きく劣化します。9000/UDPをぜひご利用ください。
- 名前解決のためにDNSの参照が必要です。



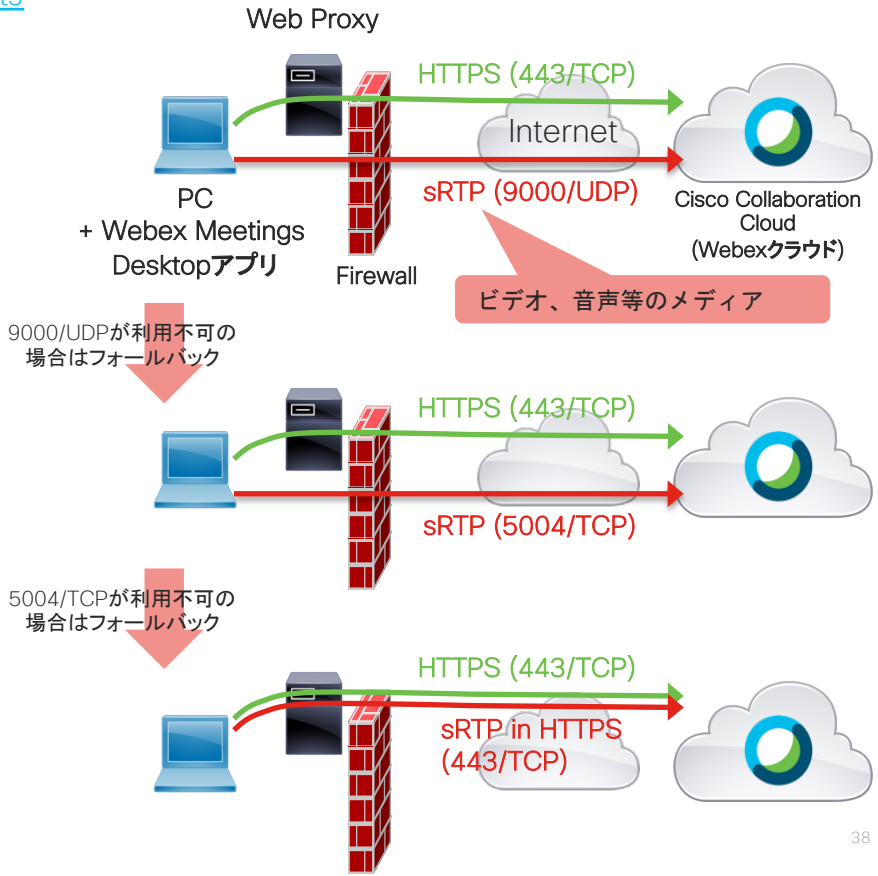
ビデオ会議ではUDPが一般的に必要とされています

	宛先UDPポート	必要とされている理由
Cisco Webex Meetings	9000	“メディア ポートを構成する際には、TCP に対して UDP が推奨されます。”
A社	3478 - 3481	“必要なメディアポートであり、開く必要があります。”
B社	3478 - 3479 8801 - 8810	Cisco社内での検証ではUDP->TCP->443と次第にフォールバックを行うことを確認しています。
C社	5000 - 5999	“If the above ports are not open, calls may connect, but can lead to quality issues with video, audio and content sharing”
D社	40000 - 49999	“softclient uses UDP/RTP for media normally, as this is the optimal protocol traffic type for real-time traffic. ”

PCおよびモバイル機器のネットワーク要件 (概要)

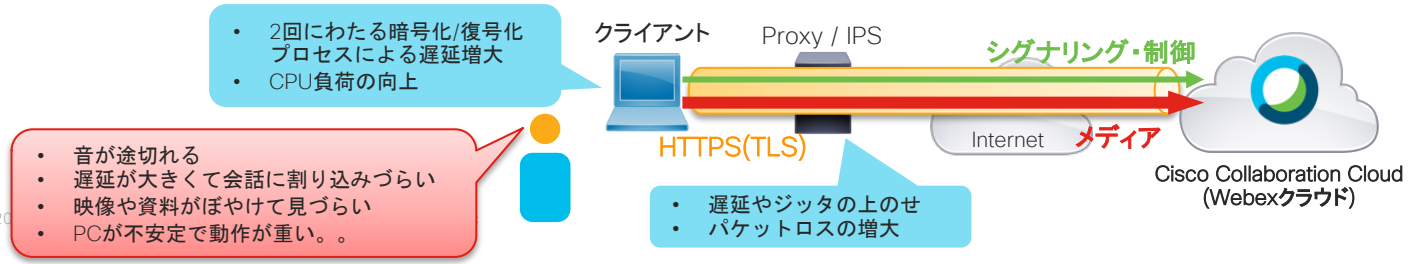
https://help.webex.com/en-us/WBX264/Network-Requirements

- PCおよびモバイルデバイスなどWebex Meetingsのクライアントから Webex Meetingsへ接続する場合の要件です。
- 音声やビデオなどのメディアは9000/UDP, 5004/TCP, 443/TCPなどを利用して送受信されます。
- ネットワーク側の対応：
  - FWは内側 (LAN/WAN) から外側 (Internet) という方向にのみトラフィックを許可するだけでOK
  - RTPは9000/UDPが利用できない場合は5004/TCPへとフォールバックし、さらに5004/TCPが利用できない場合はさらに443/TCPへとフォールバックします。(次第に品質が劣化します。)
- 443/TCPを利用する場合、つまりProxyを通過する場合は音質および画質が大きく劣化します。9000/UDPをぜひご利用ください。
- 名前解決のためにDNSの参照が必要です。



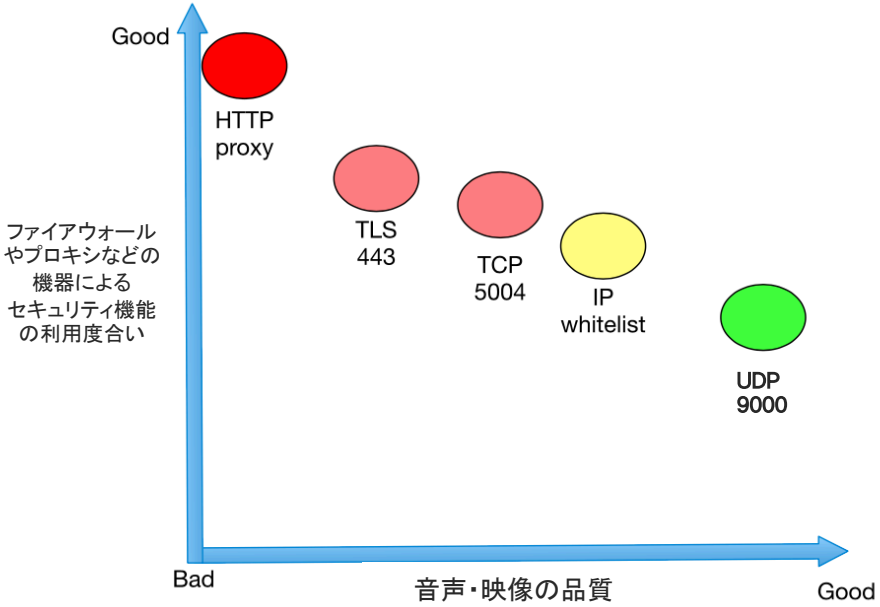
9000/UDPおよび5004/TCPを利用すべき理由

- プロキシなどが行なっているトラフィックシェイピング（バッファリングや廃棄）してしまうことにより伝送中のメディアが大きく劣化してしまう問題を回避できます。
- Webex MeetingsとWebex Teams (Webex登録デバイスはWebex Teamsのサービスを利用します) の双方のサービを利用される場合、ネットワーク側で5004だけを許可することで、Webex MeetingsおよびTeamsのアプリ、Webex登録のデバイスなどの全てについてある程度最適化されるます。それにより最小限の設定で高品質のビデオ通話を実現でき、管理の手間が減ります。
- 音声およびビデオをSRTPのストリームにエンコーディングする際に1回、それに加えてTLSのトンネル内で送信する際にもう一度暗号化するというように合計2回暗号化プロセスが実行されるオーバーヘッドを回避できます。
  - クライアントの負荷が下がります。
  - 暗号化プロセスによって発生するさらなる遅延などを回避できます。
- また、5004/TCPであっても、パケットロス発生時に送受信するOSやアプリケーション等によって再度同じTCPパケットを送信することによるデメリット（トラフィックの増大や音質の低下など）は9000/UDPより相対的にまだ課題が残ります。



ビデオ・音声の品質とセキュリティのトレードオフ

- Webexクライアントはネットワークの状況に合わせて音声メディアを適切なポートを利用して送受信します。
- ビデオや音声の品質が最良となるのは9000/UDPのポートを利用する場合です。
- 443/TCPでは品質が著しく低下し、HTTP proxyはさらに低下します。
- ビデオや音声のメディアについてはファイアウォールや侵入検知システムなどを経由しないようにすることを推奨します。
- それらの機器は遅延やジッターに大きな影響を受けるメディアの処理に対して十分な帯域や処理速度を提供することが困難です。（あるいは、十分な性能を持つそれらの製品は非常に高価です。）



セキュリティとメディアの品質の関連性

ファイアウォールに関して考慮すべきこと

- DPI (Deep Packet Inspection) はパケットをパフォーマンスに影響を与える可能性があります。リアルタイムメディア（音声やビデオ）に遅延やジッターをもたらし、品質の低下する、フリーズ、ぎくしゃくしたビデオが発生します。
- FWのCPU使用率が高い場合、パケットは効果的にランダムに破棄されやすくなり、ビデオ品質が大幅に低下します。
- 安全なWebexクラウドへのSIP/TLSコールなどの暗号化されたトラフィックに対しては一般的に役に立ちません。

シングルサインオンと
多要素認証

PCまたはモバイルデバイスについては会社支給のもののみに制限する

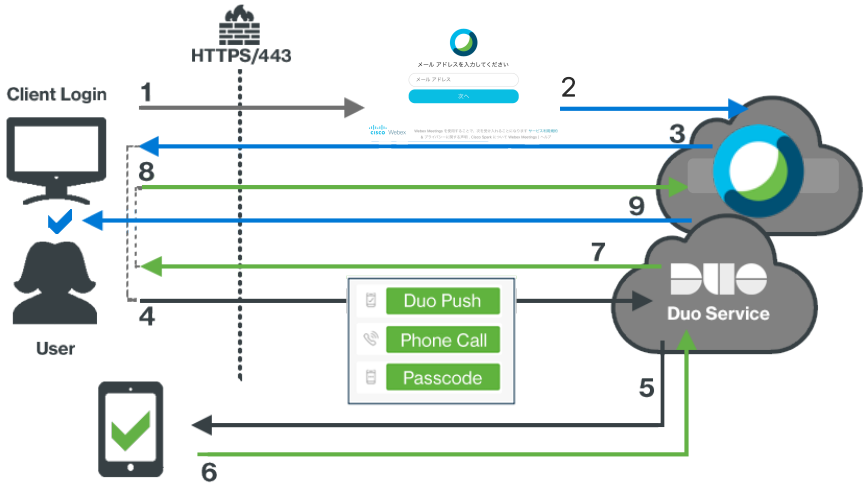
多要素認証をサポートするIdPと統合してください

- Webexは多要素認証 (MFA) やデバイスの認証 (デバイスに特定の電子証明書が格納されているかどうかなど)のような機能は備えていません。
- そのような認証が必要な場合は、必要な認証の機能を備えるIdPとWebexの組織 (またはWebexサイト) との間でSSOインテグレーションを有効にし、ポリシーをIdP側で実装してください。

Cisco DuoをIdPとして利用する例

Cisco Webex (SP) とCisco Duo (IdP) を利用して多要素認証を行う場合の例：

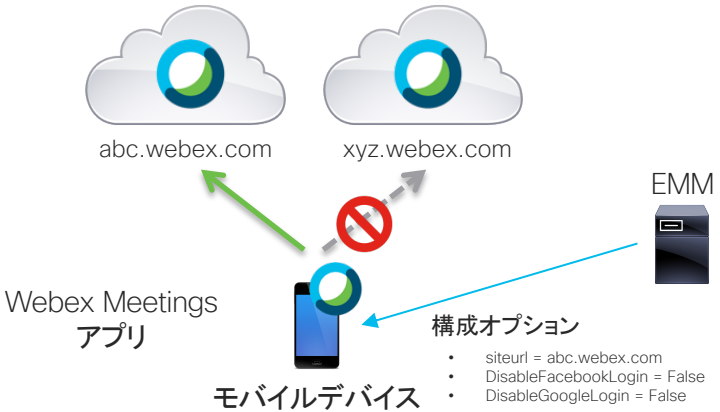
1. Webexにアクセスし、メールアドレスを入力する画面が表示される
2. メールアドレスを入力して送信
3. Webexサイトで設定されたSAML IdP (Duo)へリダイレクト
4. Duoの認証方式を選択
5. モバイルデバイスに認証リクエストをプッシュ
6. Duoサービスが認証の承認結果を返す
7. 2つ目の認証結果がユーザに返される
8. WebexにDuoの認証結果を返す
9. Webexがユーザのライセンスをもとに適切な機能の利用を許可



EMM/MDMによる
モバイルアプリの一括設定

EMM/MDMによるモバイルアプリの一括設定

- AirWatchやMicrosoft Intuneのようなエンタープライズモビリティ管理 (EMM) ソフトウェアでiOSおよびAndroidのWebex Meetingsアプリを構成することが可能です。
- Webex Meetings Desktopアプリからログインするwebexサイトを自社が利用するものに制限することも可能になります。



構成オプション

構成キー	値の種類	説明
DisableFacebookLogin	ブール値 (True または False)	ユーザーが Facebook アカウントにサインインすることを許可する。
DisableGoogleLogin	ブール値 (True または False)	ユーザーが Google アカウントにサインインすることを許可する。
DisableO365Login	ブール値 (True または False)	ユーザーが Office 365 アカウントにサインインすることを許可する。
DisableMeetingNotification	ブール値 (True または False)	開催予定のミーティング通知が送信されたかどうかを指定します。
DisableVideoSending	ブール値 (True または False)	ミーティング中にユーザーがビデオを送信することを許可します。
DisableWebexCalendar	ブール値 (True または False)	Webex カレンダーからミーティングを一覧表示することを許可します。
DisableNativeCalendar	ブール値 (True または False)	デバイス カレンダーからミーティングを一覧表示することを許可します。
DisableO365Calendar	ブール値 (True または False)	Microsoft Office 365 カレンダーからミーティングを一覧表示することを許可します。
DisableDeviceConnection	ブール値 (True または False)	ビデオ デバイスが Webex Meetings に接続することを許可します。
DisableAutoDeviceConnection	ブール値 (True または False)	ビデオ デバイスが Webex Meetings に接続することを許可します。
EnableBlockRootedDevices	ブール値 (True または False)	ルートデバイスで Webex Meetings を使用できるかどうかを指定します。
EnableForceLogin	ブール値 (True または False)	ユーザーがユーザーの Webex Meetings にサインインする必要があるかどうかを指定します。
siteurl	文字列	サインイン用のサイト URL を指定します。

モバイル デバイスの管理を使用して Cisco Webex Meetings を設定する
https://help.webex.com/ja-jp/nafabti/Use-Mobile-Device-Management-to-Configure-Cisco-Webex-Meetings


CISCO