Webex
セキュリティリファレンスガイド

シスコシステムズ合同会社
コラボレーションアーキテクチャ事業

webex by CISCO

はじめに

2020年初頭に始まった新型コロナウィルスの広がりから約3年が経ち、その間、世界中の多くの人々が場所の移動を制限されたことで、在宅勤務やハイブリッドワークを導入する企業が急増し、同僚やビジネスパートナー、そしてお客様とオンラインで繋がって仕事をすることが当たり前の時代になりました。そんな状況の中、オンライン環境を支えるコラボレーションソリューションがいかにセキュアで、安心して利用できるものであるかは、それを導入する企業や組織にとって、基本的で重要な関心事項となっています。

シスコは、セキュリティをネットワーク、プラットフォーム、およびアプリケーション　の設計、開発、導入、メンテナンスにおける最優先事項に位置付け、最も厳しいセキュリティ要件が設けられている場合でも、Webexなら自信を持ってビジネスプロセスに組み込むことができます。

本書では、重要な投資決定を行う際に役立つ、Webexおよびその基盤となるインフラストラクチャのセキュリティ対策、およびシスコのコンプライアンスに対する取り組みについて説明します。その内容をご理解いただき，安心してWebexをご利用いただくための一助となれば幸いです。

シスコシステムズ合同会社
コラボレーションアーキテクチャ事業

Webex security and compliance overview

- セキュリティの仕組み
- セキュリティに対する取り組み
- ベストプラクティス

安全な
ユーザーアクセス

ユーザーアクセスはWebexにアクセスするユーザーのIDを認証するところから始まります。認証方法にはSAML SSOがあり、この場合、Webexは顧客のパスワードを保存せず、認証のためにIdPを参照します。多要素認証は無料のHOTPベースの認証でサポートされており、お客様は業界をリードするCisco Duo Securityを使用してゼロトラストを追加することができます。管理者のために、Webexは役割ベースのアクセス制御（RBAC）をサポートしており、お客様は適切な管理者に適切な特権を簡単に割り当てることができます。

- ユーザー登録と削除の自動化（SCIMまたはAD Sync）
- お客様が選択したIDプロバイダーによるシングルサインオン
- Cisco DuoまたはHOTP Authenticatorを介したMFA
- 標準的なOAuth 2.0ベースの認証
- 匿名化されたユーザーID
- ロールベースの機能アクセス制御
- 管理権限の委譲
- トークンおよび SSO 証明書の管理

コンテンツと ストリーミングメディア の保護

エンドツーエンドの暗号化により、お客様のWebexコンテンツは全て安全に保護されます。検索も安全に暗号化されるため、Webexがコンテンツを複合化されることはありません。クラウドでの鍵管理だけでなく、お客様は暗号鍵を構内に保管するオプションもあり、究極のコントロールを実現します。エンドツーエンドの暗号化された会議オプションにより、お客様は会議の暗号化キーを独占的に管理でき、シスコや誰もが会議のコンテンツにアクセスできなくなります。

- 12年以上にわたる会議のエンドツーエンド暗号化
- 静止時および転送時の暗号化（TLS1.2）
- メッセージ、ファイル、ホワイトボードのエンドツーエンド暗号化
- 個別の暗号化キーにより、侵入された場合でもデータが安全
- 暗号化されたデータをインデックスに表示
- ロールベースの機能アクセス制御
- セキュリティ強化のため、お客様側でスペースの暗号化キー管理が可能

データ損失防止（DLP）

データ損失防止（DLP）は重要な情報が悪意を持って、または誤って会議やメッセージングで共有されるのを防ぐ必要がある多くの企業にとって大きな関心事となっています。Webexのミーティングやスペースで共有された全ての情報は、Webex　Events　APIを介してサードパーティのDLP&アーカイブソリューションと統合することが可能です。お客様はポリシーに違反した場合、メッセージの削除やユーザーへの通知など適切なアクションを定義することができます。

- ミーティングおよびメッセージングに対する組織横断ポリシー
- 会議内容、スペースに投稿されたメッセージやファイルの追跡
- スペースや会議プラットフォームに追加されたユーザー追跡
- スペースにいる不要なユーザーをコントロール
- スペース内の機密情報の偶発的な共有の回避
- 社外の人と仕事をする際の情報の安全性確保
- Cisco　Cloudlockやサードパーティベンダーなど、業界をリードするCASB/DLPプロバイダーによるポリシー適用

Webexアプリとデバイスのセキュリティ

どのデバイスを使用していても、Webexで作成された全てのコンテンツはキャッシュされたものも含めエンドツーエンドで暗号化されています。PINロックにより、誰かがPINなしでアプリを起動することもできません。お客様はControl　Hubを使ってどのユーザーがファイルをアップロードおよびダウンロードできるかを簡単に制御できます。モバイルデバイスのワイプとはデバイスの紛失や盗難または誰かが組織を離れた場合に全てのコンテンツが消去されることを意味します。

- Control Hubにネイティブな MDM機能
- リモートワイプ
- PINロック
- 強制ログアウト
- ファイル共有コントロール
- 静止データの暗号化（デスクトップ、モバイル）
- エンタープライズHTTPプロキシのサポート
- ユーザー/デバイスの認証
- 通知ブロック
- Microsoft Intune SDKとMDMアプリの設定サポート

法律・規制への対応

企業内のユーザーが調査や訴訟に巻き込まれた場合、お客様はeDiscovery機能を使って簡単にデータを検索することができます。また、これらの調査に対応するために独自の保存ポリシーを定義し、ユーザーを法的保留にすることができます。Webexの主な差別化ポイントは、統一された使いやすいコンプライアンスツールを提供できることです。このツールは、会議のコンテンツ（議事録、ハイライト、録音/録画）とメッセージングのコンテンツ（メッセージ、ファイル、スペース内で共有されるホワイトボード）の両方にスムーズに対応し、企業のコンプライアンスを遵守するために使用されます。

- ミーティングとメッセージングの企業保存ポリシーを定義する
- eDiscovery検索・抽出ツールを使用した会議およびメッセージングコンテンツの検索
- ミーティングとメッセージングのリーガルホールドによる保存ポリシーのオーバーライド
- クラウドセキュリティの法令遵守に必要な認定をサポート
- クラウドセキュリティのに法令遵守に必要な規制をサポート

ITの権限強化

Webex Control Hubを利用することで、管理者はユーザーが利用できる機能を簡単に管理し、セキュリティプロファイルを定義することができます。また、管理者ログを閲覧することで、不正な設定変更が行われた場合の対応を確認することができ「誰が何をしたのか」を確認することができます。このサービスは、ミーティング、通話、デバイス、コンタクトセンターのサービスパフォーマンスを識別するのに役立つ詳細な分析など、Control Hubの他の機能と組み合わされ、IT部門が問題を迅速にトラブルシューティングし、ユーザーに優れたサービスを提供することを可能にします。

- 外部からの通信ブロック
- 承認されたドメインからの外部通信許可
- スペースでのGIFの使用を有効/無効
- ファイル共有コントロールによる機密情報の共有リスク低減
- 社内ネットワークに接続していない時のファイル共有防止
- 管理者監査ログによるアクティビティの記録
- ミーティング、メッセージング、通話などの詳細な分析

Transport Layer Security（TLS）

WebexサービスはTLSバージョン1.2および1.3のみを使用し、以下の暗号をサポートします。

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

ECDHE :楕円曲線ディフィー・ヘルマン鍵共有
RSA :証明書 (2048ビット鍵サイズ)
AES_256：NSA最高機密の暗号化強度
AES_128：NSA秘匿暗号強度

詳細は[こちら]

エンドツーエンド暗号化

エンドツーエンド暗号化によりWebexアプリとデバイスで生成される全ての会議データ（音声、ビデオ、チャットなど）は、ローカルで取得された会議暗号化キーで暗号化されます。このようにして暗号化されたデータはWebexサービスで複合化できません

コンテンツ（メッセージ、ファイル、スペースタイトルなど）はGCMモードの対称型AES256で暗号化

クライアントと鍵管理の通信は、セッションごとのEC鍵による楕円曲線ディフィー・ヘルマン鍵交換によって保護されます

詳細は[こちら]

Webex security and compliance overview

- セキュリティの仕組み
- セキュリティに対する取り組み
- ベストプラクティス

セキュリティに対する360度アプローチ

Webex

Webexは、大企業から中小企業までクラウドコラボレーションにおけるセキュリティとコンプライアンスに対応しています。Webexはユーザー、コンテンツ、アプリケーション、デバイスをネイティブに保護する360度の総合的なアプローチにより社員がどこで誰と働いていてもデータの安全性とセキュリティを確保します。

データ保持ポリシー、eDiscovery、リーガルホールド機能により、コンプライアンス、規制、法的ニーズを満たすことができます。

セキュアな開発プロセス

Webex

シスコでは、セキュリティを補完的なものではなく世界クラスの製品やゼロから構築して提供するための統制のとれたアプローチとして採用しています。

全てのシスコ製品開発チームはCisco　Secure Development　Lifecycleに従う必要があります。これはシスコ製品の復元力と信頼性を向上させるための測定可能なプロセスです。Webex製品開発チームは、製品開発のあらゆる側面でこのライフサイクルに積極的に従います。

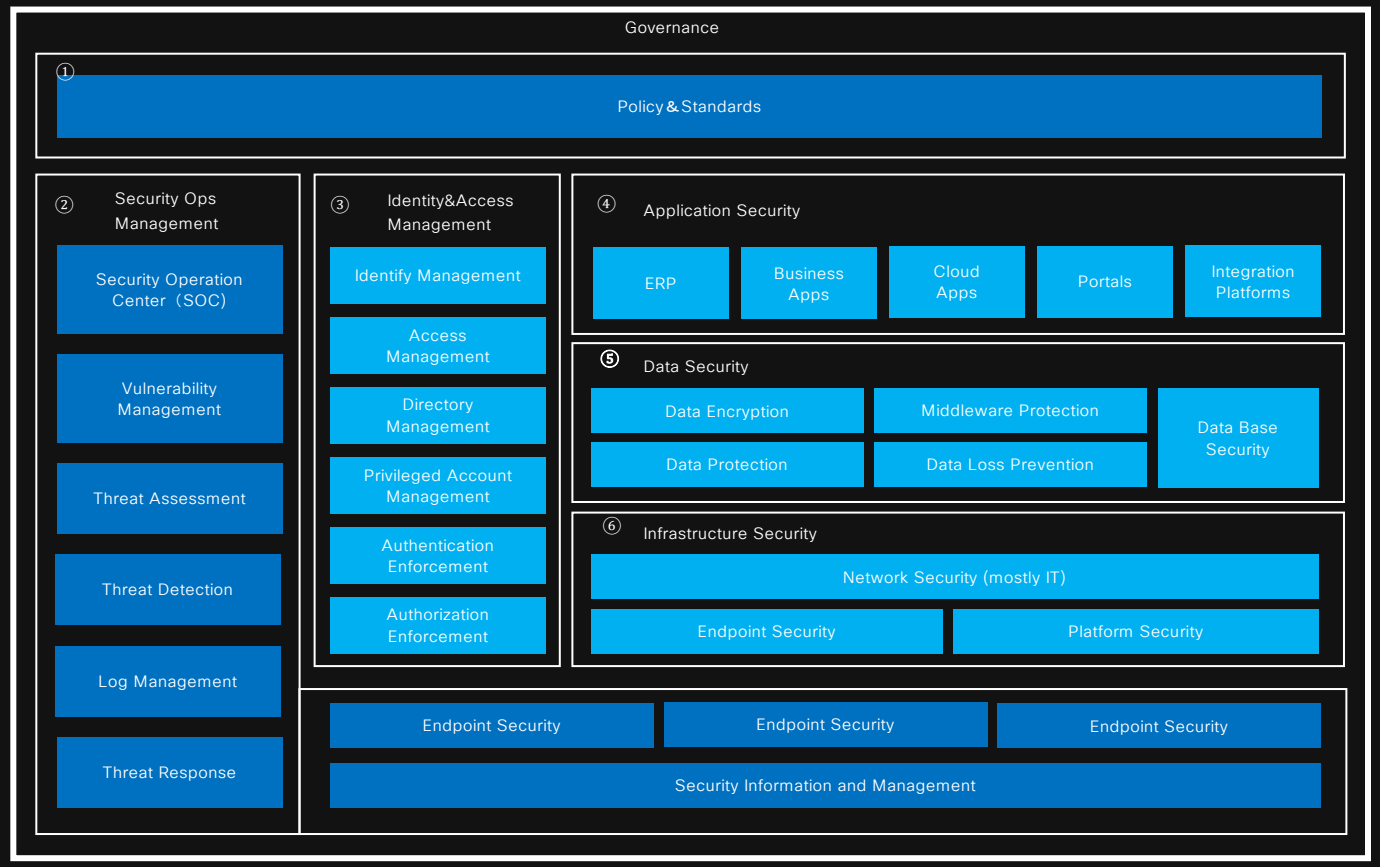
CISCO SECURE DEVELOPMENT LIFECYCLE(CSDL)

シスコの包括的セキュリティ組織「InfoSec」

Webex

クラウドのセキュリティ最高責任者が率いる「InfoSec」は、お客様に安全なWebex環境を提供する責任を担っています。

InfoSecでは、セキュリティのプロセスおよびツールを定義し、Webexのお客様への提供に関与する全ての部門にそれを適用することで、安全なWebex環境を提供しています。さらにCisco InfoSec Cloudはシスコの他チームと連携し、Webexサービスに対するあらゆるセキュリティ上の脅威に対応します。



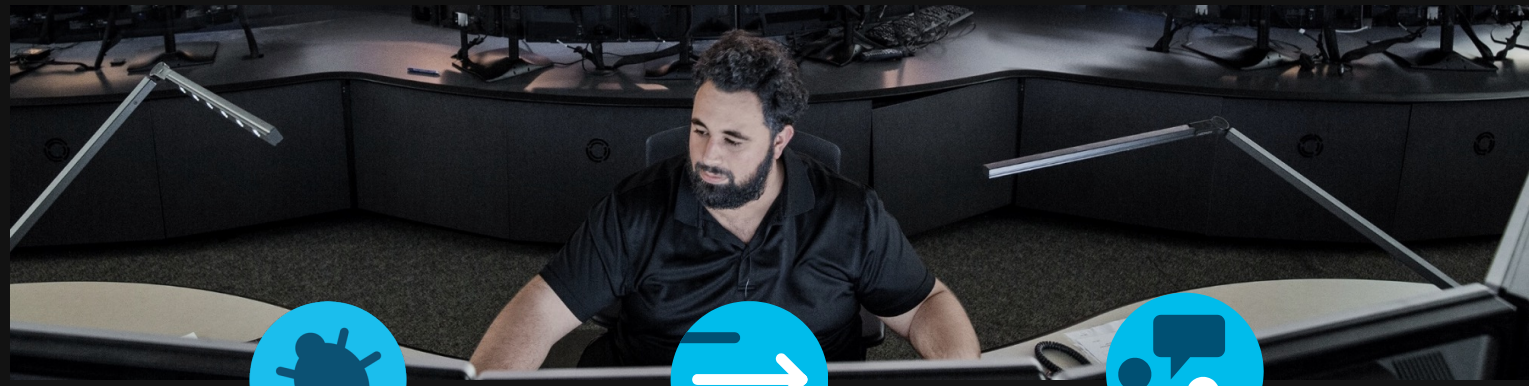
包括的なセキュリティ組織「InfoSec」

PSIRT（Product Security Incident Response Team）

Webex

Cisco PSIRTは、シスコの製品とサービスに関係するセキュリティ問題の流入、調査、およびレポートを管理する専門のグローバルチームです。

PSIRTはセキュリティ問題の重大度に応じてさまざまなメディアを使用して情報を後悔します。PSIRTは共通脆弱性評価システム（CVSS）のスケールを使用し、発見された問題の重大度をランク付けします。PSIRTはエクスプロイトの作成に役立つような脆弱性の詳細情報は公開しません。



脆弱性管理

インシデント
レスポンス

プロアクティブ
対応

内部/外部 ペネトレーションテスト

Webex

内部の評価者による厳格なペネトレーションテストを定期的に行います。また、Cisco Infosecでは、独立したサードパーティに、シスコの社内ポリシー、手順、およびアプリケーションに対する厳格な監査の実施を依頼しています。

サードパーティベンダーを通じて継続的かつ詳細なコードによるペネトレーションテストとサービス評価を実施しています。Infosecは、必要に応じてこれらのベンダーから証明書を提供できます。

脆弱性の特定

対応

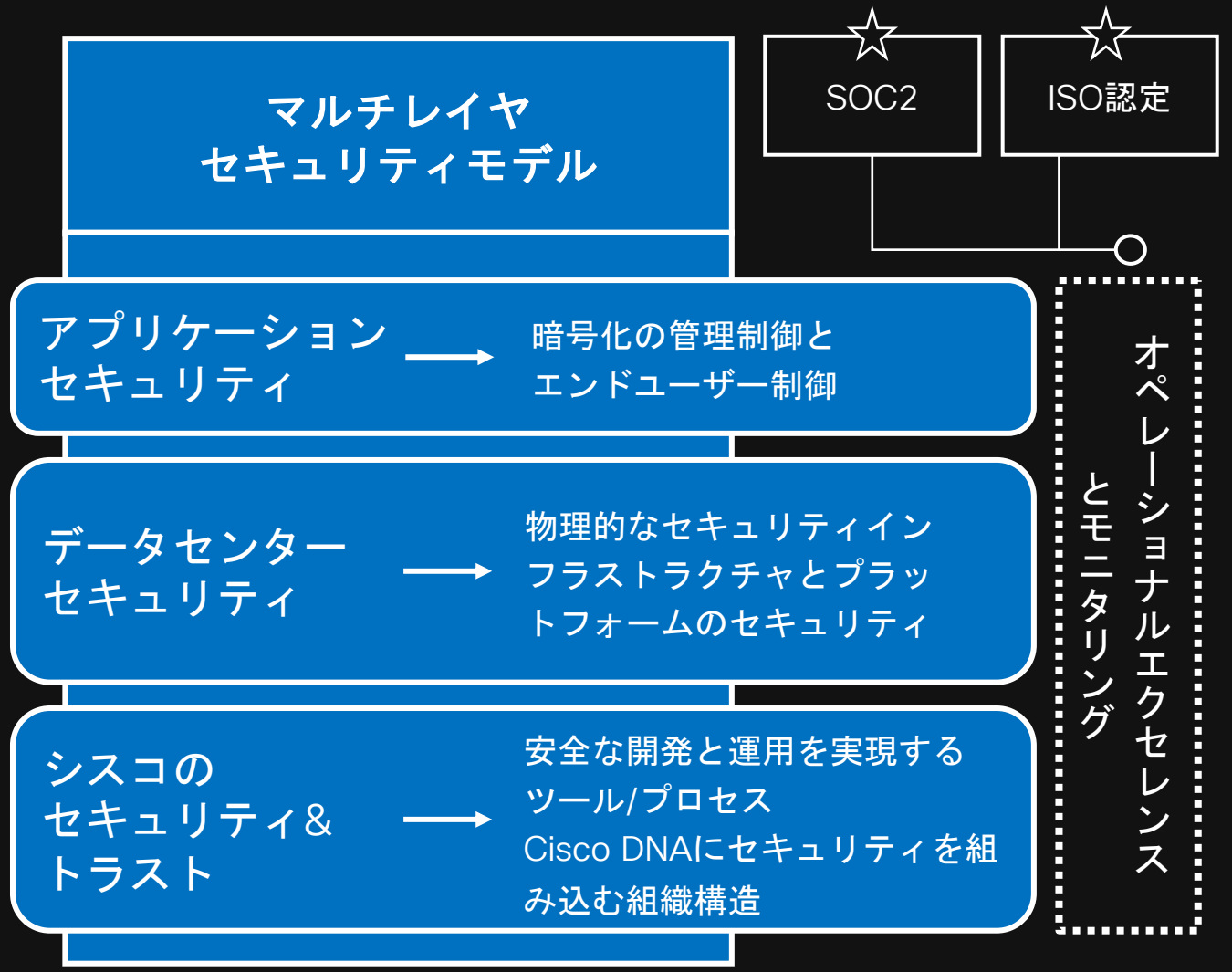
Application Penetration Test

Webex セキュリティモデル

Webex

シスコのSecure & Trust部門は社内全体のチームと連携し、コアインフラストラクチャの設計、開発、運用をサポートするフレームワークにセキュリティ、信頼性、および透過性を提供します。

また、サーバーセキュリティのリスクを軽減し管理するために必要な情報をお客様に提供することにも取り組んでいます。Webexのセキュリティモデル（図１）は、シスコのプロセスに深く刻み込まれたセキュリティ基盤を土台としています。



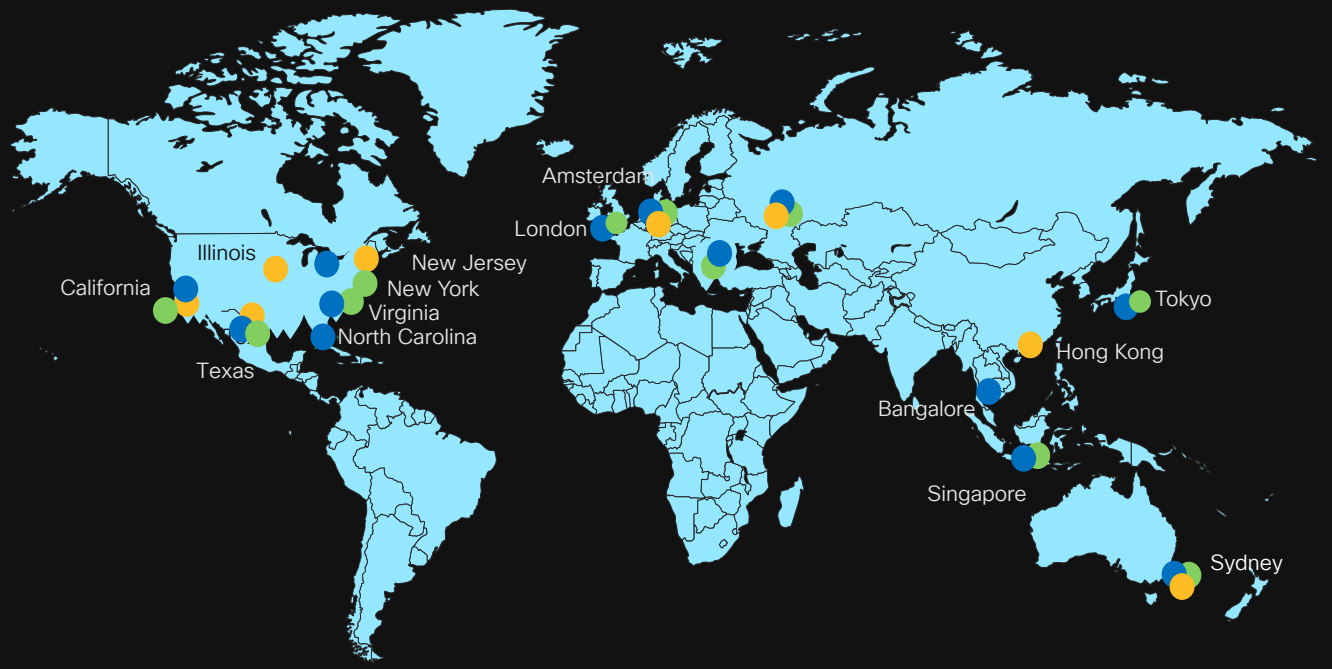
（図１）

クラウドアーキテクチャ

Webex

Webexは、業界をリードするパフォーマンス、統合性、柔軟性、拡張性、および可溶性を備えた非常に安全なサービス配信プラットフォームであるWebexクラウドを通じて提供されるSaaSソリューションです。

Webexクラウドサービスの大半にはシスコのデータセンターが使用されていますが、SOC2やISOに準拠しているAmazon Web Service (AWS) とMicrosoft Azureデータセンターも使用しています。



Global Distributed Meetings（GDM）

Webex

GDMとは、異なるデータセンターで稼働している複数のサーバーに会議を分散させることができる機能です。

この機能により、GDM対応の会議に参加すると、参加者は自動的に最適な場所に接続されるようになるため、最も質の高いパーフォーマンスでWebexをご利用いただくことができます。

※GDMはデフォルトで有効化されています。

データセンターの物理的セキュリティ

Webex

データセンターの物理セキュリティには施設や建物のビデオ監視や入室の際の二要素認証などが含まれます。データセンターサーバーはインフラストラクチャの機密度に基づいて「信頼ゾーン」にセグメント化されます。

例えば、データベースは「厳重に保護」されていて、ネットワークインフラストラクチャには専用の部屋があり、全ての装置ラックはロックされています。シスコのセキュリティ担当者、およびシスコの担当者が承認済みの訪問者だけがデータセンターに入ることができます。

物理
セキュリティ

サーバー管理

情報セキュリティとコンプライアンスの第三者認証

International & Local

Information Security + Privacy

- ISO 2700X i.e ISO 27001 / 27017 / 27018 / 27701
- SOC 2 Type II and SOC 3
- Cloud Computing Compliance Controls Catalog (C5)
- FedRAMP
- Cisco's Quality Management System
- ISO 9001
- CSA STAR L2

Regulatory

- HIPAA
- GDPR
- FERPA
- COPPA
- PIPEDA
- PHIPA
- CCPA
- PCI
- Continually assessing regs
- FISC

Cross-Border Transfers

- Binding Corporate Rules
- APEC cross-border privacy rules
- EU Standard Contractual Clauses

GDPR（EU一般データ保護規制）の遵守

Webex

シスコは個人データの取得先や扱い方にかかわらず、個人データを尊重し保護することによりお客様やパートナーの支援に努めています。また、義務付けられたプライバシーに関する法律を世界中で遵守しています。

シスコは、セキュリティ、データ保護、プライバシーに関するプログラムを長期にわたり確立しており、既存のプログラムにはGDPR の要件も含まれています。こうしたプログラムは、数々の規制、お客様のニーズ、シスコの社内行動規範に従うことへのコミットメントなど、GDPR と重なる要件をすでに多く備えています。

詳細はこちら

FISC安全対策基準第９版への準拠

Webex

Webexは、金融情報システムセンター（FISC）の安全対策基準第９版の第三者評価を行い、評価の必要がある全項目に対して適合判断を取得しています。

FISCにより金融機関等の自主基準として策定された金融機関等コンピュータシステムの安全対策基準・解説書（FISC安全対策基準・解説書）は、システムアーキテクチャおよび運用に関する指針として多くの金融機関によって活用されています。

FISCへの準拠は、セキュリティの３大原則が守られるセキュアなサービスであるかどうかの判断基準となります。

セキュリティ３大原則

Webex security and compliance overview

- セキュリティの仕組み
- セキュリティに対する取り組み
- ベストプラクティス

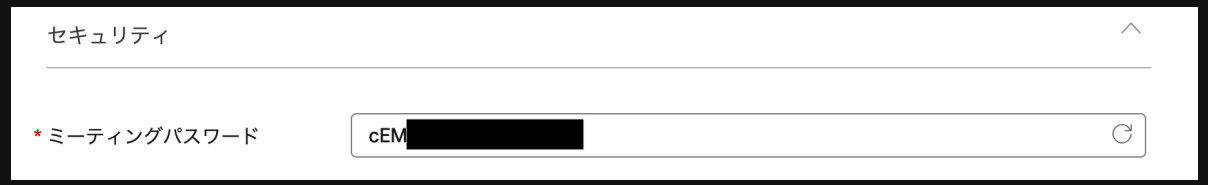
このパートでは、Webexの会議をより安全に
ご利用いただくためのベストプラクティスをご紹介します

セキュリティベストプラクティス –主催者編–

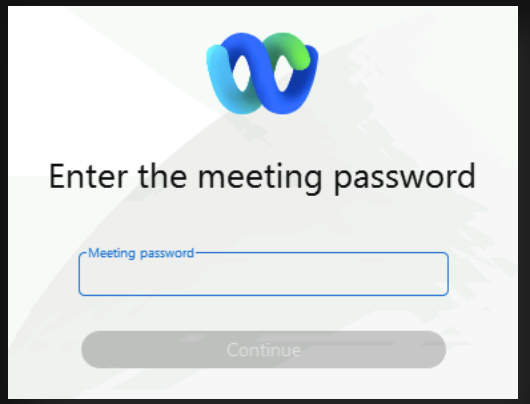
- WebexのIDを持っている方はサイト(xxx.webex.com）内で、セキュリティを高めるための様々な管理ができます

パスワードで保護された会議

主催者編

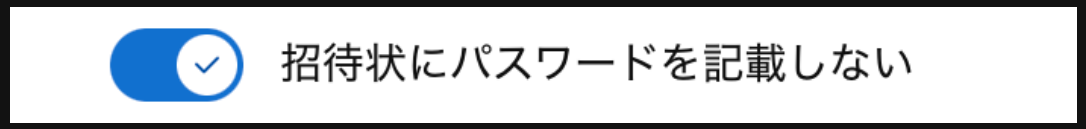


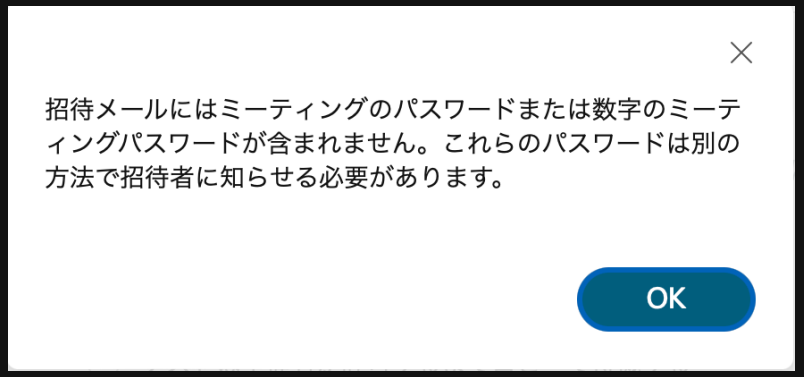
- 全ての会議にパスワードの自動適用が可能
- パスワードによる不正参加防止
- パスワードの強制は、参加者の参加体験に影響を与えません
- ビデオデバイスで参加するユーザーにもパスワードの強制が有効な場合があります



招待状にパスワードを記載させない方法

主催者編

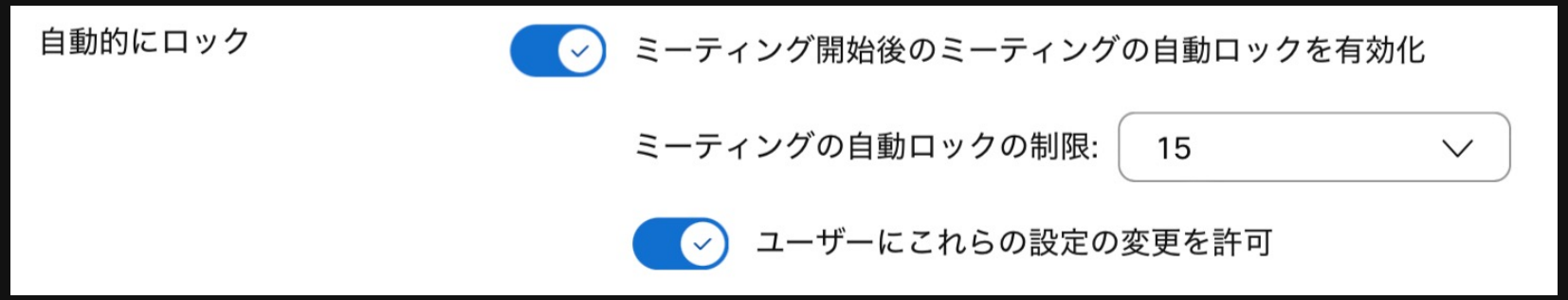




- この設定を有効にするとパスワードを設定していても招待状には記載されません
- パスワードが分からない場合は主催者に個別に聞く必要があるため、より強固なセキュリティ対策になります
- 招待状が正しい参加者に届いたことを確認するのに有効です

会議の自動ロック

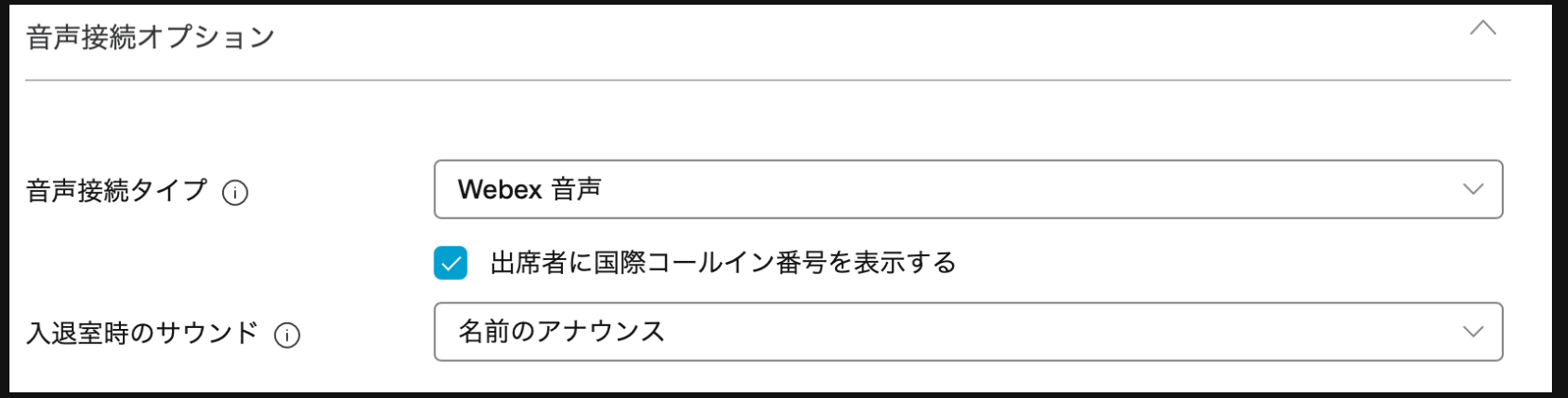
主催者編



- 会議開始後、自動的に会議をロック
- 会議開始後、0分、5分、10分、15分、20分の選択があります
- この設定はスケジュール会議と個人会議室（PMR）に別々に適用されます

入退室音/名前のアナウンス機能

- 誰も気づかないところで会議音声に参加されるのを防止する
- トーン無し
- ビープ音と名前のアナウンス



会議のマニュアルロック

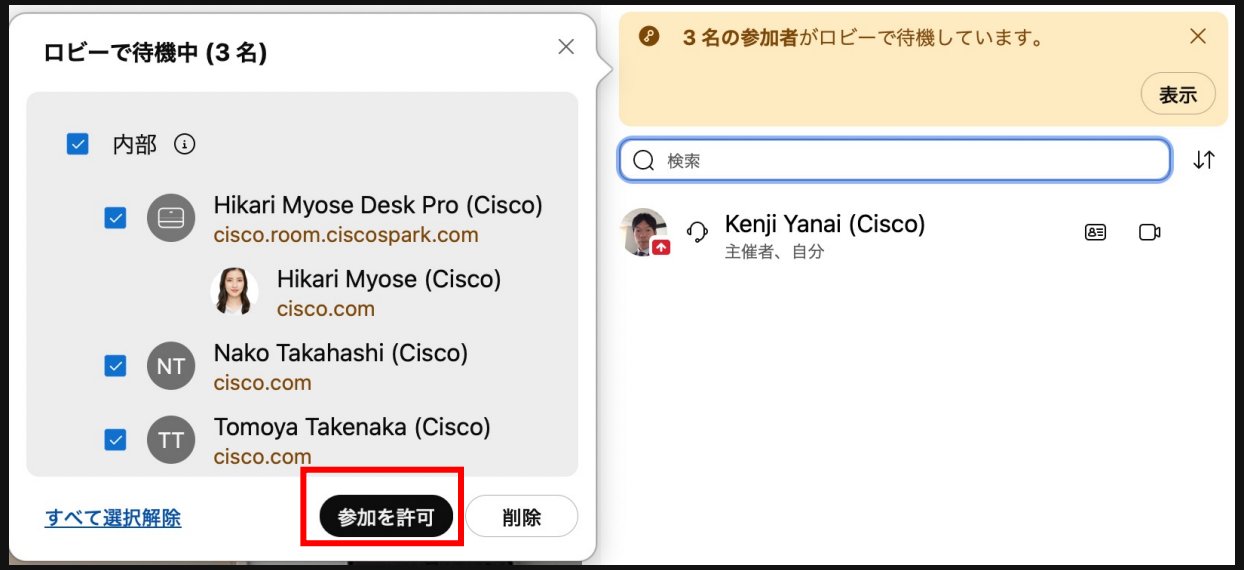
主催者編

- 会議の途中でもマニュアルでロック/ロック解除ができます

会議室ロビー

主催者編

- 会議室をロックすることで参加者は入室前にロビーで待たされます
- 主催者側で参加者を確認してから入室を許可することが可能です
- これにより悪意を持った第三者の不正参加を防ぐことができます



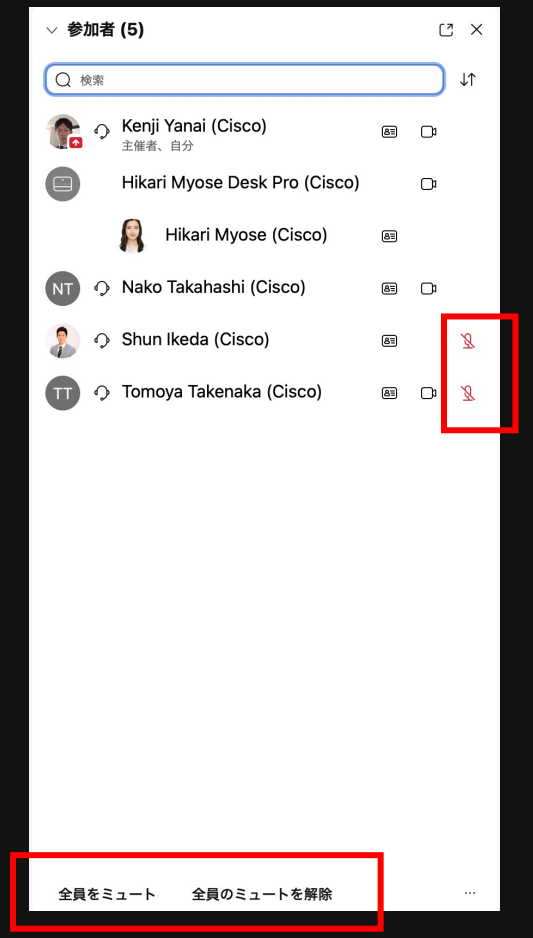
主催者画面

参加者画面

ミュート機能

主催者編

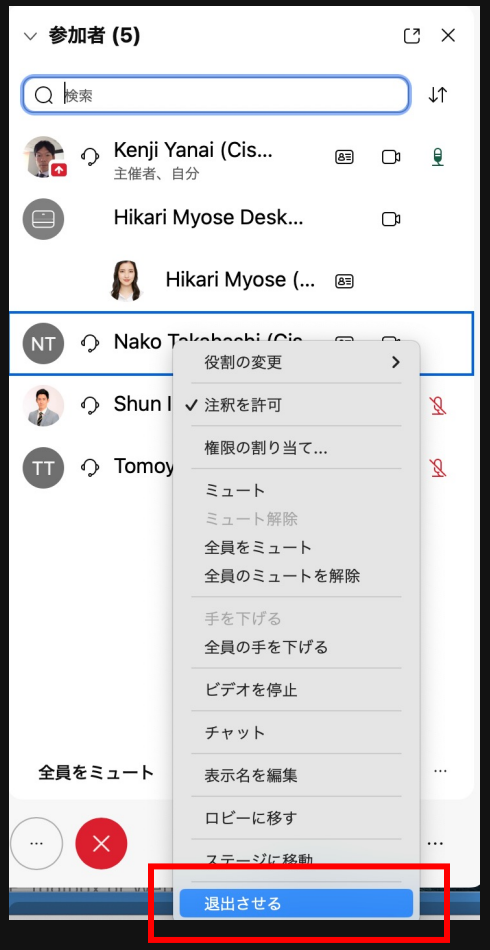
- 参加者の音声を主催者側でミュートすることができます（一括/個別）



強制退室機能

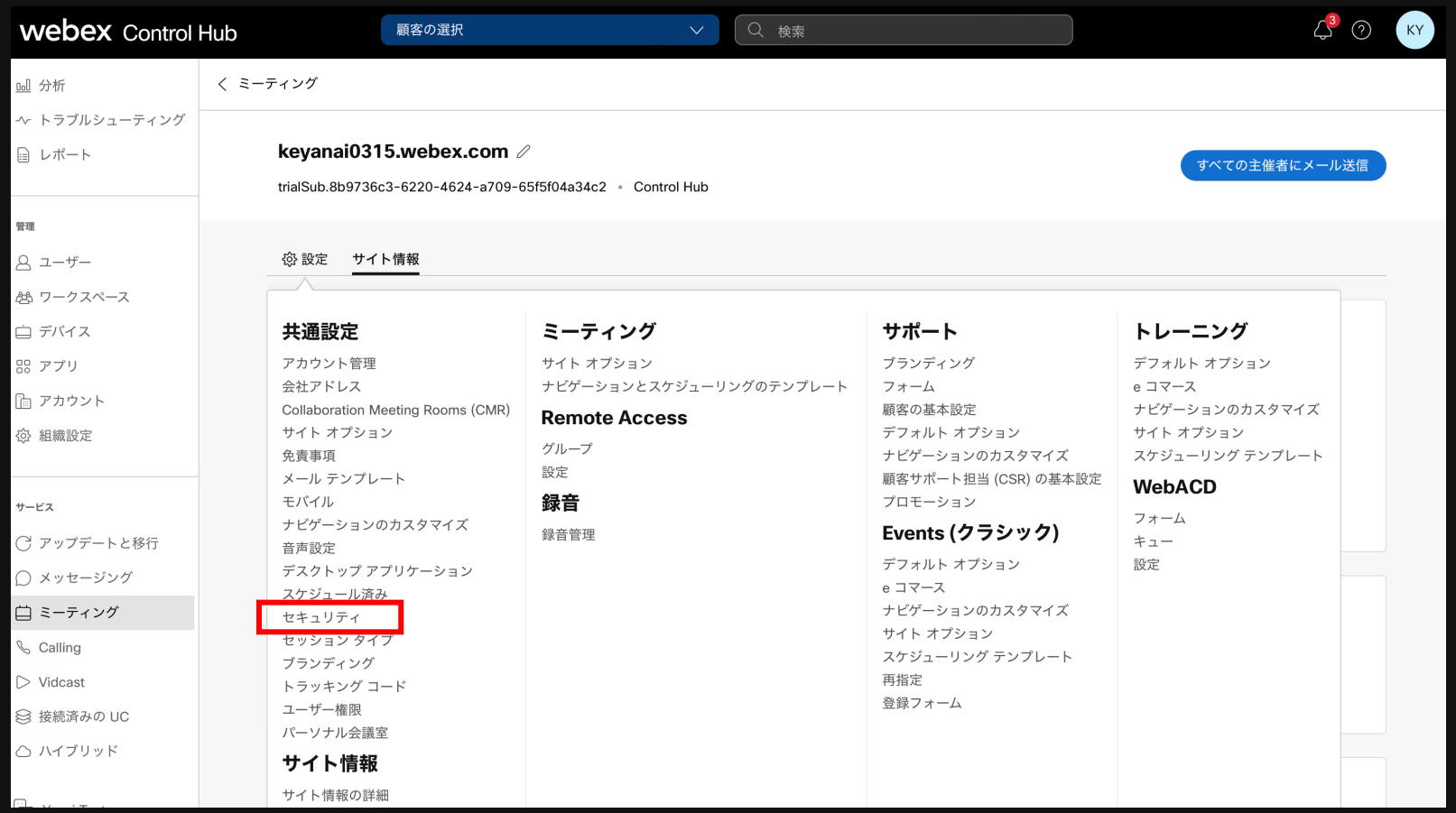
主催者編

- 素性の分からない人や、確認の取れてない参加者を主催者の判断で強制退室させることができます



セキュリティベストプラクティス –管理者編–

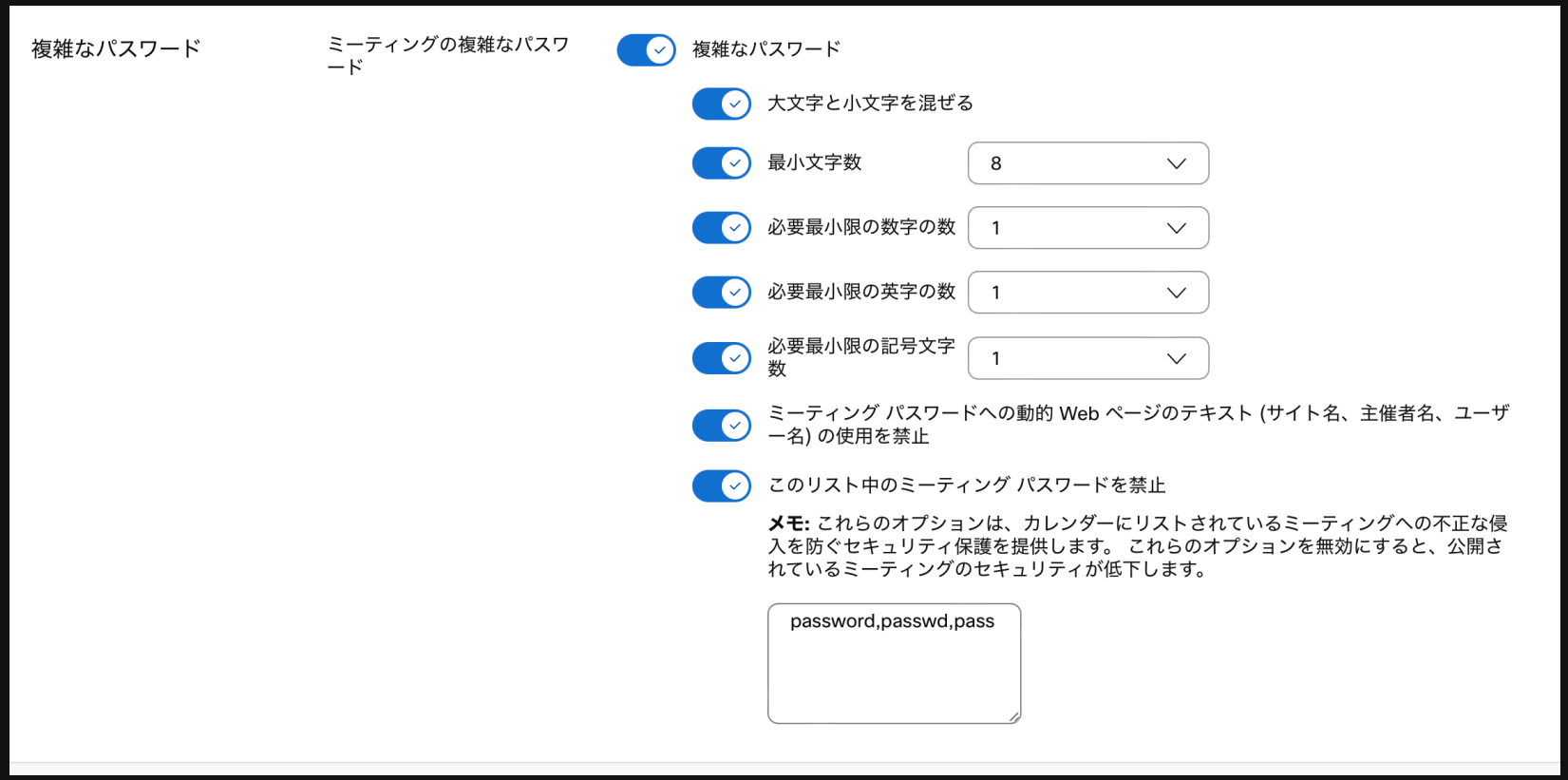
- 管理者の方はControl Hubにログインし「セキュリティ」タブ内でセキュリティの様々な管理ができます



複雑なパスワードの設定

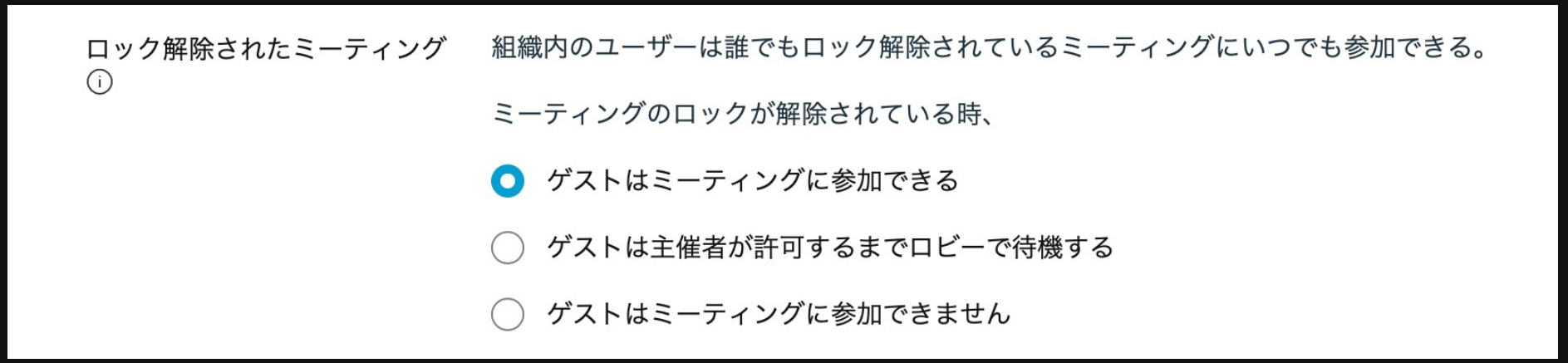
管理者編

- 最小文字数や大文字/小文字の混在など、パスワードの複雑性を管理できます



ロック解除された会議

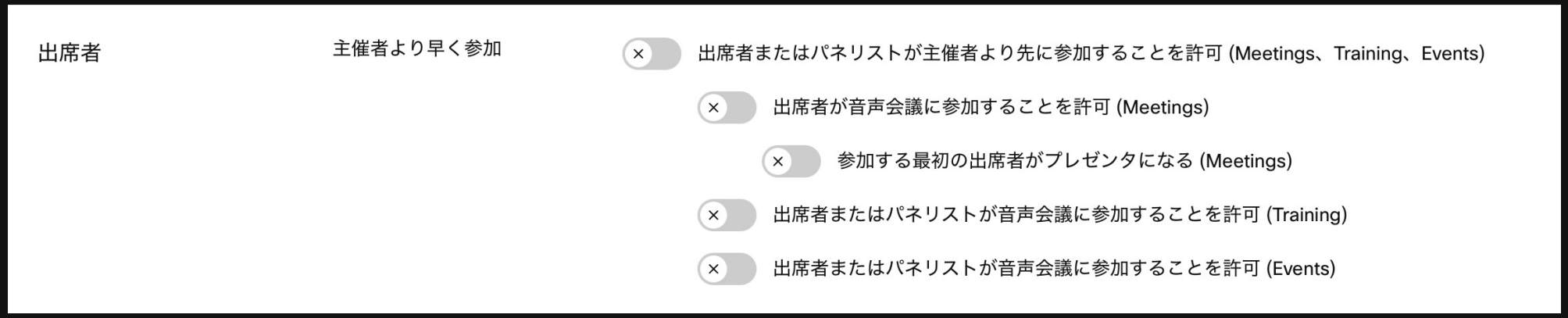
管理者編



- ロック解除時に会議に参加したゲストの扱いを選択できます
- 組織のユーザーのみに限定することができます

主催者より早く会議に参加

管理者編



- この設定を有効化すると参加者は主催者が会議を開始する前に参加することができます（音声接続も可能）
  ※シスコでは、この設定は無効にしておくことを推奨しています

セッションタイプ

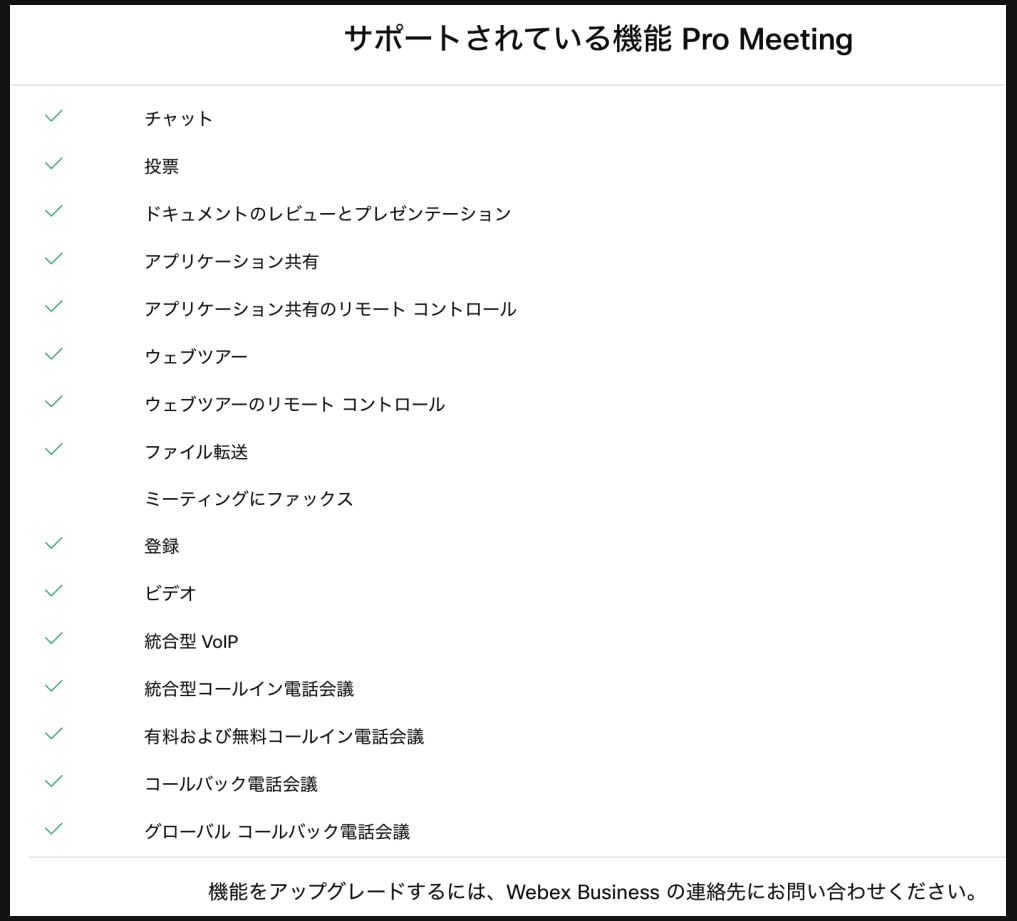
ミーティング> 設定 > セッションタイプ

- デフォルトセッションタイプ

- Standard Meeting (STD)
- Pro Meeting (PRO)
- Online Event (ONS)
- Training Session (TRS)
- End to End Encrypted Meetings (E2E) *(by request)

- サイト管理者のユーザー設定により、管理者はこれらのミーティングセッションタイプを個々のユーザーが利用できるようにすることができます。

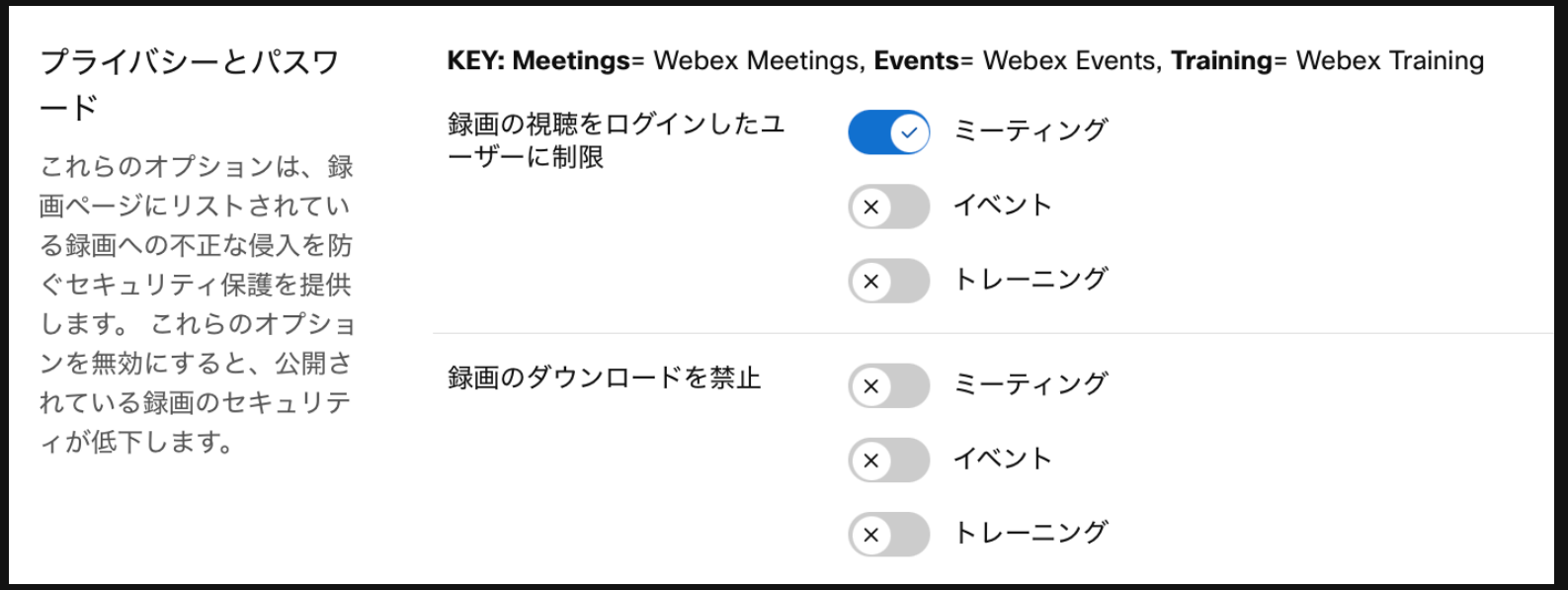
- ユーザーは、個人用 Webex ページで会議をスケジュールするときに、使用する会議タイプを選択できます。



録画コンテンツの保護

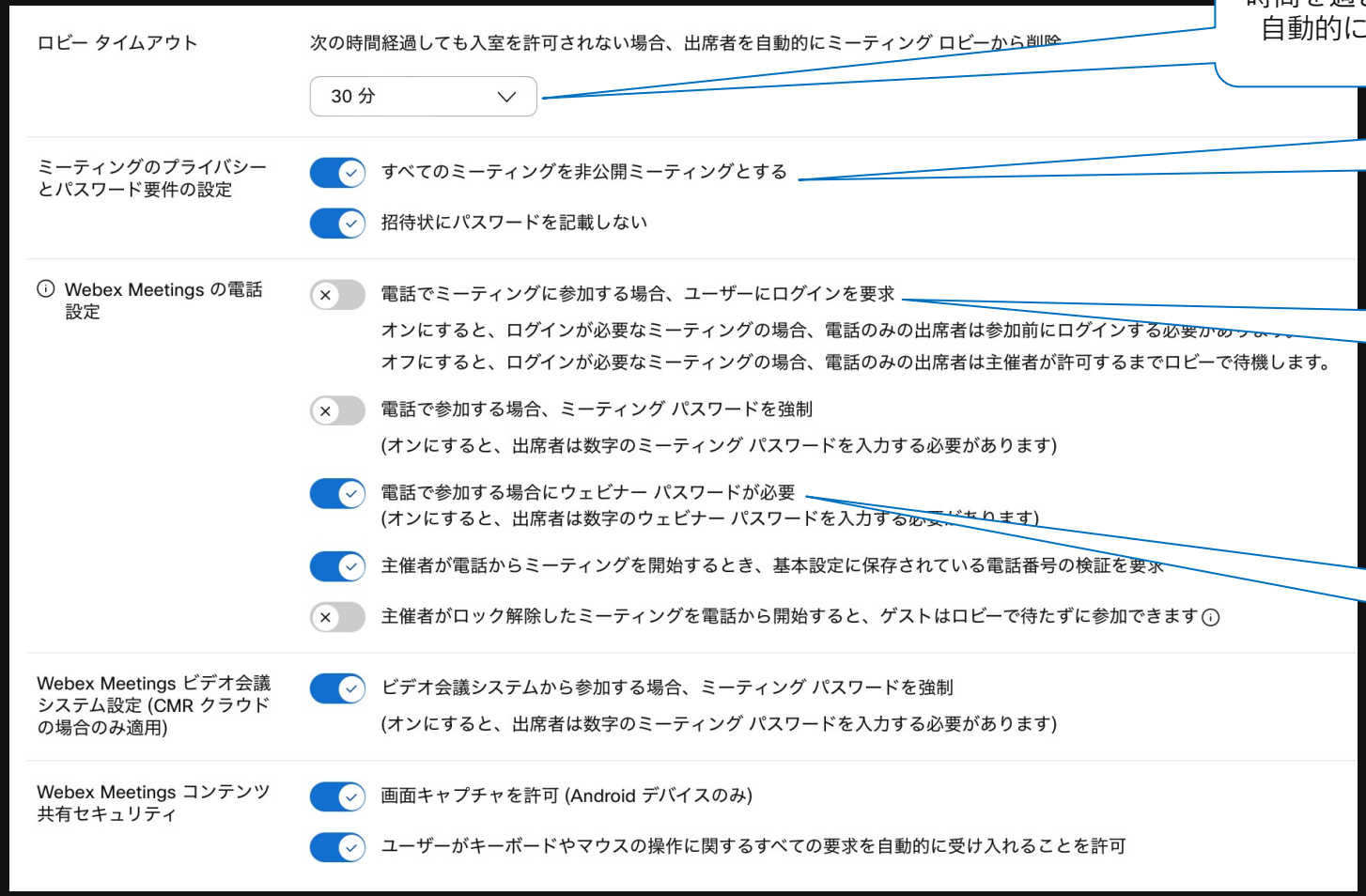
管理者編

- 主催者によって録画された会議コンテンツへの不正アクセス防止



その他のセキュリティ設定

管理者編



時間を過ぎて会議に入れないユーザーを自動的に退出させることが可能な設定

未確認のユーザーやゲストが参加する会議がリストアップされます

会議が事前登録者だけのものである場合に使用されることがあります

電話機に会議用パスワードを数字で入力させる設定

Webex音声

管理者編

- Webex音声に関連したセキュリティインシデントの防止

ベストプラクティスのまとめ -主催者-

- 一般に公開されているWebサイトのパスワードを公開しない
- 音声PINは誰にも共有しない
- 会議のパスワードは、それを必要とするユーザーにのみ提供する
- 出席者が確定するまで、機密情報を会議で共有しない
- 会議の自動ロックを積極活用する
- 会議のトピックは慎重に選択する
- なるべく招待状から会議のパスワードを削除する
- ロックされていない会議にゲストが参加できないようにする
- 入退室音や名前のアナウンス機能を使用するEnd the meeting

ベストプラクティスのまとめ -管理者-

- 特定の国のコールイン/コールバックを無効にしておく
- 会議は非公開にしておく
- 電話やビデオ会議システムから参加する際に、会議のパスワードを強制的に設定する
- 主催者が会議を開始するより前に参加することを許可しない
- 既定時間後に会議を自動ロックする
- 会議中、参加者から会議リンクを隠す
- 未認証のユーザーの参加を制限する


webex
by CISCO