Cisco Webex セキュリティの強み

目次

シスコのセキュリティ技術は、Fortune 100 企業の過半数で導入されています。シスコの数十年にわたる豊富なセキュリティのノウハウを活かした Cisco Webex は、データを保護し、コンプライアンスを可視化し、会議の管理をサポートしてきました。部門内や部門間でのコラボレーションを強力に支え、データのセキュリティを維持するコラボレーション プラットフォーム、それが Webex なのです。

シスコのコラボレーション ソリューションは、通話、会議、メッセージング、ホワイトボード共有、ビデオデバイス、そしてシスコ ユニファイド コンタクト センターを 1 つのプラットフォームに統合します。すべての製品は、Cisco Secure Development Lifecycle（SDL）に従って構築されています。SDL には、プライバシーの影響評価、プロアクティブなペネトレーションテスト、および脅威モデリングが含まれます。Webex のセキュリティとプライバシーはシスコのセキュリティ・トラスト部門が監督し、セキュリティの脆弱性をお客様に開示します。

プライバシー、セキュリティ、透明性

シスコの 3 つのセキュリティの原則は次のとおりです。

- Webex は、お客様のデータの**プライバシー**を重点的に保護します
- Webex は、導入時から**安全**です
- Webex では**セキュリティ サイバー ガバナンス**が整備されており、セキュリティ上の問題が見つかった場合も**透明性**が維持されます

データプライバシーとセキュリティプロセス

表 1 は、Cisco Webex 製品に組み込まれているプライバシーとセキュリティ機能の概要です。

表 1. Webex のプライバシー・セキュリティ関連のポリシー、プロセス、機能、コミットメント

機能	Cisco Webex に含まれるコミットメント
厳格なプライバシーポリシー	• Webex がお客様の情報を第三者と共有、貸与、または販売することはありません。
セキュリティとプライバシーのガバナンス	• 独立したセキュリティおよびトラスト部門が存在します。利害の対立を回避するために、製品のエンジニアリング部門とは分離されています。 • 全社的なデータ保護とプライバシープログラムにより、お客様のデータのプライバシーを維持します。 • Cisco Trust Center • Cisco Secure Development Lifecycle（SDL）
セキュリティの問題や修正に関する透明性の高いレポート	• 24 時間 365 日体制のグローバルな Product Security Incident Response Team（PSIRT：プロダクト セキュリティ インシデント レスポンス チーム）により、セキュリティ脆弱性の通達と公示を管理します。 • Cisco Emergency Response（CSIRT を含む）により、脅威の包括的な調査と防止を可能にします。 • NDA で利用可能なペネトレーションテストの結果に関する証明書
お客様によるデータの格納場所の選択	• お客様は、Webex Meetings や Webex Teams™ のデータとユーザ ID を保管するリージョンを選択できます。 • 暗号化キーは、ホームリージョンで生成および管理されます。 • Meetings で生成/共有されたメディアの保存先を特定のリージョンに限定できます。

機能	Cisco Webex に含まれるコミットメント
中国市場のサポート	• Cisco Webex Meetings では、現地の独立したサードパーティパートナーを通じて、中国市場専用のサポートが提供されています。 • 中国市場の会議クラスタは分離されています。中国市場のクラスタから中国国外のクラスタとメディア、データ、または運用能力が共有されることはありません。中国市場のクラスタはグローバル会議機能には対応していないため、メディアが中国のサーバを通過するリスクはありません。 • 中国の Webex サービス用のすべての暗号化キーは中国で生成されます。
Cisco Trust Center とデータプライバシー プログラム https://trustportal.cisco.com/	• シスコは、お客様のプライバシーと透明性のニーズに応えるため、Trust Center をホストしています。 • Trust Center は、セキュリティ、トラスト、データ保護、およびプライバシーへのコミットメントを共有するプラットフォームです。 • Trust Center ホストは、Cisco Webex Meetings、Teams、および Messenger など、56 を超えるプライバシーデータシートとデータマップを保有しています。 • シスコの Trust Portal は、公開および社外秘のセキュリティアシュアランス文書をオンデマンド配信するプラットフォームです。お客様は、ホワイトペーパー、プライバシーデータシートなどをダウンロードできます。 • プライバシーデータシートは、シスコの法務とセキュリティのチームによってレビューされ、最新の状態に保たれます。 • シスコは独自のデータプライバシーオフィスを運用しています。データプライバシー責任者が 3 人勤務し、地域のプライバシー要件に変更がないか常に見張っています。米州、EMEAR（欧州、中東、アフリカ、ロシア）、および APAC（アジア太平洋地域）の要件にシスコ製品を適合させるための重要な任務です。
Cisco Secure Development Lifecycle（SDL）	• 製品のセキュリティベースライン：200 を超える特定のセキュリティ要件 • 脅威モデリング：四半期ごとに 1,000 以上の機能のリスクを特定、評価、および軽減 • すべての新機能のプライバシーとデータの影響評価 • 製品とエンジニアリングに関する必須のセキュリティトレーニング：35,000 人を超える従業員が認定済み • 従業員の行動規範 • データプライバシー、データの分類、およびデータの処理に関する年 1 回の従業員トレーニング
サードパーティの Cisco Cloud Access Provider Review（CASPR）	• サードパーティのクラウドベンダーのセキュリティに対するデューデリジェンス、およびそのプライバシー慣行のアセスメント • マスターデータ保護契約書（MDPA）がシスコとシスコの関連会社の間で結ばれており、シスコによるお客様への製品やサービスの供給に関連するリスクを軽減します。 • ベンダーリスク評価
セキュアな DevOps	• 企業の実稼働環境に対する企業ネットワークと多要素認証アクセス • ロールベースで最小の権限アクセス • 四半期ごとのユーザアクセスレビュー • 定期的な脆弱性スキャン • 外部および内部のチームによる継続的なペネトレーションテスト：クラウドおよびハイブリッドのサービス • 継続的な生産資産インベントリ • 資産廃棄インベントリ • 論理的に分離された実稼働環境と非実稼働環境
セキュリティとプライバシーの認定	• ISO 27001 / 27017 / 27018 • SOC 2 Type II と SOC 3 • クラウド コンピューティング コンプライアンス コントロール カタログ（C5） • HITRUST（Teams） • FedRAMP Moderate（Meetings、Teams、UCMC-G） • シスコの品質管理システム ISO 9001

機能	Cisco Webex に含まれるコミットメント
適合規格	• HIPAA • FERPA • COPPA • CIPA • EU GDPR • カナダの個人情報保護および電子文書法（PIPEDA） • 個人健康情報保護法（PHIPA）
国を跨ぐデータ転送	• 拘束力のある企業ルール • EU - 米国間のプライバシーシールド • スイス - 米国間のプライバシーシールド • APEC クロスボーダー プライバシー ルール • APEC プライバシー処理者認定 • EU 標準契約条項

お客様は、ミッションクリティカルなコラボレーション、会議、メッセージ、通話、およびデータを Cisco Webex に委託します。データの保護は、グローバルなプライバシー法規制の遵守に欠かせません。競合他社への漏洩、機密情報の公開、信頼の喪失、復旧コスト、罰金、不要な圧力、および悪評のリスクが軽減されます。

Cisco Webex は、お客様のデータを保護するための強化されたコラボレーション プラットフォームです。それを実現するために、Cisco Webex は、プライバシーとセキュリティを、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ています。Cisco Webex では、プライバシーとセキュリティの要件を確実に満たせるように、複数のテクノロジー、手順、およびチームを採用しています。

- シスコは、反復可能で測定可能なプロセスである、成熟度の高い Secure Development Lifecycle を実施しています。これには、セキュリティ要件、脅威モデリング、セキュアな設計とコーディング、静的分析、脆弱性テスト、プライバシー影響評価、およびサードパーティのセキュリティアセスメントなどが含まれています。
- Cisco Webex は、導入環境の脆弱性を継続的に評価して修復するためのセキュリティ アセスメント プログラムを用意しています。
- Cisco Webex は、「need to know」の原則、職務の分離、ロールベースのアクセス、および多要素認証に基づいて、管理とサポートのためのシステムへのアクセスを管理します。
- Cisco Webex は、ネットワークとシステムを監視して、停止、サービス遅延、セキュリティインシデント、その他の異常および不正なアクティビティとイベントを検出します。アラームに対処するために、担当者が常に待機しています。
- Cisco Product Security Incident Response Team は、製品のセキュリティインシデント対策を担当しています。Cisco Computer Security (and Data) Incident Response Team は、プロアクティブな脅威分析、インシデント検出、および内部調整されたセキュリティインシデント対応を提供します。
- 独立した外部および内部の監査とリスク評価が継続的に実施されます。Cisco Webex は、改善が必要だと判断された分野の解決に取り組んでいます。
- お客様に対するシスコの取り組みはオープンでクリアです。シスコは、組織をリスクにさらす可能性がある技術的な問題などについて、お客様と明確な意思疎通を図ります。ペネトレーションテストの結果は、機密保持契約（NDA）の下でお客様に提供されます。

- シスコは、お客様の個人識別情報（PII）を保護するために、プライバシーバイデザインに基づくプライバシープログラムを保持しています。このプログラムには、プライバシー影響評価（PIA）、インシデント対応、お客様への通知、およびサブジェクト要求の管理が含まれます。
- すべてのスタッフに、オンボーディング時および年に 1 回、プライバシーとセキュリティに対する意識を向上させるための教育とトレーニングのプログラムが義務付けられています。

シスコのコラボレーションの最高セキュリティ責任者とセキュリティチームは、シスコのセキュリティ・トラスト部門（S&TO）に属しています。S&TO は、Cisco Webex 部門から独立していて、プライバシーとセキュリティのポリシーを強化します。セキュリティチームは、プロセスのコンプライアンスの確保、アセスメントの実行、およびエンジニアリングチームとオペレーションズチームへのガイダンスの提供を行います。

参考資料

- Trust Center
- Trustworthy ソリューション
- CSDL
- Data Protection Program
- シスコのプライバシー

ユーザとアイデンティティの保護

表 2 に、ユーザとアイデンティティを保護するために、Webex 製品ポートフォリオ内で利用可能な機能の概要を示します。

表 2. ユーザとアイデンティティの保護

機能	Cisco Webex
Webex Control Hub のエンタープライズグレードの自動化されたユーザプロビジョニングとライフサイクル管理	• Active Directory の同期：一方向の同期により、ユーザが入社時にプロビジョニングされます（総所有コストの削減）。さらに重要な点として、退職時にプロビジョニング解除され、トークンが取り消されます。 • アイデンティティの証明：管理者が社内のドメインを確認して、プロビジョニングしているユーザが本人であることを確認します。これにより、コラボレーションで参加者の相手を信頼できます。 • System for Cross-Domain Identity Management（SCIM）のプロビジョニング：業界標準である SCIM を使用して、Okta と Azure AD の統合を通じてユーザをオンボードします。シスコは、業界での関係を活かして、サポートする製品のリストに、主要なアイデンティティ プロバイダーを継続的に追加しています。シスコは、独自プロトコルではなく標準規格を使用しているため、新しい IdP を迅速に追加できます。 • Developer.webex.com の People API と CSV もサポートされています。
多要素認証（MFA）	• Webex Identity Service は MFA 多要素認証を提供して、安全なリモートコラボレーションを実現します。オプションの 1 つとして、Webex の導入で Cisco Duo を使用することができます。これは、ご使用の IdP（PingIdentity、Forgerock、Microsoft、または Okta）とともに、2 番目の要素としてオプションで導入できます。
Oauth2.0 ベースの標準化された認可（ソフトウェア開発キットではない）	• すべての統合では、クライアント ID とクライアントシークレットを使用し、承認付与フローで、サードパーティの統合と共有される範囲をユーザに示します。
サービス全体のアイデンティティの難読化	• ユーザアイデンティティ情報は、プロビジョニング時にお客様が選択したデータ格納リージョンに保管されます。難読化された ID のみが、ユーザの電子メールアドレスではなくサービスによって使用されます。

機能	Cisco Webex
お客様が選択したアイデンティティプロバイダー（IdP）による SSO のサポート	• サポートされているオンプレミスの IdP：Ping Identity、ADFS、ForgeRock、Shibboleth、OracleAM、IBM Secure Access Manager、F5 BigIP • サポートされている IDaaSpartner：Microsoft Azure AD、Okta、PingOne、LastPass、Simplified、OneLogin、OnePassword
Webex Teams への個人アカウントログインの使用をブロック	データ損失の懸念を軽減するため、ユーザは社内ネットワークで自社の電子メール Webex のみを使用できます。
アクセスポイントでのリスクを阻止したり、ユーザ認証環境の変化に適応したりするリスクベースの認証	Cisco Webex は、主要な IdP プロバイダーと連携し、リスクベースの認証モジュールと統合するために、Cisco Duo、Okta、Microsoft AzureAD、ForgeRock、および Ping Identity を含む、ゼロトラスト ソリューションをサポートしています。Cisco Webex セキュリティと連携してこれらのソリューションを使用することで、お客様はアクセスを管理できます。IP アドレス、ロケーション、デバイスフィンガープリント、ログイン履歴、および機械学習と人工知能を使用した地理位置情報など、30 種類の値を使用して、状況に適した最適な認証チャレンジを提供します。

ユーザプロビジョニングとライフサイクル管理

ユーザライフサイクル管理：シスコの共通アイデンティティにより、ユーザ、グループ、ボット、およびデバイスに対するセキュアな ID 管理、ディレクトリサービス、および認証と認可が提供されます。これにより、お客様は、重要なビジネスや個人のアクティビティのためにコラボレーションしている人を信頼できるようになります。この信頼は、ユーザが作成、更新、および削除される前にユーザを証明することから始まり、ライフサイクル全体を通じて維持されます。

Active Directory の同期：この一方向の同期により、企業へのオンボーディングの際にユーザがプロビジョニングされるだけでなく（総所有コストの削減）、さらに重要なこととして、企業がプロビジョニング解除する必要があると判断した場合に、ユーザがプロビジョニング解除され、トークンが取り消されます。

アイデンティティの証明：管理者が自分のドメインを確認して、プロビジョニングしているユーザが本人であることを確認します。これにより、会議に参加するときに、コラボレーションしている相手を信頼できます。この証明メカニズムにより、管理者は確認するドメインに対する権限を確実に持つため、電子メールを受信したり、別の証明サービスを利用して本人であることを確認したりせずに、ユーザを作成できます。

SCIM のユーザプロビジョニング：お客様は、業界標準である SCIM を使用して、Okta と Azure AD の統合を通じてユーザをオンボードできます。シスコは、業界での関係を活かして、サポートする製品のリストに、主要なアイデンティティ プロバイダーを継続的に追加します。シスコは、独自プロトコルではなく標準規格を使用しているため、新しい IdP を迅速に追加できます。

追加のユーザプロビジョニング：Webex Control Hub プラットフォームにより、パートナー、開発者、およびお客様は、API と CSV のサポートを通じてユーザをプロビジョニングできます。

認証と認可：シスコは、標準ベースのメソッドを使用して、ユーザが小規模企業であるか、最高レベルのセキュリティを必要とする連邦政府機関であるかを問わず、ユーザに対して認証と認可のセキュアなメソッドを提供します。ユーザ名とパスワードを使用している組織では、米国国立標準技術研究所（NIST）のガイドラインに準拠した、一定レベル以上の複雑性でパスワードを保護します。お客様は、パスワードのエントロピーを強化する必要がある場合、要素（必要な文字数、特殊文字、大文字、および数字など）を変更することで、パスワードの複雑さを変えることができます。

セキュリティ アサーション マークアップ言語（SAML）2.0 シングルサインオン：シスコは、SAML 2.0 を使用して、市場における主要なアイデンティティ プロバイダーに対する認証を連携します。これには次のようなものがあります。

- サポートされているオンプレミスの IdP（Ping Identity、ADFS、ForgeRock、Shibboleth、OracleAM、IBM Secure Access Manager、F5 BigIP など）
- サポートされている IDaaSpartner（Microsoft Azure AD、Okta、PingOne、LastPass、Simplified、OneLogin、OnePassword など）

これにより、企業は Webex からユーザを IdPand にリダイレクトすることができます。また、ユーザは、パスワードと認証フローを、雇用者が提供するさまざまなアプリケーションに使用できます。また、フローの一部として認証に 2 番目の要素を使用することもできます。

多要素認証：現在、ほとんどの人々は、異なるインターネットサイトで 5 つ未満のパスワードを使い回しているため、攻撃者は、そのパスワードが使い回されているサイトを見つけるまで、感染したサイトから他のアカウントでパスワードのリプレイ攻撃ができてしまいます。Cisco Duo は、市場における主要な多要素ソリューションです。Webex Control Hub をライフサイクル管理の主要なアイデンティティ プロバイダーと組み合わせることで、Duo はゼロトラスト コラボレーション環境を提供します。Cisco Duo は通常の MFA 以上のものを提供します。リスクの高いデバイスを特定して、コンテキストに応じたアクセスポリシーを適用し、デバイスの正常性をレポートします。エージェントレスアプローチの使用にも、デバイス管理ツールとの統合にも対応します。

リスクベースの認証：Cisco Webex は、主要な IdP プロバイダーと連携し、ベンダーのリスクベースの認証モジュールと統合するために、Cisco Duo、Okta、Microsoft AzureAD、ForgeRock、および Ping Identity を含むゼロトラスト ソリューションをサポートしています。Cisco Webex セキュリティと連携してこれらのソリューションを使用することで、お客様はアクセスを管理できます。IP アドレス、ロケーション、デバイスフィンガープリント、ログイン履歴、および機械学習と人工知能を使用した地理位置情報など、30 種類の値を使用して、状況に適した最適な認証チャレンジを提供します。SCIM ベースのプロビジョニングと組み合わせることで、これらのリスクベースのエンジンはユーザを無効にすることもできるため、すぐにアクセスできなくなります。

Webex への個人アカウントログインの使用をブロック：すべてのユーザが企業アカウントのみを使用して Webex にアクセスできるようにします。シスコは、Cisco Web セキュリティアプライアンス（WSA）などの主要なネットワークプロキシと連携して、Webex への認証が許可されているドメインを指定するルールを追加しました。たとえば、acme.com が acme.com からのユーザの認証のみを求めている場合、企業はルールで acme.com を指定し、Webex は認証ヘッダーを調べて、acme.com ドメインを持たないすべてのユーザからの認証を拒否します。このオプションを設定する方法については、シスコのサポートサイトを参照してください。

アプリケーションとデバイスの保護

表 3 に、アプリケーションとデバイスを保護するための Webex 機能の概要を示します。

表 3. アプリケーションとデバイスの保護

機能	Cisco Webex
MAM アプリのラッピングプロセス	Webex Meetings と Webex Teams でサポート
MDM の検証	Webex Meetings と Webex Teams でサポート
Appconfig のサポート	Webex Meetings でサポート

機能	Cisco Webex
顔認証と指紋認証によるモバイルログイン	Webex Meetings でサポート
リモートワイプ：Webex のネイティブセキュリティ管理	Webex Teams でサポート
PIN ロックの要件：Webex のネイティブセキュリティ管理	Webex Teams でサポート
デバイスタイプ別のファイル共有管理：ネイティブセキュリティ管理	Webex Teams でサポート
クライアントのローカルキャッシュの完全な暗号化	Webex Teams デスクトップとモバイルクライアントでサポート
Web アプリと Control Hub のカスタム アイドル タイムアウト	Webex Teams のブラウザベースのクライアントと Control Hub でサポート

MAM アプリのラッピング

BYOD 環境をサポートするお客様は、通常、エンタープライズ アプリケーションのコンテナ化が必要です。お客様が選択した MAM プロバイダーから Cisco Webex モバイルアプリへのアプリのラッピングを実行できるオプションを使用すると、企業のコンプライアンス要件を満たす方法で、ユーザをより安全に Webex Teams にオンボードできます。

MDM の検証

すべての Cisco Webex モバイルアプリは、マルチデバイス管理（MDM）プロバイダーで検証されていて、アプリケーションに適用できるコントロール（コピー/貼り付けの防止、またはリモートでのアプリケーションの削除など）が可能です。

AppConfig のサポート

IT 管理者は、MDM AppConfig サービスを使用して、管理されたモバイルデバイスで Webex Meetings アプリを設定することで、サインインメソッド、会議ソース、ビデオアクセスなどのアプリ機能へのユーザアクセスを制御できます。

Webex Teams のネイティブセキュリティ管理

Cisco Webex Teams アプリは、ネイティブに構築された多くのコントロールを通じて管理および制御できます。これは、BYOD の環境があり、MAM を使用しないお客様が利用できます。いくつかの例を以下に示します。

- **リモートワイプとリセット**：デバイスを紛失したり、ユーザが会社を辞めたりした場合、管理者はデバイス上の Cisco Webex Teams のコンテンツをリモートで消去できるため、企業の知的財産を保護できます。
- **PIN ロックの要求**：BYOD 環境を使用するお客様は、ユーザが Cisco Webex Teams モバイルアプリを使用するためには、個人的に管理されたデバイスで必ず PIN ロックを設定するように求めることができます。
- **ファイル共有管理**：ロックダウンされた環境を使用するお客様は、ユーザが優先クライアントタイプ（モバイルではなくデスクトップなど）からのみ、ファイルのアップロードとダウンロードを実行できるようにすることが可能です。

- **メッセージプレビューの無効化** ：お客様は、モバイル通知のメッセージプレビューを常に無効にして、近くのユーザが交換されるメッセージをのぞき込むことができないようにします。または、デバイスがロックされて誤って置き忘れられた場合、他のユーザは、デバイスのロックされた画面を見て、送信されたメッセージのプレビューを見続けることはありません。
- **暗号化されたローカルキャッシュ**：業界初の標準として、メッセージングワークロードをサポートする Cisco Webex Teams は、コンテンツをローカルデータベースに保存し、常に完全に暗号化します。
- **ブラウザインターフェイス用のカスタム アイドル タイムアウト**：Control Hub を使用する Cisco Webex 管理者、またはブラウザベースの Teams インターフェイスを使用するユーザは、ラップトップが無人のままであることを心配する必要はありません。Control Hub でカスタムタイムアウトを設定する機能により、管理者は一定期間のタイムアウト（10 分 ~ 60 分）の後でアイドルセッションを終了することで、このようなイベントのセキュリティリスクを軽減できます。また、Control Hub には、20 分のデフォルトのアイドルタイムアウトが設定されています。これらのタイムアウトは、ネットワーク内外でさらにカスタマイズできます。ユーザが VPN のセキュリティでシステムにログインしている場合、企業ネットワークのアイドルタイムアウト期間は長くなる（またはオンにならない）可能性があります。パブリックネットワーク上では、期間を短くすることができます。

デフォルトのコンテンツの保護

表 4 に、デフォルトでコンテンツを保護するための Webex 機能の概要を示します。

表 4. コンテンツの保護

機能	Cisco Webex
Webex Meetings のエンドツーエンドの暗号化	• このオプションのコントロールにより、会議の主催者は Webex Meetings アプリを使用するときに暗号化を許可できます。 • 高拡張性 • 会議暗号化キーは、会議の主催者によって生成され、会議の参加者に安全に配布されます。Webex Cloud には、会議暗号化キーへのアクセス権がありません。
Webex Teams のエンドツーエンドの暗号化	• Webex Teams スペースで共有されるユーザが生成したコンテンツ（メッセージとファイル）は、いくつかの例外を除き、TLS 経由で Webex Teams クラウドに送信される前に、Webex Teams アプリによってエンドツーエンドで暗号化されます。このユーザが生成したコンテンツは、Webex クラウドに暗号化された形式で保存されます。 • エンドツーエンドの暗号化キーは、Webex Teams キー管理サービス（KMS）を使用して、Webex Teams スペースごとに作成されます。 • お客様は、Webex Teams のクラウドベースの KMS を使用するか、または（Hybrid Data Security [HDS] サービスの一部として）オンプレミスで KMS を導入するかを選択できます。これにより、顧客はキーを保持できます。
社内での録音の議事録	• すべての録音と議事録は AES256 で暗号化され、Webex クラウドに保管されます。 • 録音は、HSM 派生キーで暗号化されます。 • HSM は、シスコの個別のセキュリティチームによってホストおよび運用されます。Webex Meetings チームは、キーにアクセスできません。 • 顧客データは、文字変換サービストレーニングには使用されません。
コンテンツ共有の保護	• 記録の閲覧をサインインしたユーザのみに制限します。 • 記録のダウンロードを不可にします。 • すべてのネットワークベースの記録にパスワードを適用します。 • 外部統合によりコンテンツ共有を有効/無効にします。 • アプリケーション共有を制限します（Meetings）。 • デスクトップ、アプリケーション、ホワイトボード、およびファイル共有を防止するための、きめ細かいコントロールが利用可能です（Meetings）。

セキュリティのための柔軟な管理者用コントロール

表 5 に、Webex 管理者向けのセキュリティコントロールの概要を示します。

表 5. 管理者のセキュリティコントロール機能

機能	Cisco Webex
無認可の出席者の会議への参加を防止	• 招待状を持つユーザのみに、一意のパスワードで保護されたリンクを使用します（デフォルト）。 • 会議室を自動的にロックして、入室を制限します（デフォルト）。 • 外部または未認証の参加者を待合室に自動的に移動します（デフォルト）。 • 電話機とビデオデバイスにパスワードまたはサインオンを適用します。
会議中の中断を防止	• 主催者より前に会議に参加できないようにします。 • 手動でルームをロックします。 • 共有の取得を防止します。 • 指定した期間の経過後に自動的にロックするようにルームを設定します。 • ロックされている個人ルームに参加する参加者を、主催者が承認するまでロビーに配置するようにします。
会議を内部ユーザのみに制限	• 参加またはパーソナル ミーティング ルーム エントリに SSO を適用します。 • 出席者の役割が必要です。
招待状の転送を防止	• 招待されたユーザのみが会議に参加できるようにします。
個人ルームの会議を安全に管理する権限を主催者に付与	• 名簿内の内部/外部ユーザの視覚的な違い • 入室と退室の色の違い • ルームをロックします。 • 不在中に個人ルームのロビーへの入室があった場合、電子メール通知が送信されるようにします。 • チャット、ビデオ、音声オプションなどの使用可能な機能を有効/無効にします。 • 退席、ロック、ミュートなど
ファイル共有制御の管理	• 管理者は、ファイル共有を有効または無効にすることを選択できます（Meetings と Teams）。 • 管理者は、クライアントタイプに基づいてファイル共有を制限できます（Webex Teams）。
外部統合の管理（Meetings と Teams）	Webex Meetings と Teams でサポート
ボットの管理	Webex Teams でサポート

外部統合の管理

お客様は、ユーザが、Google アカウント、Microsoft Office 365 アカウント、Facebook アカウント、およびその他のサードパーティ製アプリケーションを Cisco Webex アカウントと統合することを許可または拒否できます。さらに、セキュリティとデータ処理の標準規格を満たす Webex Teams（developer.webex.com から API を使用して開発された）のサードパーティ製アプリケーションのみを、ユーザに対して有効にできるようにすることも可能です。お客様は、組織内の全員または特定のユーザに対して、これらのサードパーティ製アプリケーションへのアクセスを許可または拒否することを選択できます。

ボットの管理

お客様は、外部統合管理などの Webex Teams スペースにボットを管理して、情報の流出を制御し、リスクを軽減することができます。管理者は、組織のボットを許可または拒否するためのグローバルポリシーを設定できます。「グローバル拒否」の場合は、個々のボットをホワイトリストに登録できるため、組織の従業員が通信するためにグループとダイレクトのスペースでそれらのボットを利用できるようにすることが可能です。

外部通信のブロック

外部通信のブロック機能により、管理者は次の方法で組織間のコラボレーションを制御できます。

- 組織内のすべてのユーザは、Webex Teams 内で外部組織のすべてのユーザとの通信を制限されています
- 組織内のユーザは、承認済みドメインの外部のユーザを追加したり、Webex Teams の未承認のドメインで作成されたスペースに参加したりできません
- 参加者のロールと [サイトアクセスの前にログインが必要（Require login before site access）] コントロール を使用して、Meetings サイトの外部にいる参加者をブロックします（図 1）

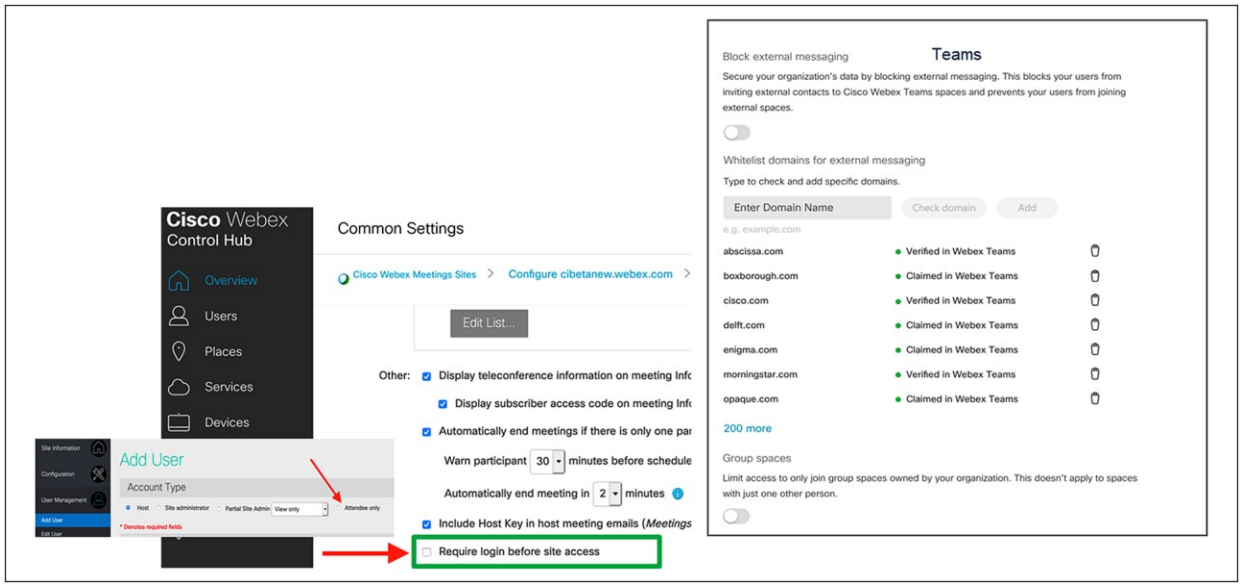

図 1.
外部通信機能のブロック

組み込み型のコンプライアンスツールにより、サードパーティ製ソリューションを不要にする

表 6 で、お客様がサードパーティ製ソリューションを不要にするために使用できるコンプライアンスツールについて説明します。

表 6. 利用可能なコンプライアンスツール

機能	Cisco Webex
柔軟な保持コントロール	次のような、柔軟でカスタマイズ可能な保持ポリシーを使用します。 • 7 日間から最大 12 ヵ月間、無制限のストレージで録画を保持（Webex Meetings） • 30 日間から無期限、メッセージとファイルを保持（Webex Teams）
法的保留	• ユーザが生成したコンテンツ（メッセージとファイル）に対する Webex Teams のネイティブサポート
eDiscovery	• ユーザが生成したコンテンツ（メッセージとファイル）に対する Webex Teams のネイティブサポート

Cisco Webex Control Hub の組み込み型のコンプライアンスツールは、組織がコンプライアンスを確保し、リスクとコストを削減し、サードパーティのコンプライアンス ソリューションを不要にするための単一のソリューションを提供します。規制対象の組織専用に設計された柔軟な保持ポリシー、法的保留、および eDiscovery 機能を使用して、すべての電子通信データをオンデマンドで収集、保存、確認、およびエクスポートできます。

柔軟な保持

組織は、Webex Control Hub でカスタム保持期間を設定することで、リスクを管理し、企業の保持ポリシーに適合させることができます。管理者は、Webex Teams 内の組織全体の保持ポリシー、または Webex Meetings のサイトレベルのデータ保持ポリシーを定義することで、すべての関連するコンテンツが、設定された保持タイムフレームに完全に削除されるようにすることができます。これにより、長期間にわたって機密情報にアクセスできるリスクが軽減され、電子メールやその他のアプリケーション間での保持ポリシーの調整にも役立ちます。

法的保留

法的調査をサポートするためのコンプライアンス要件を満たすために、Webex Control Hub の法的保留ツールを使用することで、組織は、エンドユーザ エクスペリエンスに影響を与えることなく、訴訟や調査に関連するユーザが生成したすべての形式のコンテンツを容易に保持できます。

コンプライアンス責任者は、法的事項を作成し、カストディアン（ユーザ）に法的保留、表示とダウンロードの問題、およびリリースの問題を示すことができます（図 2）。法的保留中のデータは、組織の保持期間に基づいて削除されることはありません。ケースがクローズされると、法的保留が解除され、その時点でデータが組織の保持期間に基づいて削除の対象になります。

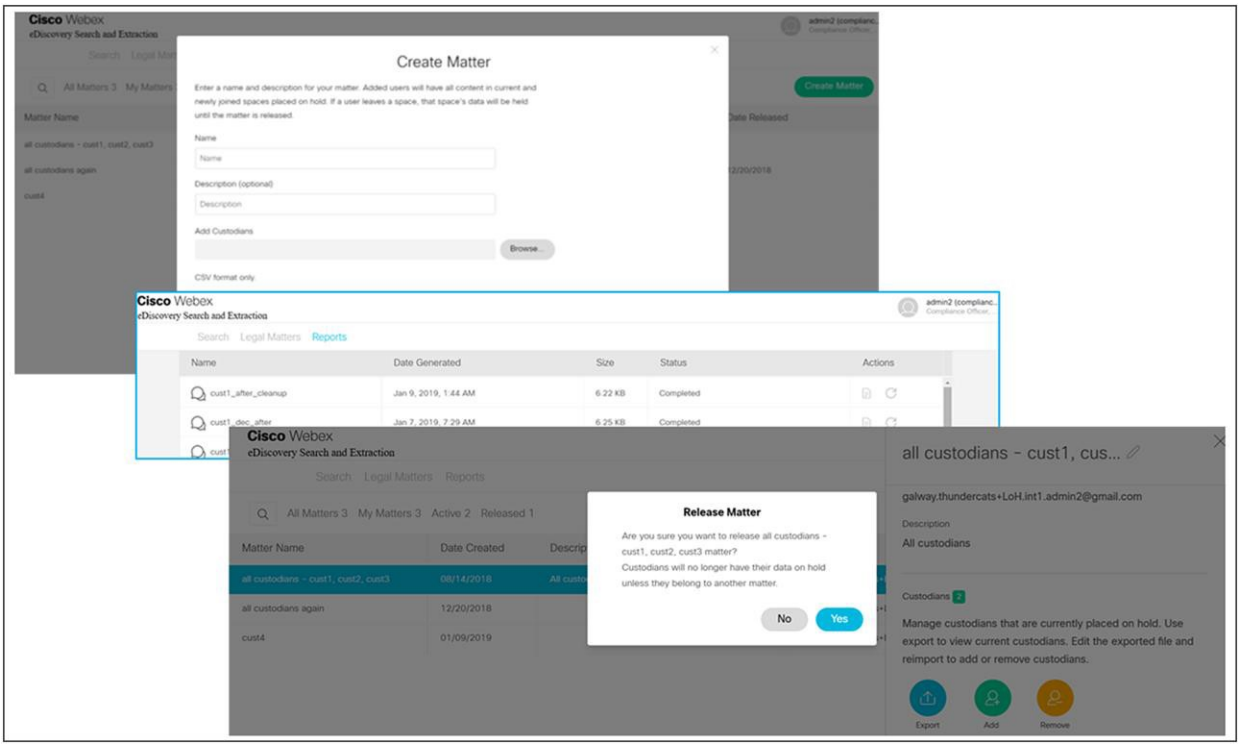

図 2.
案件の作成、表示、およびリリース

eDiscovery

Webex Control Hub の組み込み型の eDiscovery 検索ツールは、特定のカストディアン（ユーザ）によって生成されたコンテンツを、目的の時間範囲にわたって検索して抽出する機能を提供します。コンプライアンス責任者として、eDiscovery を使用して Webex Teams アプリ内のすべての会話を検索できます（図 3）。会社内の特定の人物を探して、その人たちが共有してきたコンテンツを探したり、特定のスペースを検索したりしてから、調査結果のレポートを生成できます。これにより、コンプライアンス責任者と法律顧問が、セルフサービス方式で法務、人事、および規制調査のデータを収集することができます。

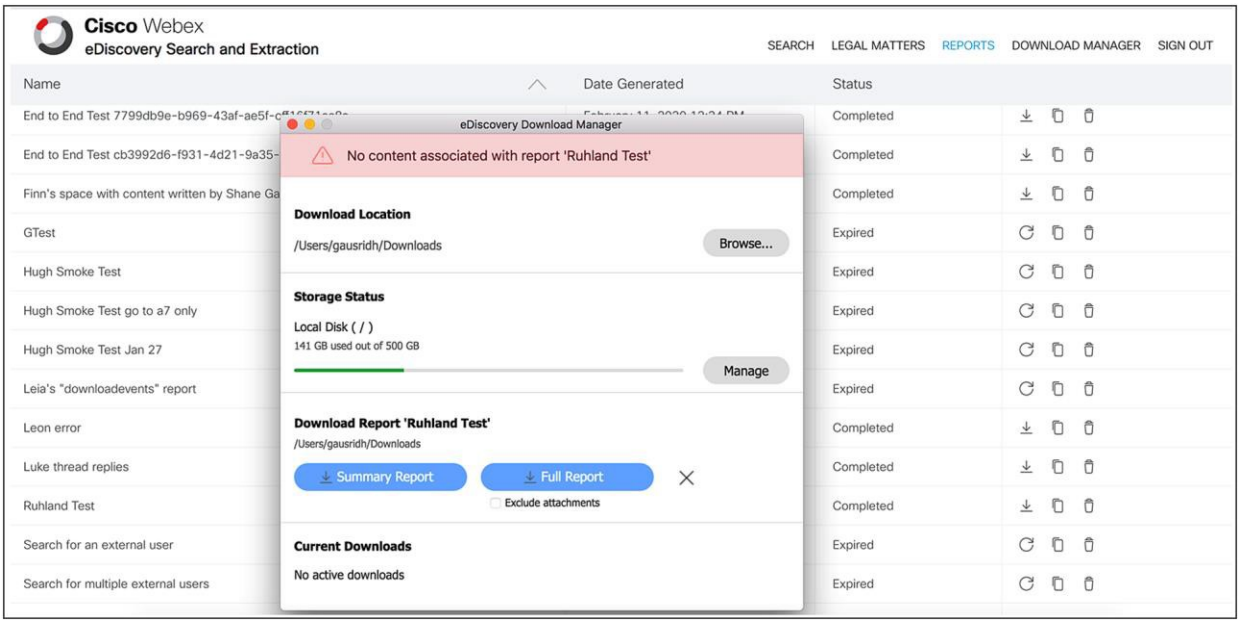

図 3.
Webex Teams 内のデータの検索

データ損失防止

表 7 で、Webex 製品に組み込まれているデータ損失防止機能の詳細を説明します。

表 7. 利用可能なデータ損失防止機能

機能	Cisco Webex
センシティブデータ漏洩の保護	• Webex Teams 用の Cisco Cloudlock® およびサードパーティと統合されたデータ損失防止 • Webex メッセージング専用に作成および調整された検出と修復ポリシー（スペースメンバーシップ、メッセージ、およびファイルベースの違反） • 導入時間を短縮するための、いくつかの規制対象業種（金融、医療など）向けの設定済みのポリシー
DLP とアーカイブ パートナー エコシステム	• 10 を超える業界トップクラスのアーカイブとデータの損失防止/クラウド アクセス セキュリティ ブローカ（CASB）ベンダーを備えた、メッセージングと会議用の広範なパートナーエコシステム • 事前構築およびテストされた統合により、製品化までの時間が短縮され、カスタム開発作業が減少されます • 大規模なパートナーエコシステムにより、お客様はパートナーベンダーからの既存のデータ損失防止製品を使用するオプションを選択できます
組織を跨いだポリシー	• すべての外部通信をブロックします • 特定のドメインとの外部通信を許可します

データ損失防止（DLP）

データ損失防止（DLP）ツールは、センシティブデータの損失または不正アクセスを防止し、コラボレーション アプリケーションの保護に不可欠な要素となります。ADLP エンジンは、ユーザによって生成されたコンテンツをスキャンし、ポリシー違反を特定して可視化します。DLP ポリシーエンジンは、金融（ルーティング番号、銀行口座番号）、医療（PII、医薬品名）、教育（学生ローン情報、FERPA）だけでなく、最も一般的なデータ侵害の発生につながるさらに多くの業種にわたって、事前定義された豊富なポリシーをサポートすることが必要不可欠です。

また、企業にはビジネスニーズとリスクポスチャに合わせたカスタムポリシーを作成する機能が必要です。違反が特定された場合、DLP エンジンは（エンドユーザと管理者に）アラートを送信したり、スペース内のメッセージングからユーザを削除したり、ユーザが生成した問題のあるコンテンツ（チャットメッセージ、ファイルなど）を削除したりするなどの修復アクションを適用する必要があります。これらの修復アクションにより、組織を危険にさらす可能性があるセンシティブデータを、ユーザが誤ってまたは故意に共有しないようにします。

通信境界線が組織の外部で拡大すると、データ損失のリスクと悪影響が大きく増加します。

クラウドアプリケーションとコラボレーション プラットフォームは、パブリック API またはその他の手段によって、ユーザが生成したデータや重要なイベントへのアクセスを DLP エンジンに提供する必要があります。DLP ベンダーの優れたエコシステムは、お客様に選択肢を提供し、既存の DLP/CASB ベンダーへの投資を引き続き活用できるようにするためにも重要です。DLP エンジンで使用される検出アルゴリズムは、コラボレーションの使用例、コンテンツタイプ、およびコンテキストに最適になるように調整する必要があります。コラボレーション プラットフォームは、多くの場合、ユーザが別の組織のスペース（またはテナント）でコンテンツを生成するときに、ほとんど可視性のないブラックボックスになります。このような場合、検出されない可能性があるデータ漏洩のリスクが高くなります。

Cisco Webex は、組織内のすべてのユーザによって生成されたデータを取得するために、パートナーが呼び出すことができるパブリック REST AP（イベント API と呼ばれます）を提供します。パブリックインターフェイスでは、任意のパートナーが Webex プラットフォームと統合して、目的のイベントを取得し、適時にポリシーを適用することができます。Webex Extended Security Pack を通じて提供される事前構築された統合により、製品化までの時間が短縮され、重要なデータと知的財産の損失を防ぎます。

図 4 と 5 に、Webex 製品内の DLP ポリシー機能を使用する方法をスクリーンショットで示します。

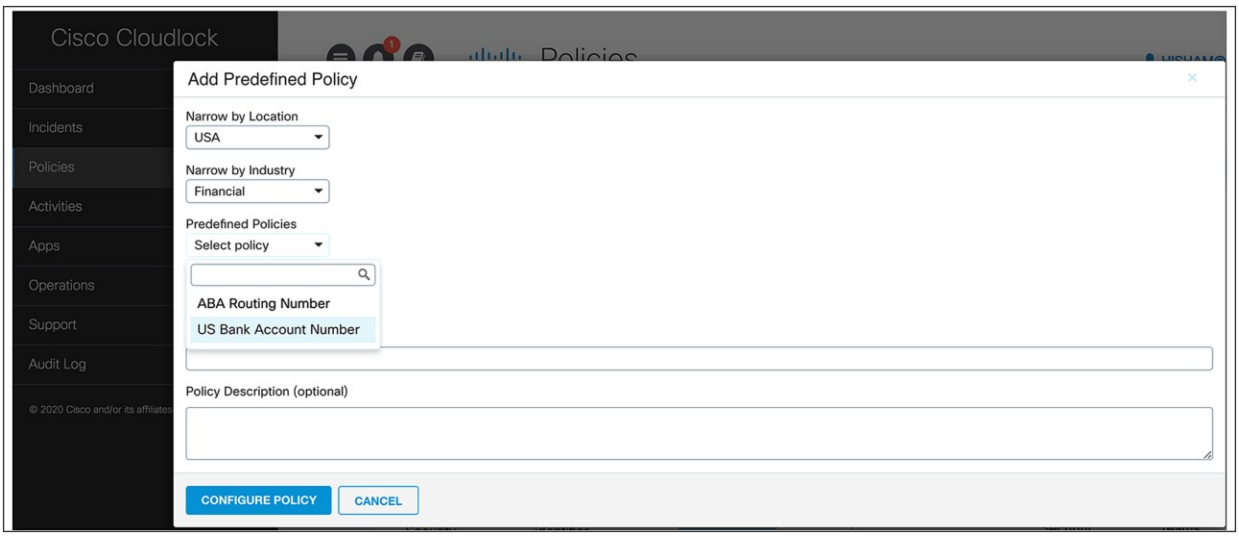

図 4.
定義済みの米国の金融業界ポリシーの設定

図 5.
違反を強調したインシデントダッシュボード

DLP とアーカイブ パートナー エコシステム

シスコは、主要なクラウド アクセス セキュリティ ブローカ（CASB）、DLP、およびアーカイブベンダーとの重要な関係を築き、Cisco Webex プラットフォームで生成されたデータを保護し、事前統合されたエンタープライズグレードのコンプライアンス機能を提供しています。業界をリードするパートナーの例を以下に示します。

Cisco on Cisco の強みと拡張セキュリティオプション

表 8. 利用可能な拡張セキュリティオプション

機能	Cisco Webex
セキュリティバンドル：Cisco Cloudlock	Webex Teams のチームコラボレーションのための統合された CASB と DLP
セキュリティバンドル：Cisco Talos® ClamAV	Webex Teams 内の悪意のある脅威からユーザを保護するためにアップロードおよびダウンロードされたすべてのファイルの、統合されたマルウェア対策スキャン

Cisco Webex Control Hub Extended Security Pack：この Cisco on Cisco のベストオブブリードの統合ソリューションは、お客様の企業データ、パートナー、および顧客を保護するために、きわめて迅速に購入および導入できます。センシティブデータ漏洩を防ぎ、マルウェア対策保護と多要素認証を提供します。

データ損失防止のための Cisco Cloudlock

- Cisco Webex Teams に保存されている機密情報の可視化を実現し、管理します。管理者は、80 を超える既存のポリシーを利用したり、新しいカスタムポリシーを作成したりできます。
- センシティブデータが検出された場合に、優れた自動応答アクションによってクラウドデータ漏洩のリスクを軽減します。ポリシーに違反した場合、Cloudlock は自動的にファイルまたはメッセージを削除し、ユーザまたは管理者に通知し、スペースからユーザを削除します。
- クラウドアプリケーションのセキュリティ インシデント ライフサイクルにおけるコンプライアンス規制への準拠を、SIEM システムから直接サポートします。

マルウェア対策保護のための Cisco TalosClamAV

Cisco TalosClamAV は、Webex クラウドに組み込まれたマルウェア対策エンジンです。これは、すべてのファイルのアップロードをスキャンして、トロイの木馬攻撃、ウイルス、マルウェア、およびその他の悪意のある脅威をスキャンします。指定した Webex Teams スペース内のすべてのファイルは、外部ユーザによってアップロードされた場合でも、スキャンおよび修復されます。感染したファイルは明確にマーキングされ、エンドユーザは企業管理デバイスと個人管理デバイスの両方でダウンロードできなくなります。Cisco TalosClamAV は、1,000 万を超えるユーザの 10 億ものファイルを毎日スキャンし、年間 7.2 兆もの攻撃を阻止しています。

お問い合せ先

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

C11-743769-00JA 20.06