ホワイトペーパー

Webex のセキュリティ上の強み

webex by CISCO

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実績に基づき、Webex は、お客様データの保護、コンプライアンス状況の可視化、会議の管理をサポートしています。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。

Webex は、電話、会議、メッセージ、ホワイトボード共有、ビデオデバイス、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ています。すべての製品は、シスコ セキュア開発ライフサイクル（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、脅威モデリングが含まれています。シスコのセキュリティ&トラスト部門が、Webex のセキュリティとプライバシーを統括し、セキュリティの脆弱性についても公開しています。

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、お客様データの**プライバシー**を尊重することに注力しています。
- Webex は、導入時から**安全**です。
- Webex は、**セキュリティ サイバー ガバナンス**を導入しており、セキュリティ上の問題が見つかった場合の**透明性**を維持します。

データプライバシーとセキュリティプロセス

表 1 は、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を示しています。

表 1. Webex のプライバシーと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	Webex に含まれる機能とコミットメント
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&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 • シスコ セキュア開発ライフサイクル（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）が、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）が、脅威の包括的な調査と防止を担います。 • NDA に基づいて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 のデータとユーザー 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。
中国市場のサポート	• 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ー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。

表 1. Webex のプライバシーと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	Webex に含まれる機能とコミットメント
Cisco Trust Center およびデータ プライバシー プログラム	• 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。 • Cisco Trust Center では、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管理しています。 • 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確認しています。Americas(南・北・中央アメリカ)、EMEAR(欧州、中東、アフリカ、ロシア)、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。
シスコ セキュア開発ライフサイクル (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取得済み • 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。 • ベンダーリスクアセスメント
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 • ロールベースおよび最小権限でのアクセス • 四半期ごとのユーザーアクセスレビュー • 定期的な脆弱性スキャン • 社内および社外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 • 実稼働環境資産の継続的な確認 • 廃棄資産確認 • 論理的に分離された実稼働環境と非実稼働環境

表 1. Webex のプライバシーと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	Webex に含まれる機能とコミットメント
セキュリティとプライバシーの認定	• ISO 27001/27017/27018 • SOC 2 Type II および 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
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）
国を超えたデータ転送	• 拘束的企業準則 • 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 プロセッサー向けプライバシー識別 • EU 標準契約条項

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、電話、データに、安心して Webex を利用できます。

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。また、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、望まない圧力、悪評といったリスクの軽減にもつながります。

Webex は、お客様のデータを保護するようにセキュリティが強化されたコラボレーション プラットフォームです。そのため Webex では、ネットワーク、プラットフォーム、アプリケーションの設計、開発、導入、メンテナンスにおいて、プライバシーとセキュリティを最優先にしています。また、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、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。
- 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。
- Webex は、「need to know」の原則、職務の分離、ロールベースのアクセス、多要素認証に基づいて、管理システムやサポートシステムへのアクセスを管理しています。
- Webex は、ネットワークとシステムをモニターして、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。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公開されています。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、「設計時点からプライバシーを考慮する方針」に基づいたプライバシープログラムを導入しています。このプライバシープログラムには、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、データサブジェクト要求の管理なども含まれています。
- 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、Webex 部門から独立しており、プライバシーとセキュリティのポリシーの強化に専念しています。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

ユーザーとアイデンティティの保護

表 2 に、ユーザー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. ユーザーとアイデンティティの保護

機能	Webex に含まれる機能とコミットメント
エンタープライズグレードのユーザー自動プロビジョニング機能とライフサイクル管理機能（Control Hub）	• Active Directory の同期 : 一方向の同期により、ユーザー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ーが本人であることを検証します。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。 • 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、Okta と Azure AD の統合を通じてユーザー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ーに示します。
サービス全体のアイデンティティの難読化	• ユーザー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。サービスで使用されるのは、ユーザーの電子メールアドレスではなく、難読化された ID のみです。
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 IDaaS パートナー : Microsoft Azure AD、Okta、PingOne、LastPass、Simplified、OneLogin、OnePassword

表 2. ユーザーとアイデンティティの保護

機能	Webex に含まれる機能とコミットメント
個人アカウントを使用した Webex へのログインをブロック	データ損失の懸念を軽減するため、ユーザー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、ユーザー認証環境の変化に適応したりするリスクベースの認証	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、Ping Identity などのゼロトラストソリューションをサポートしています。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、機械学習 / 人工知能に基づく地理位置情報など、30 種類の値を使用して、状況に最適な認証チャレンジを提供します。

ユーザープロビジョニングとライフサイクル管理

ユーザー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、ユーザー、グループ、ボット、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、認証 / 認可を実現できます。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、ユーザーが作成、更新、および削除される前にユーザー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

一方向の同期により、ユーザー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ーが本人であることを検証します。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保できるため、ユーザーを作成する際に、電子メールを受信したり、別の証明サービスを利用したりして本人であることを確認する必要はありません。

SCIM によるユーザープロビジョニング

お客様は、業界標準である SCIM を使用して Okta と Azure AD を統合し、ユーザー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。

新たなユーザーのプロビジョニング

Control Hub では、パートナー、開発者、お客様が、API と CSV を利用してユーザーをプロビジョニングできます。

認証と認可

シスコは、認証 / 認可に必要な標準ベースのセキュアなメソッドをユーザーに提供しています。ユーザーが小規模企業であっても、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っても同じです。ユーザー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のパスワードを要求します。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、各種要素（必要な文字数、特殊文字、大文字、数字など）を変更することで、パスワードの複雑さを変えられます。

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 IDaaS パートナー（Microsoft Azure AD、Okta、PingOne、LastPass、Simplified、OneLogin、OnePassword など）

これにより、企業は Webex からユーザーを IdP にリダイレクトすることができます。また、ユーザーは、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で使用できます。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、ほとんどの人は、5 つ未満のパスワードを異なるインターネットサイトで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をします。Cisco Duo は、市場における主要な多要素認証ソリューションです。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ています。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ています。

リスクベースの認証
Webex は、主要な IdP プロバイダーと連携して、Cisco Duo、Okta、Microsoft AzureAD、ForgeRock、Ping Identity などのゼロトラストソリューションをサポートし、それらのベンダーのリスクベースの認証モジュールと統合しています。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、機械学習 / 人工知能に基づく地理位置情報など、30 種類の値を使用して、状況に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ー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。

個人アカウントを使用した Webex へのログインをブロック
Webex にアクセスする際に、すべてのユーザーが企業アカウントのみを使用するようにできます。シスコは、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 からのユーザー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ー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	Webex
MAM アプリのラッピングプロセス	Webex でサポート
MDM の検証	Webex でサポート
AppConfig のサポート	Webex でサポート
Microsoft Intune SDK のサポート	Webex でサポート
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 でサポート
PIN ロック要件 : Webex のネイティブセキュリティ管理	Webex 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 でサポート
IP 範囲に基づくファイル共有管理	Webex でサポート
Active Directory グループに基づくファイル共有管理	Webex 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 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 のブラウザベースクライアントと 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 Webex モバイル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に沿った方法で、安全に Webex の利用が開始できます。

MDM の検証

すべての Webex モバイルアプリは、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、リモートでのアプリケーションの削除など）に関して、マルチデバイス管理（MDM）プロバイダーで検証されています。

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に Webex Meetings アプリや Webex Messaging 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にユーザーがアクセスするのを制御できます。

Microsoft Intune SDK のサポート

Webex モバイルアプリケーションは、Microsoft Intune とソフトウェア開発キット（SDK）の統合をサポートしています。IT 管理者は、この SDK を利用することで、Webex Meetings および Messaging のアプリケーション機能と設定ポリシーにユーザーがアクセスするのを制御し、企業データを管理 / 保護できます。

Webex のネイティブセキュリティ管理

Webex 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。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**：デバイスの紛失時やユーザーの退職時に、管理者はデバイス上のコンテンツをリモートから消去できるため、企業の知的財産を保護できます。
- **PIN ロック要求**：BYOD 環境を使用するお客様は、ユーザーが Webex モバイルアプリを使用する際に、個人管理のデバイスで必ず PIN ロックを設定するように依頼できます。
- **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、ユーザー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、交換されるメッセージを近くのユーザーがのぞき込めないようにすることが可能です。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、他のユーザーは、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 Webex 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 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ーは、ノート PC がロックされていないことを心配する必要はありません。管理者は、Control Hub でカスタムタイムアウトを設定することができます。一定期間のタイムアウト（10 ～ 60 分）の後でアイドルセッションが終了するため、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。ユーザーが 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。

デフォルトで提供されるコンテンツ保護

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

表 4. コンテンツの保護

機能	Webex に含まれる機能とコミットメント
Webex Meetings のエンドツーエンドの暗号化	• 会議の主催者は Webex Meetings を使用するときに暗号化を指定できます。 • 優れた拡張性 • 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 は、会議暗号化キーにアクセスできません。
Webex でのエンドツーエンドの暗号化	• ユーザーが生成して Webex スペースで共有されるコンテンツ（メッセージとファイル）は、いくつかの例外を除き、TLS 経由でクラウドに送信される前に、Webex アプリによってエンドツーエンドで暗号化されます。このユーザーが生成したコンテンツは、暗号化された状態でクラウドに保存されます。 • エンドツーエンドの暗号化キーは、Webex キー管理サービス（KMS）を使用して、Webex スペースごとに作成されます。 • お客様は、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、お客様がキーを保持できます。
社内での録音の議事録	• すべての録画および録音と文字起こしは AES256 で暗号化され、クラウドに保管されます。 • 録画および録音は、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。 • お客様のデータを文字起こしサービスのテストに使用することはありません。
コンテンツ共有の保護	• 録画および録音の再生はサインインしたユーザーのみに制限します。 • 録画および録音のダウンロードを禁止できます。 • ネットワーク上にあるすべての録画および録音にパスワードを適用します。 • 外部システムとの連携による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	Webex に含まれる機能とコミットメント
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ーのみに、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。
会議を内部ユーザーのみに制限	• 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。 • 出席者ロールが必要です。
招待状の転送を防止	• 招待されたユーザー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	• 名簿に登録された内部ユーザーと外部ユーザーを視覚的に区別できます。 • 入室と退室の色が分かれています。 • ルームをロックできます。 • 不在中に個人ルームのロビーに誰かが入室した場合、電子メール通知が送信されるように設定できます。 • チャット、ビデオ、音声オプションなどの使用可能な機能の有効 / 無効を制御できます。 • 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ができます（Meetings と Messaging）。 • 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 Messaging）。
外部システムとの連携の管理（Meetings と Teams）	Webex でサポート
ボットの管理	Webex でサポート

外部システムとの連携の管理

お客様は、ユーザーが、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 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したサードパーティ製アプリケーション（developer.webex.com の API を使用して開発）のみを、ユーザーに対して有効化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ーに対して、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 スペース用ボットを管理することで、情報の流出を制御し、リスクを軽減できます。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、個別に許可すれば、組織の従業員がグループスペースや 1 対 1 のスペースでボットを利用できます。

外部とのコミュニケーションのブロック

外部とのコミュニケーションをブロックする機能を使って、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ーは、Webex から外部組織のユーザーとのコミュニケーションをすべて制限されています。
- 組織内のユーザーは、承認済みドメイン以外のユーザーを追加したり、Webex の未承認ドメインで作成されたスペースに参加したりすることはできません。
- 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）] を使用して、外部サイトにいる参加者を制御およびブロックします（図 1）。

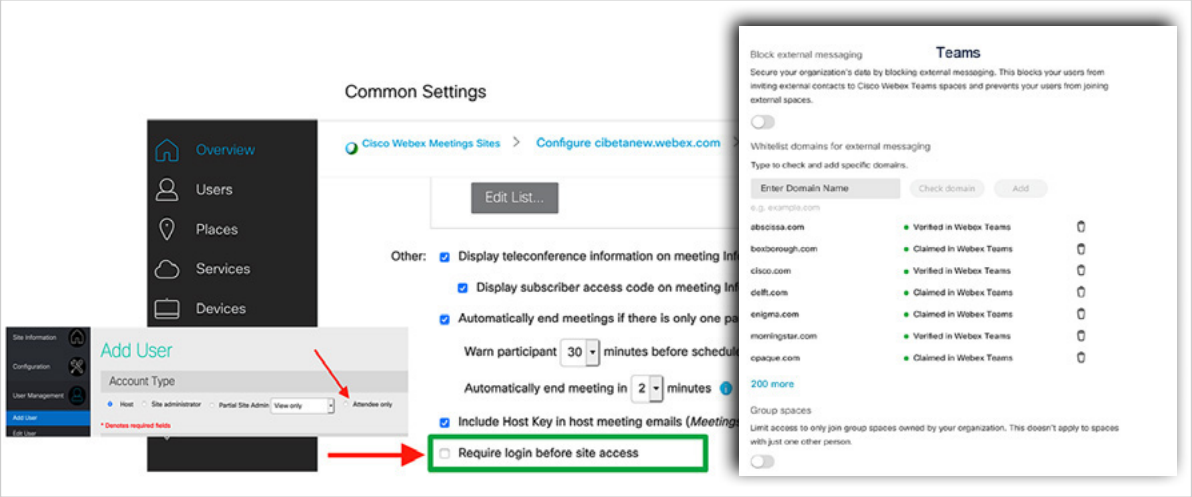

図 1. 外部とのコミュニケーションのブロック

組み込み型のコンプライアンスツール（サードパーティ製ソリューションが不要）

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	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 日間から無期限で、メッセージとファイルを保持（Webex Messaging）
法的保留	・ ユーザーが生成したコンテンツ（メッセージとファイル）に対して Webex Messaging でネイティブにサポート
eDiscovery	・ ユーザーが生成したコンテンツ（メッセージとファイル）に対して Webex Messaging でネイティブにサポート

Control Hub に組み込まれている単一のコンプライアンスツールを利用すれば、組織は、サードパーティのコンプライアンス ソリューションを利用しなくても、コンプライアンスを確保し、リスクとコストを削減できます。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、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 内で組織全体の保持ポリシーを定義するか、Webex Meetings にサイトレベルのデータ保持ポリシーを定義することで、関連するすべてのコンテンツが、設定された保持タイムフレームで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

コンプライアンス要件に対応して法的調査をサポートするために、Control Hub の法的保留ツールを使用することで、組織は、エンドユーザー 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、ユーザー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（ユーザー）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。

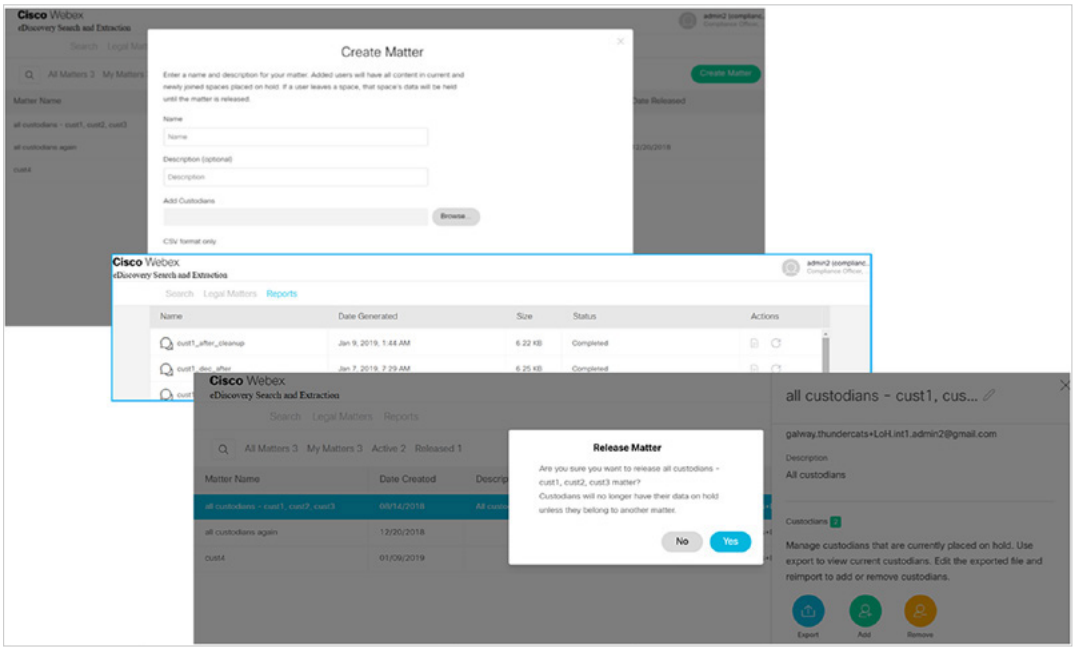

図 2. 案件の作成、表示、およびリリース

eDiscovery

Control Hub に組み込まれている eDiscovery 検索ツールを利用すれば、特定のカストディアン（ユーザー）によって生成されたコンテンツを、希望の期間で検索して抽出できます。コンプライアンス責任者として、eDiscovery を使用して Webex アプリ内のすべてのコミュニケーションを検索できます（図 3）。社内の特定の人物を探し、その人が共有しているコンテンツや特定のスペースを検索してから、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。

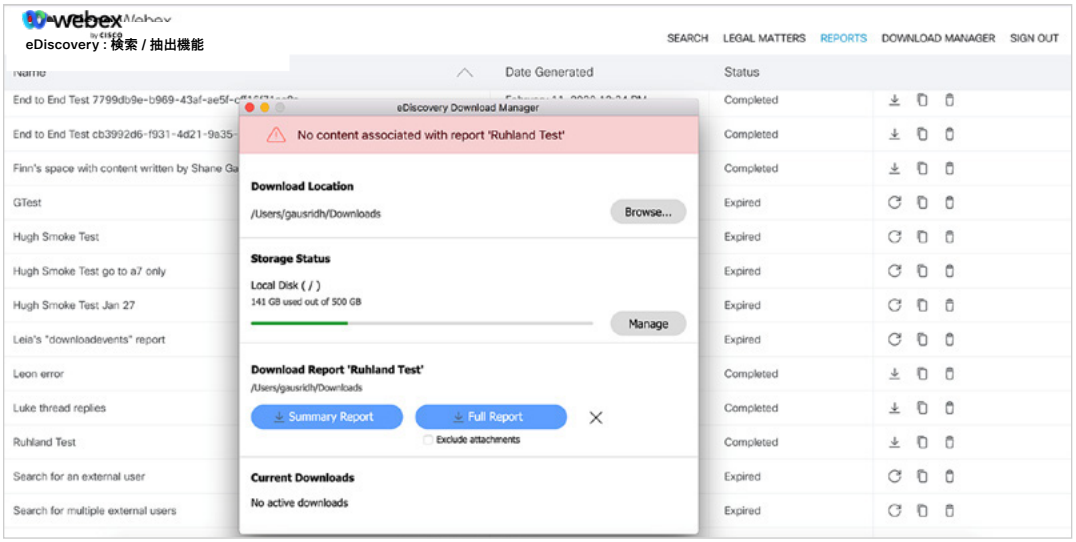

図 3. Webex 内のデータの検索

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	Webex
センシティブデータ漏洩の保護	• Cisco Cloudlock® および Webex 向けサードパーティ製品との連携 • Webex 専用に作成 / 調整された検出 / 修復ポリシー（スペースメンバーシップ、メッセージ、ファイルベースの違反） • 導入時間を短縮するために特定の規制対象業種（金融、医療など）向けに事前に設定されたポリシー
DLP とアーカイブ パートナー エコシステム	• 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で、10 を超える業界トップクラスのアーカイブベンダーおよびデータ損失保護 / クラウド アクセス セキュリティ ブローカ（CASB）ベンダーと連携しています。 • 事前に構築してテストされた統合機能により、カスタム開発作業が少なくて済み、製品化までの時間が短縮されます。 • 大規模なパートナーエコシステムにより、お客様は、すでに利用しているパートナーベンダーのデータ損失保護製品を使用することもできます。
組織を超えたポリシー適用	• 外部とのすべてのコミュニケーションブロックします。 • 外部の特定のドメインとのコミュニケーションを許可します。
スペース分類	• 管理者は、Webex で作成されたスペースをエンドユーザーに分類させることができます。 • センシティブデータが不注意で漏洩するのを防止できます。

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、ユーザー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が発生する可能性のある多くの業種全体で、事前に定義された豊富なポリシーをサポートする必要があります。

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（エンドユーザーと管理者に）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ーを削除したり、ユーザー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、ユーザーが誤ってまたは故意に共有しないようにします。

コミュニケーションの境界線が組織の外部まで拡大すると、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、ユーザー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、ユーザー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。

Webex は、パブリック REST API（イベント API と呼ばれます）を提供しています。パートナーは、この API を呼び出すことで、組織内のすべてのユーザーによって生成されたデータを取得できます。パブリックインターフェイスを利用すれば、すべてのパートナーが Webex と統合して目的のイベントを取得し、適切なタイミングでポリシーを適用できます。Webex 拡張セキュリティパックを通じて提供される事前構築された連携機能は、製品化までの時間を短縮し、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。

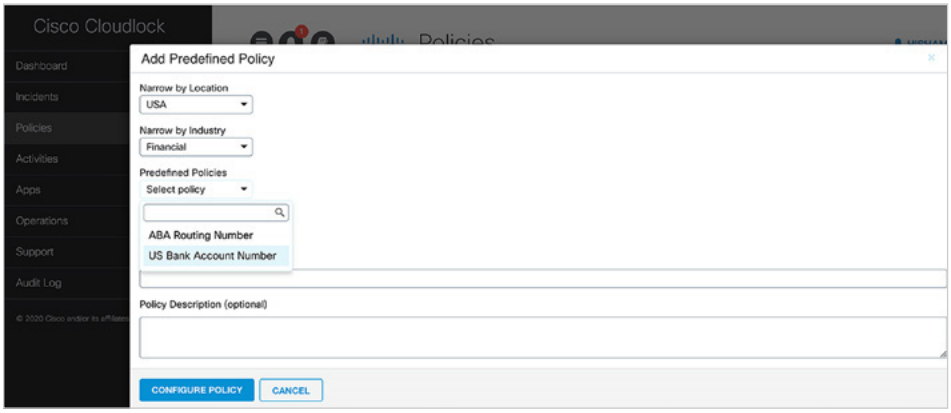

図 4. 定義済みの米国の金融業界ポリシーの設定

図 5. インシデントダッシュボードでの違反の強調表示

スペース分類

スペース分類機能により、組織の管理者は、データガバナンスポリシーに基づいて分類ラベルを定義し、それを利用して、すべてのユーザーに、作成したスペースを分類させることができます（「公開」、「機密」、「極秘」、「秘密」など）。管理者は、既存の分類を編集したり無効にしたりすることができます。また、新しい分類を追加することも可能です。そのため組織は、分類基準と標準を長期的に改善していくことができます。

直感的なクライアントビジュアル設計により、スペースの分類レベルと分類コンテキストをユーザーが把握できるため、センシティブデータを処理する際にコンプライアンスを確保するのに役立ちます。分類済みの各スペース内のメッセージ作成エリアに目立つように表示された分類バッジによって、スペースの機密性についてユーザーに注意を促すことができ、不注意によるデータ損失を最小限に抑えられます。

DLP パートナーは、コンプライアンス API を活用して分類イベントを利用し、豊富なコンテンツとコンテキストに基づいたポリシーを適用することで、知的財産およびデータが漏洩するのを防げます。また、提供された API を使用してデータ共有を管理するルール（例：機密データが共有されるスペースには外部の人間を参加させない）を適用することで、組織のユーザーが、機密情報の共有に関する企業全体のデータガバナンスポリシーに自動的に対応できるようになります。

注：ポリシーは外部の DLP エンジンに適用する必要があり、Webex のネイティブではサポートされていません。Webex で提供するのは必要な API のみです。

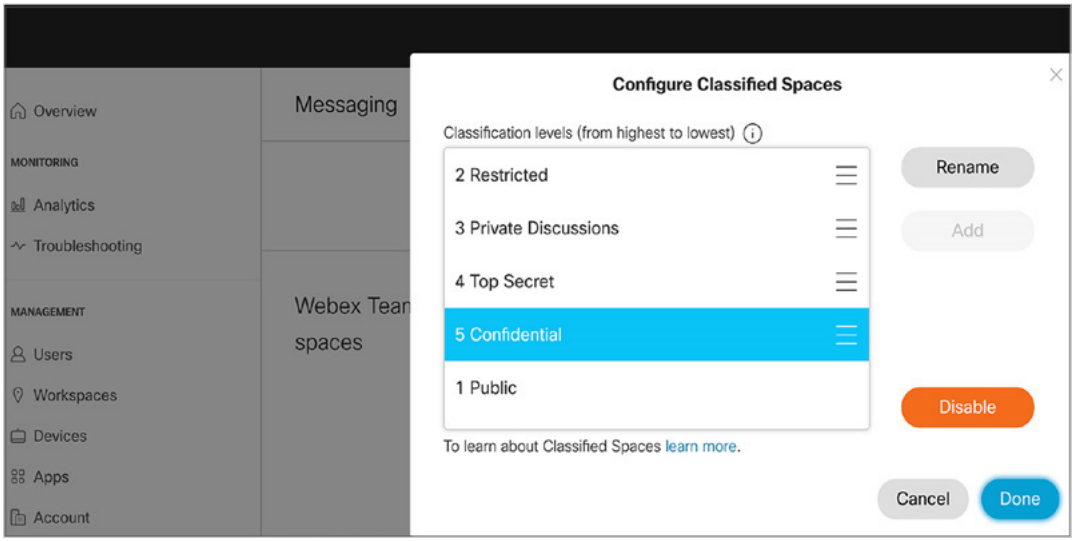

図 6. スペース分類用の Control Hub 設定

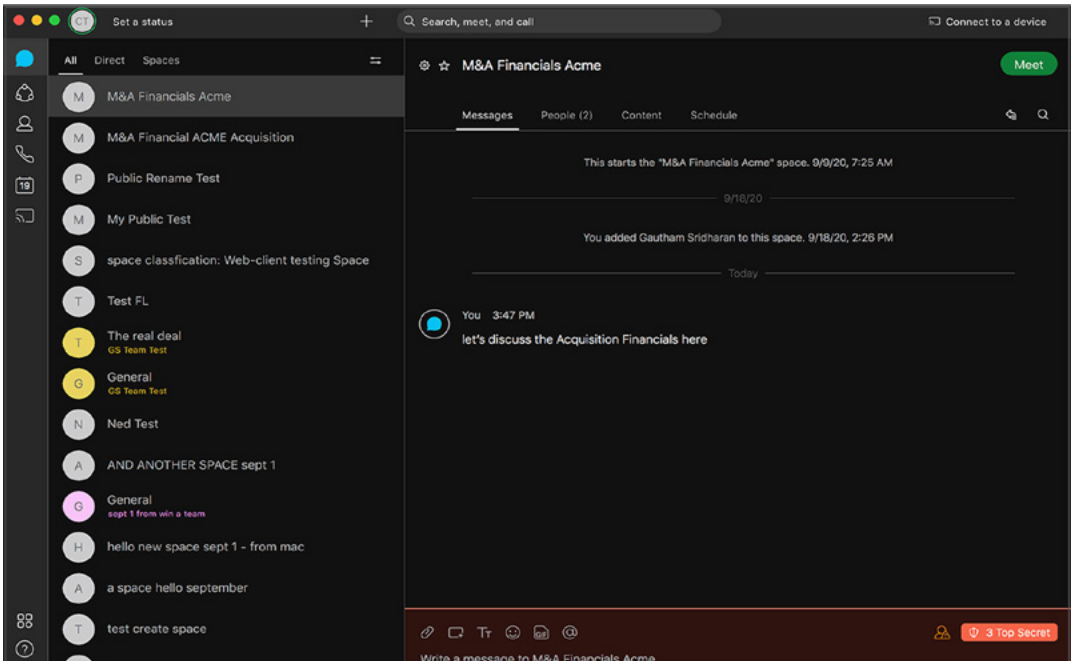

図 7. スペース分類用の Control Hub スペースラベル

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、アーカイブベンダーと重要な関係を築くことで、エンタープライズグレードのコンプライアンス機能を事前に統合し、Webex で生成されたデータを保護しています。業界をリードするパートナーの例を以下に示します。

図 8. Webex DLP/ アーカイブパートナー

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	Webex
セキュリティバンドル：Cisco Cloudlock	Webex Messaging でのチームコラボレーションのために統合された CASB と DLP
セキュリティバンドル：Cisco Talos ClamAV	Webex 内の脅威からユーザーを保護するために、アップロード / ダウンロードされたすべてのファイルのマルウェアをスキャンする統合マルウェア対策機能

Control Hub 拡張セキュリティパック

この Cisco on Cisco の優れた統合ソリューションは、お客様の企業データ、パートナー、顧客を保護するために、非常に迅速に購入して導入できます。マルウェア対策機能と多要素認証機能を備え、センシティブデータの漏洩を防ぎます。

データ損失防止のための Cisco Cloudlock

- 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、ユーザーまたは管理者に通知し、スペースからユーザーを削除します。
- 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いて、コンプライアンス規制に準拠するための機能を、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、組み込みのマルウェア対策エンジンです。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、マルウェアなどの脅威をスキャンします。指定した Webex スペース内のすべてのファイルは、外部ユーザー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、エンドユーザーは、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 万を超えるユーザーの 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。

詳細情報
webex.com をご覧ください

2021 年 6 月