Webex Control Hub

Extended Security Pack データシート

目次

Webex® は、パートナーとのコラボレーションであれ、お客様の顧客とのコラボレーションであれ、人同士、そしてその仕事を結び付けます。

Webex は、従業員とカスタマーエクスペリエンスを最適化し、近代化するために、非常に安全な世界クラスのメッセージング、会議、およびコールエクスペリエンスを、モバイルから会議室まで幅広いケースで提供します。

製品概要

企業は、従業員がコラボレーション ツールを使用して偶発的に、または意図的に機密情報や重要な情報を送信しないように制御する必要があります。このような情報の例としては、知的財産、患者記録、クレジットカード番号、社会保障番号などがあります。

IT 管理者は、外部でファイルを共有したり、企業の IT チームが管理していないデバイスを使用したりするときに配布される可能性のあるマルウェアやランサムウェアからも保護する必要があります。

Extended Security Pack for Control Hub は、アドオン Flex コラボレーションオファーにデータ損失防止機能とマルウェア対策機能をバンドルすることで、会社のデータ、パートナー、顧客を保護するのに役立ちます。

Extended Security Pack は、コラボレーション管理者に俊敏性と安心感を提供します。これにより、すべての情報セキュリティの問題に 1 つの緊密に統合されたソリューションで対処することで、Webex をより安全に企業に導入できます。

データ損失防止（DLP）

Extended Security Pack には、Cisco Cloudlock® for Webex のすべての機能が含まれています。Cloudlock は、Webex に保存されている機密データを完全に可視化し、制御することで、組織がより安全に Webex を採用できるようにします。Cloudlock は、個人を特定できる情報（PII）、個人の健康情報（PHI）、および支払いカード情報（PCI）などの重要な情報、および法規制の遵守と内部データ保護の義務を順守するその他の機密情報を特定します。機密情報が顧客ポリシーに違反して検出されると、Cloudlock はインシデントをトリガーし、エンドユーザーと管理者に違反を通知し、Webex スペース、Webex Meetings の会議後のトランスクリプトそして、ハイライトから違反コンテンツ（ファイルまたはメッセージ）を削除するなどのリスクに適切なアクションを自動的に実行します。図 1 は、Cloudlock 内のインシデント表示のスクリーンショットです。

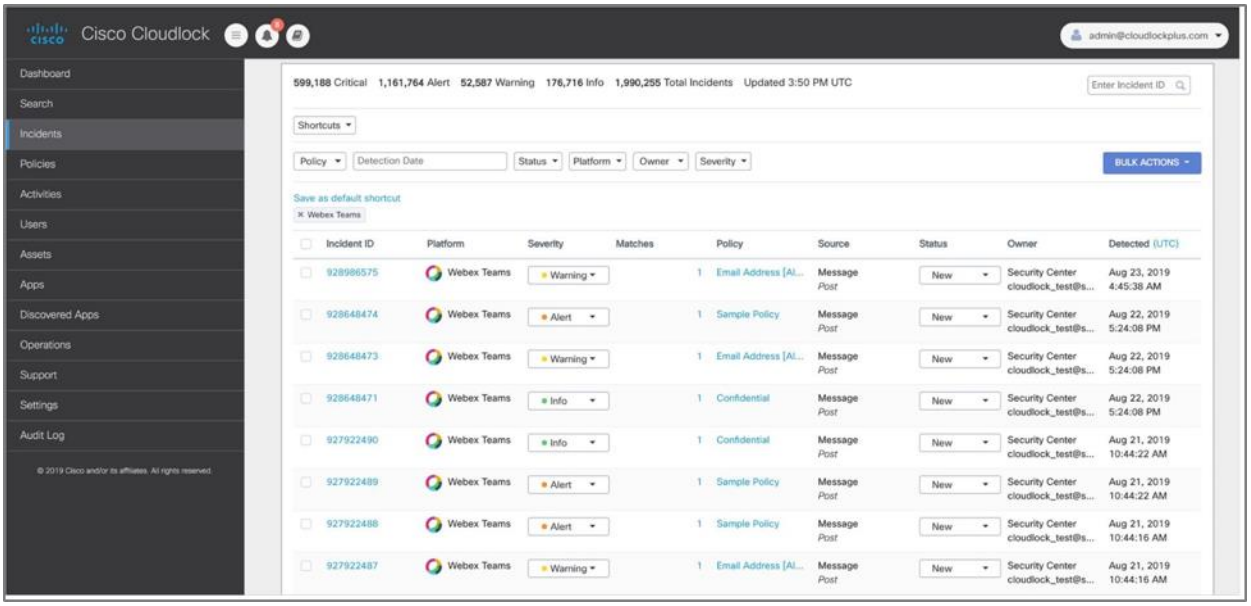

図 1.
Webex 用 Cisco Cloudlock - インシデント表示

主な機能のハイライト

クラウドアプリケーションにおけるデータ漏洩リスクの軽減

クラウド環境のコラボレーション性と、ユーザによる機密情報へのアクセス、作成、共有の容易さを考えると、クラウドでのデータ漏洩の防止は困難な場合があります。組織は、従来のデータ保護ツールと、クラウド環境内で提供される限られたレベルの可視性と制御の間のギャップを埋めるのに苦労しています。これは特に、クラウドアプリケーションが外部ユーザー、または企業ネットワーク上にいないリモートのローミング従業員によってアクセスされている場合に当てはまります。

クラウド環境内の機密データの識別

Cloudlock は、クラウド環境に保存されている機密情報がポリシーに違反していることを特定できる強力なクラウドデータ損失防止（DLP）エンジンを使用して、Webex 環境を継続的に監視します。Cloudlock を使用することで、セキュリティ専門家は、クレジットカードデータ保護基準（PCI-DSS）や HIPAA 遵守、カスタムポリシーなどの一般的な機密情報セットに焦点を当てた、すぐに使用できるポリシーを適用して、知的財産などの所有データを特定します。カスタム正規表現（RegEx）入力、しきい値設定、およびプロキシミティ制御などの高度な機能により、真陽性率が高く、偽陽性率が低くなります。

自動応答によるリスクの軽減

Cloudlock は、設定可能なクロスプラットフォームの自動応答アクションを提供することで、検出を超えたクラウド DLP を実現します。Cloudlock は、API 主導のクラウド アクセス セキュリティ ブローカ（CASB）アーキテクチャを通じて、Webex のネイティブ機能（エンドユーザおよび管理者の通知から機密データの自動削除まで）を活用する、高度で統合された応答ワークフローをサポートします。図 2 は、Cloudlock の自動応答の Web インターフェイスを示しています。

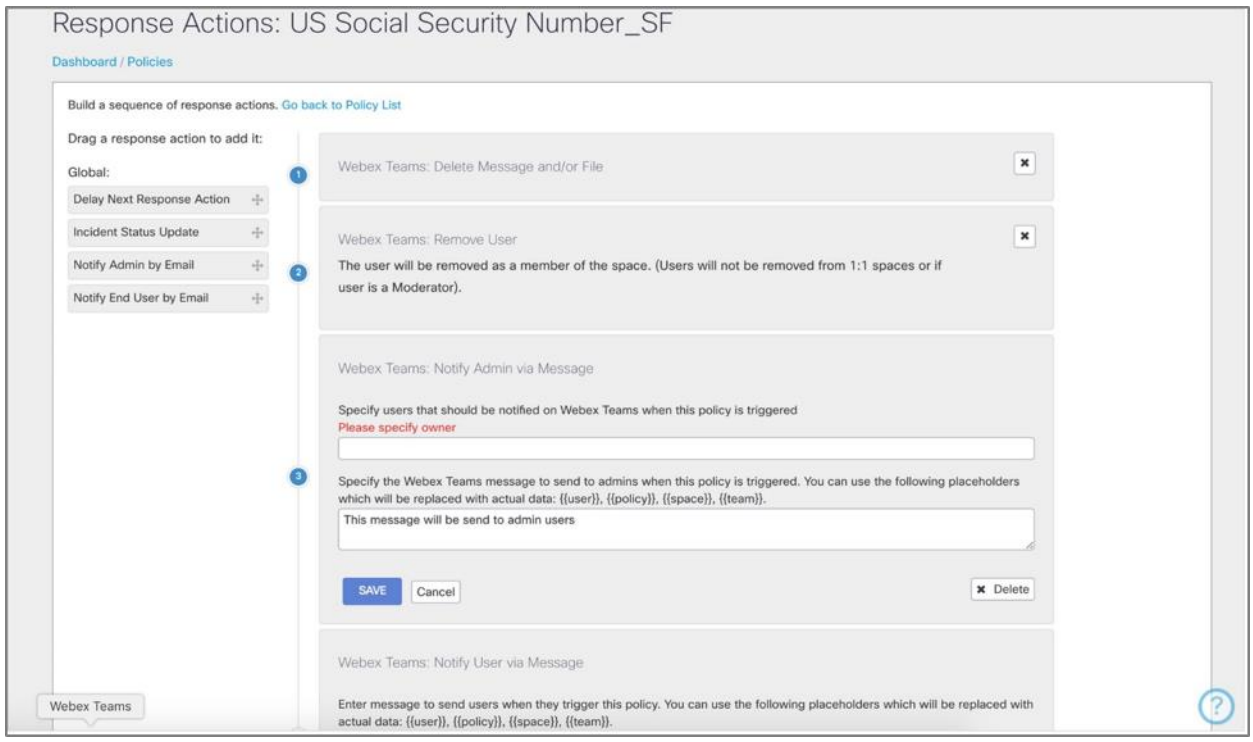

図 2.
Webex 用 Cisco Cloudlock - 自動応答

マルウェア対策機能

Extended Security Pack には、ビルトインのマルウェア対策エンジンが含まれています。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、エンドユーザーは企業管理デバイスと個人管理デバイスの両方で該当ファイルをダウンロードできなくなります。この Extended Security Pack のサブスクリプションの一部としてスキャンできるファイルの数に制限はありません。

図 3 は、ファイルをブロックする Extended Security Pack のインスタンスを示しています。

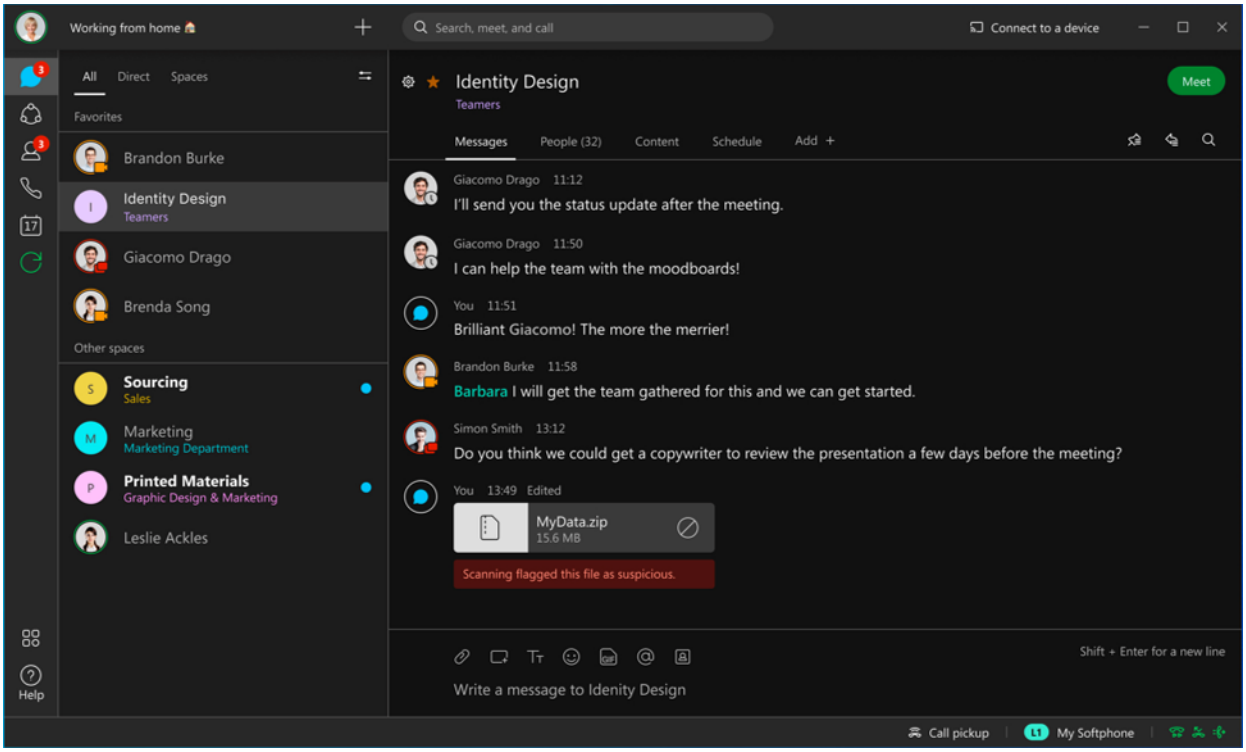

図 3.
感染ファイルのブロック

Ethical Wall

Ethical Wall（内部通信のブロックとも呼ばれます）を使用すると、Webex 管理者は Control Hub で簡単なルールを定義して、特定のユーザーグループが Webex Spaces 内で相互にコラボレーションするのを防ぐことができます。管理者は、Active Directory（AD）グループごとに最大 5 つのポリシーを構成できます。ポリシーを定義すると制限されたグループは、お互いをスペースに招待できなくなるか、会話ができなくなりますが、社内の他のユーザーとは連絡を取り合うことができます。通常、ポリシーの施行は制御されています（つまり、違反は発生前に特定され、ブロックされます）。

例えば、大手銀行では利益相反を避けるために、投資担当者と企業調査アナリストのコミュニケーションを制限する必要があります。

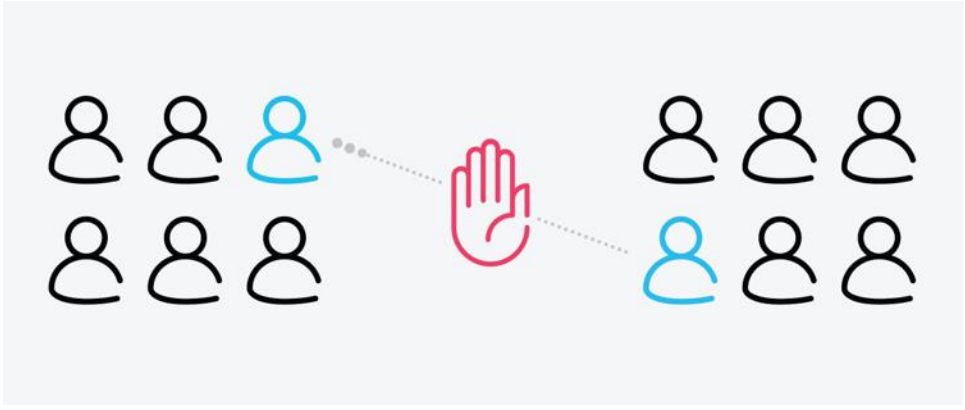

図 4.

Ethical Wall

Webex を使用すると、エンドユーザーは、誰と連絡を取り合えるかを心配する必要が無くなります。これは、Ethical Wall 企業ポリシー Webex は、Webex Control Hub で定義されたシンプルなルールに基づいて制限付きかつ未許可のユーザーを招待することを自動的自動的にブロックするためです。

この機能により、組織は関連する企業の業界標準規格および規制（FINRA など）への遵守を維持し、潜在的な利益相反を回避できます。

Ethical Wall 機能は、Control Hub で管理者がこの機能を有効化した後に先々の事を考えて機能します。今後の機能強化（現在は利用制限中）では、Webex Spaces の既存の違反を遡及的にスキャンし、ポリシーに準拠していないスペースからユーザーを追い出し、違反を排除する機能を提供します。このシナリオは通常、ユーザーが転職し、その過程で AD グループメンバーシップの変更が発生したときに発生します。このメンバーシップ変更により、1 つ以上の Ethical Wall ポリシー違反に該当する場合があります。

注： 上記の遡及的なポリシー適用のサポートは間もなく開始され、機能の一般提供時に利用可能になります（目標:22 年第 1 四半期）。

機能要約

表 1 に、Webex のコンプライアンス機能の概要を示します。

表 1. コンプライアンス機能

機能	説明
データ損失防止	Cisco Cloudlock を使用すると、次のことが可能になります。 • Webex 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 以上の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	ビルトインの高性能のマルウェア対策エンジン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、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。感染したファイルはマークされ、エンドユーザはダウンロードできません
Ethical Wall	IT 管理者は、組織内の特定のユーザーグループ間における連絡の取り合いを防ぐことができます。これは、組織が関連する業界標準規格および規制（FINRA など）への遵守を維持し、潜在的な利益相反を回避するのに役立ちます。

発注情報

Webex Extended Security Pack は、Collaboration Flex Plan のサブスクリプション（A-FLEX）内で購入できます。この機能を Collaboration Calling または Meetings のサブスクリプションに追加する方法の詳細については、『Collaboration Flex Plan Ordering Guide』を参照してください。

表 2. 製品の SKU および説明

PID PID	説明
A-FLEX-NU-SEC-PK	Extended Security Pack NU アドオン
A-FLEX-EA1-SEC-PK	Extended Security Pack EntW アドオン（250 ～ 1,999 KW）
A-FLEX-EA2-SEC-PK	Extended Security Pack EntW アドオン（2,000 ～ 9,999 KW）
A-FLEX-EA3-SEC-PK	Extended Security Pack EntW アドオン（10,000+ KW）
A-FLEX-AU1-SEC-PK	Extended Security Pack Active User アドオン（250 ～ 1,999 KW）
A-FLEX-AU2-SEC-PK	Extended Security Pack Active User アドオン（2,000 ～ 9,999 KW）
A-FLEX-AU3-SEC-PK	Extended Security Pack Active User アドオン（10,000+ KW）
A-FLEX-SEC-PK-ENT	Extended Security Pack 権限

よくある質問

Q. Extended Security Pack の Cloudlock 機能の制限はありますか。

A. いいえ。Cisco Cloudlock のすべての機能が Extended Security Pack にパッケージ化されています。必要なのは、Control Hub でコンプライアンス責任者ユーザをプロビジョニングし、そのユーザに Webex 向け Cloudlock を承認させることだけです。

Q. Webex 向け Cloudlock を気に入った場合は、他の SaaS や Box などのクラウドサービスに使用して保護できますか。

A. はい。アカウントチームまたはパートナーに連絡することで、Box およびその他の SaaS サービスの追加ライセンスを購入できます。すべてのアプリケーションの管理は、単一のコンソールを介して行われます。

Q. デバイスにすでにマルウェアスキャナがあるため、DLP 機能のみを有効にできますか。

A. はい。マルウェアスキャンを有効または無効にする Control Hub 設定があります。

Q. マルウェアスキャンはファイルのアップロードを遅らせ、ユーザエクスペリエンスに影響しますか。

A. いいえ。マルウェア対策エンジンのパフォーマンスは高く、数秒以内にファイルがスキャンされます。ファイルはすぐにスペースにアップロードされますが、マルウェアのスキャンが完了するまでダウンロードまたはプレビューできません。エンドユーザエクスペリエンスに目に見える違いはありません。

Q. 管理者は、組織のマルウェアスキャンを無効または有効にすることができますか。

A. はい。管理者は Control Hub で組織のマルウェアスキャンを無効にすることができます。

Cisco Capital

目的達成に役立つ柔軟な支払いソリューション

Cisco Capital により、目標を達成するための適切なテクノロジーを簡単に取得し、ビジネス変革を実現し、競争力を維持できます。総所有コスト（TCO）の削減、資金の節約、成長の促進に役立ちます。シスコの柔軟な支払いソリューションは 100 か国以上で利用可能であり、ハードウェア、ソフトウェア、サービス、およびサードパーティ製の補完的な機器を、利用しやすい計画的な支払方法で購入できます。詳細はこちらをご覧ください。

米国本社
Cisco Systems, Inc.
サンノゼ(カリフォルニア州)

アジア太平洋本社
Cisco Systems (USA) Pte. Ltd.
シンガポール

ヨーロッパ本社
Cisco Systems International BV Amsterdam,
アムステルダム(オランダ)

シスコは世界各国 200 箇所にオフィスを開設しています。各オフィスの住所、電話番号、FAX 番号は当社の Web サイト(https://www.cisco.com/go/offices [英語])をご覧ください。

Printed in USA C78-742773-03 01/22