Cisco Webex Control Hub

（コンプライアンス）

目次

コンプライアンスの概要

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、または悪意を持って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、クレジット カード番号、ソーシャル セキュリティ番号、知的財産、患者記録などがあります。Cisco Webex Teams™ は、いくつかのデータ損失防止（DLP）ソリューションと統合されています（Webex Teams の API を使用）。

違反の影響は深刻である可能性があるため、シスコは Webex® ポートフォリオに統合と制御を導入し、お客様がコンプライアンス ポリシーの適用を管理できるようにしています。Cisco Webex® Control Hub は、Cisco Webex サービスのプロビジョニングと運営と管理が可能な Web ベースの直感的な一括管理型管理ポータルです。

Pro Pack for Webex Control Hub は、さらに高度な機能や、既存のソフトウェア（コンプライアンス、セキュリティ、分析）との統合を必要とするお客様向けのプレミアム サービスです。

法的な理由で従業員が生成したコンテンツを検索・抽出されたい場合、e-discovery 検索および抽出機能を使用して、コンプライアンス管理者がこの情報をレポートで抽出できるようにします。

さらに、コンプライアンス責任者は保持ポリシーに例外を追加し、ユーザが調査中の場合はそのユーザを法的保留にすることができます。これにより、調査中に組織全体の保持ポリシーによってユーザが自身のコンテンツを保持し、削除できないようにすることができます。

また、企業はビジネス価値のないデータを定期的に消去することで、セキュリティ リスクを制御し、責任を抑えたいとも考えています。保持機能により、それを行うことができます。

また、Cisco Webex Teams は、Webex Teams の既存のネイティブ ファイル共有とストレージに加えて、IT 管理者がユーザに対して Microsoft OneDrive および SharePoint Online をエンタープライズ コンテンツ管理（ECM）ソリューションとして有効にできる柔軟性も備えています。そのため、ユーザは Webex Teams の作業スペース内の最新の OneDrive ファイルおよび SharePoint Online ファイルを共有、編集、取得でき、それと同時にファイルは ECM で安全に保管され、お客様の既存の DLP/CASB およびマルウェア対策ソリューションを通じて保護されます。

スペースの所有

Webex Teams は、組織の境界を超えたコミュニケーションを可能にします。そのため、ユーザは他の企業の社員と通信することができます。また、Webex Teams はスペースの所有権という概念を使用します。所有ルールは、グループ スペースと個人とのコミュニケーションによって異なります。

グループ スペース

グループ スペースの場合、単一の組織がそのスペースの所有者です。ユーザがスペースを作成する組織がスペースの所有者となります。スペースを所有する組織には、特定の権限があります。組織に、その組織が所有していない参加者であるユーザがいる場合、その組織を参加組織と言います。

表 1 に、コンプライアンス責任者のコンテンツ権限の概要を示します。

表 1. グループ スペースに対するコンプライアンス責任者のコンテンツ権限

特権	所有している組織	参加組織
作成		
スペースにコンテンツを投稿する	×	×
読み取り		
自身のユーザがスペースに投稿したコンテンツ（メッセージとファイル）を読む	○	○
スペース内の任意のユーザが投稿したコンテンツを読む	○	×
更新		
ユーザがスペースに投稿したコンテンツを変更する	×	×
削除		
スペースの保持ポリシーを定義する	○	×
任意のユーザがスペースに投稿したコンテンツを削除する	○	×
自身のユーザによって投稿されたスペース内のコンテンツを削除する	○	○

2 つの異なる組織の参加者を含む Cisco Webex Teams の 1 対 1 のスペースには、そのスペースを所有する組織は存在しません。代わりに、スペース内のユーザが組織によって制御されているかどうかに応じて、2 つの参加組織があります。表 2 に、スペースのコンテンツ権限に関する 1 対 1 のスペース（個人間の通信）での各参加組織の権限の概要を示します。

どちらの組織も、独立した保持ポリシーを設定できます。1 つの組織の保持ポリシーが期限切れになると、そのユーザによって送信されたメッセージが削除されます。2 つ目の組織の保持ポリシーが期限切れになると、そのユーザによって送信されたメッセージが削除されます。

表 2.　1 対 1 のスペースに対するコンプライアンス責任者のコンテンツ権限（個人間の通信）

特権	各参加組織
作成	
スペースにコンテンツを投稿する	×
読み取り	
自身のユーザがスペースに投稿したコンテンツ（メッセージとファイル）を読む	○
スペース内の任意のユーザが投稿したコンテンツを読む	○
更新	
ユーザがスペースに投稿したコンテンツを変更する	×
削除	
スペースの保持ポリシーを定義する	○
任意のユーザがスペースに投稿したコンテンツを削除する	×
自身の組織のユーザによって投稿されたスペース内のコンテンツを削除する	○

イベント API

Webex Teams では、ユーザは社外のユーザを自身の企業が所有するスペースに招待したり、別の会社のスペースに参加したりして、社外のユーザとコミュニケーションを取ることができます。イベント API は、監視組織が所有していないスペースであっても、ユーザのアクティビティを可視化します。イベント API を使用することで、DLP ソフトウェアはこのようなコンテンツの問題を是正するための措置を講じることもできます。https://developer.webex.com/resource-events.html を参照してください。

e-Discovery：検索および抽出

コンプライアンス責任者は、e-discovery 検索および抽出コンソールを使用して、法的調査に必要なデータを抽出できます。電子メール アドレス、スペース ID、またはキーワードを使用してデータを検索できます。また、このインターフェイスを使用して、コンプライアンス責任者は時間枠を指定することもできます。

検索レポートは、JSON 形式でダウンロードできます。必要に応じて、管理者は Webex Teams によって提供される参照スクリプトを使用して、JSON 出力をコンコーダンス形式に変換し、e-discovery ソフトウェアにエクスポートすることができます。この機能へのアクセスは、ロールベースのアクセス コントロール内にある、組織によって定義されたコンプライアンス責任者に制限されます。e-discovery 検索とレポートには、Webex Control Hub からアクセスできます。レポート サマリーには、ユーザ、メッセージ、ファイル、スペース ID の数などの情報が表示されます。

コンプライアンス責任者は、過去のレポートのリストを表示し、JSON 形式でダウンロードしてから、選択した e-discovery ツールにレポートをエクスポートして、法的調査を行うこともできます。レポートは 10 日間利用できます。

組織全体の Webex チームにカスタム保持期間を設定することで、リスクを管理し、グローバルな保持ポリシーにも沿うことができます。Pro Pack for Webex Control Hub により、フルアクセス権を持つ管理者は、組織の保持ポリシーと合わせて、その期間よりも古いデータを消去するための保持期間を Webex Teams に設定できます。デフォルトの保持期間は無期限ですが、最小保持期間を 1 ヵ月単位で設定することで、このデフォルトを上書きできます。保持期間に達すると、すべてのコンテンツ（メッセージ、アクティビティ、ファイル）は削除され、回復不能になります。

データ損失防止（DLP）

Cisco Webex Teams には、2 重の DLP 戦略があります。まず、通信しているコンテキストをユーザに認識させることで、データ損失の可能性について通知します。ユーザには、スペースの所有、保持、外部の参加者の有無に関する情報が通知されます。エンドユーザは、メッセージの削除、開封確認、スペースのロック、モデレータの継承などの伝達制御機能によって権限が強化されます。

この戦略の 2 番目の部分では、メッセージの投稿や削除、ファイルの添付、Webex Teams 内のスペースへのユーザの追加やそこからのユーザの削除などのイベントに API を介してアクセスできるようにすることが含まれます。これにより、DLP ソフトウェアはそれらのイベントを利用して、違反を確認したり、問題を修復するための措置を講じたりできます。管理者は、ユーザの行動を監視して応答するために、Webex イベント API を使用して、イベントとコンテンツをポーリングできます。

DLP インテグレーションにアプローチするには、次の 3 つの方法があります。

- 既製ソリューション：インテグレーションは、主要なコンプライアンス パートナーによって認定されています。クラウド アクセス セキュリティ ブローカ（CASB）、DLP ISV、および Cisco® Cloudlock は、Webex イベント API を介して Webex Teams と統合され、Webex Teams のためのターンキー DLP 機能を提供します。ポリシー違反をチェックし、是正するための措置を講じます。
- エンドツーエンドのカスタム ソリューション: お客様は、シスコ アドバンスド サービスと連携して、優先する DLP ベンダーとのカスタム インテグレーションを構築できます。
- 自己対応型：Webex イベント API は公開されています。お客様は、API を使用して、自社のソリューションや他のサードパーティの DLP ベンダーと統合できます。

アーカイブ統合

お客様は、Cisco Webex イベント API を使用して、アーカイブ ソフトウェアと統合できます。DLP と同様に、アーカイブ統合にアプローチするには、既製ソリューション、エンドツーエンドのカスタム ソリューション、または DIY ソリューションの 3 つの方法があります。

監査管理者のアクティビティ

管理者アクションのログは、多くの組織および業界のコンプライアンス要件です。フルアクセス権を持つ管理者は、Control Hub に保存されている管理者監査ログを使用して、管理者によって実行された重要なアクション（組織設定の変更など）を表示できるようになりました。これらの管理者監査ログは、Control Hub で表示できます。ここで、特定の日付範囲内の管理者アクションを検索したり、特定のアクションまたは特定の管理者を検索したりできます。また、ログをカンマ区切り値（CSV）ファイルにエクスポートできます。

保持

管理者は組織全体のデータ保持ポリシーを定義して、関連するすべてのコンテンツが設定された保持期間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、さらに電子メールやその他のアプリケーションにおける保持ポリシーにも合わせることができます。

法的保留

法的保留機能により、コンプライアンス責任者の役割を持つユーザは、組織の保持ポリシーに関係なく、訴訟が合理的に予想される場合に、ユーザに関連付けられた関係するすべての形式の Cisco Webex Teams のコンテンツを保持できます。コンプライアンス責任者は、法的事項を作成したり、管理者（ユーザ）を法的保留にしたり、問題を表示、ダウンロード、およびリリースしたりできます。法的保留中のデータは、組織の保持期間に基づいて削除の対象となることはありません。ケースがクローズされると、法的保留を解除でき、その時点でそのデータは組織の保持期間に基づいて削除の対象になります。

エンタープライズ コンテンツ管理の統合

Cisco Webex Teams は、ネイティブのファイル共有とストレージに加えて、IT 管理者がユーザに対して Microsoft OneDrive および SharePoint Online をエンタープライズ コンテンツ管理（ECM）ソリューションとして有効にできる柔軟性も備えています。そのため、ユーザは Webex Teams の作業スペース内の最新の OneDrive ファイルおよび SharePoint Online ファイルを共有、編集、取得できます。

Webex Control Hub で 1 回切り替えるだけでセットアップできます。また、既存のファイル共有権限およびデータ損失防止（DLP）ポリシーを変更する必要はありません。IT 管理者は、有効にする SharePoint Online および OneDrive ドメインまたは Microsoft Azure Tenant ID を決定する全権限を有しています。これにより、IT 部署承認のドメインのみ使用できるようになり、ユーザは個人用の OneDrive フォルダを使用できなくなります。これは、データ損失のリスクを排除するだけでなく、マルウェア脅威からの保護を可能にします。

最高レベルの管理の場合、IT 管理者はすべてのコンテンツが既存のエンタープライズ ファイル ストレージ サービスを通じてルーティングされるように、Webex Teams でネイティブ ファイル ストレージをオフにすることもできます。新しいファイルとフォルダは、Webex Teams から OneDrive および SharePoint Online にアップロードできます。また、Webex Teams 内でファイルの共有、表示、共同編集も可能です。

Cisco Webex Teams の ECM 統合ソリューション：

- IT 管理者は、ファイル共有とストレージのために、Webex Teams のネイティブ ファイル ストレージまたは Microsoft OneDrive および SharePoint Online、あるいは両方を有効にすることができます
- ユーザは、Webex Team スペースで ECM システムからファイルを共有、オープン、編集、共同編集することができます
- ユーザは、Webex Team スペースからファイルやフォルダを ECM システムにアップロードすることができます
- ユーザは、共有ファイルを確認して共同編集できる人を定義できます
- ユーザが常に最新バージョンのファイルを表示できるようにします
- ECM ファイル、メッセージ、およびホワイトボード図面へのリンクをエンドツーエンドで暗号化します
- 既存の DLP および CASB と連携します

- Webex Teams スペースで共有されているため、ファイルを追加で複製しません
- 個人用またはシャドー IT の OneDrive または SharePoint Online のフォルダをブロックし、承認されたインスタンスのみ許可します

コンプライアンス機能の概要

表 3 に、Webex Teams のコンプライアンス機能の概要を示します。

表 3. コンプライアンス機能

機能	説明
e-discovery レポート：電子メールベースおよびスペースベースの検索	コンプライアンス管理者は、ユーザの電子メール アドレスまたはスペース ID を使用してコンテンツを検索および抽出できます。複数のカンマ区切りの電子メール アドレスを入力として提供できます。電子メール アドレスの数のハード リミットは 5 ですが、レポートの集約サイズは 5 GB に制限されます。
e-discovery レポート：キーワードベースの検索	コンプライアンス管理者は、検索時に 1 つ以上のカンマ区切りキーワードを提供できます。これらのキーワードは、電子メール アドレスまたはスペース ID と組み合わせて入力できます。
e-discovery レポート：時間枠	コンプライアンス管理者は、検索を制限する時間枠を指定できます。 **標準オファー：**過去 90 日間に生成された検索データ **Pro Pack：**過去 90 日を超える検索データ
e-discovery レポートのダウンロード	コンプライアンス管理者は過去のレポートのリストを表示し、JSON 形式でダウンロードできます。その後、選択した e-discovery ツールにレポートをエクスポートして、法的調査を行うことができます。レポートは 10 日間利用できます。レポートのサイズは 5 GB に制限されています。
保持	**標準オファー：**無期限の保持、設定不可 **Pro Pack：**管理者は、Webex Teams でデータの保持期間を設定できます。この期間が経過すると、すべてのコンテンツ（ファイル、メッセージ、およびイベント）が削除され、回復不能になります。最小保持期間は 1 ヵ月です。デフォルトの保持期間は無期限です。保持期間は、1 ヵ月単位で最大 120 ヵ月まで設定できます。保持ポリシーは、Webex Teams 内のすべてのスペースに適用されます。
法的保留	**標準オファー**：利用不可 **ProPack**：組織内のコンプライアンス責任者の役割を持つユーザは、組織の保持ポリシーに関係なく、訴訟が合理的に予想される場合に、ユーザに関連付けられた関係するすべての形式の Cisco Webex Teams のコンテンツを保持できます。コンプライアンス責任者は、法的事項を作成したり、管理者（ユーザ）を法的保留にしたり、問題を表示、ダウンロード、およびリリースしたりできます。
DLP：ユーザの登録	Webex Teams アプリケーションには、ユーザを DLP のプロセスに登録できる機能があります。ユーザには、スペースの所有、保持、外部の参加者の有無に関する情報が通知されます。メッセージの伝達は、メッセージの削除、開封確認、スペースのロック、およびモデレータの継承によって制御されます。

機能	説明
Webex イベント API：DLP	Webex プラットフォームは、Webex イベント API を公開します。この API は DLP ソフトウェアと統合することで、ポリシー違反をチェックし、問題を修復するための措置を講じることができます。イベントには、メッセージやファイルの投稿、スペースへのユーザの追加などが含まれます。実行されるアクションとして、ユーザまたは管理者への警告、メッセージの削除などがあります。 **標準オファー：**リアルタイム API の使用。カスタム データ範囲は過去 90 日以内である必要があります。 **Pro Pack：**リアルタイム API の使用。データの保持期間内のカスタム データ範囲が設定され、利用可能になります。
Webex イベント API：アーカイブの統合	Webex イベント API は、Webex Teams データをアーカイブするために、アーカイブ ソフトウェアによって使用できます。 **標準オファー：**リアルタイム API の使用。カスタム データ範囲は過去 90 日以内である必要があります。 **Pro Pack：**リアルタイム API の使用。カスタム データ範囲に制限はありません。
エンタープライズ コンテンツ管理の統合	また、Cisco Webex Teams は、独自のネイティブ ファイル共有とストレージに加えて、IT 管理者が、**Microsoft OneDrive および SharePoint Online** をエンタープライズ コンテンツ管理（ECM）ソリューションとして使用できるようにする柔軟性も備えています。その結果、ユーザは Webex Teams の作業スペース内の最新の OneDrive ファイルおよび SharePoint Online ファイルを共有、編集、取得できます。 **標準オファー：**Microsoft OneDrive と SharePoint Online の統合。ただし、Webex ネイティブ ファイル ストレージを無効にする機能はありません。 **Pro Pack：**Webex Teams のネイティブ ファイル ストレージを無効にする機能がある Microsoft OneDrive と SharePoint Online の統合。

よくある質問（FAQ）

Q. コンプライアンス責任者として、自社が所有していないスペースで自社の従業員が投稿したコンテンツを検索できますか。

A. はい。コンプライアンス責任者は、従業員が所属するすべてのスペースで、組織の従業員によって投稿されたコンテンツを検索できます。

Q. お客様が、Webex Teams がインテグレーションを認定していない CASB またはアーカイブ システムを導入した場合はどうなりますか。

A. その場合は、以下の 2 つの追加オプションがあります。

- イベント API を使用して、Webex Teams と CASB またはアーカイブ システム間の統合を構築します
- Cisco アドバンスド サービスと連携して、イベント API を使用して統合を構築します

Q. イベント API を通じて公開されるイベントのタイプにはどのようなものがありますか。

A. イベント API は次のイベントをキャプチャします。

- メッセージの投稿
- ファイルの投稿
- メッセージまたはファイルの削除
- スペースへのユーザの追加
- スペースからのユーザの削除
- ホワイトボードのスナップショット

Cisco Capital

目標の達成を支援する柔軟な支払いソリューション

Cisco Capital は、お客様が目標の達成、ビジネス変革の実現、競争力の維持に合ったテクノロジーを導入できるよう支援します。総所有コスト（TCO）の削減、資金の節約、成長促進を支援します。100 カ国以上で利用できる Cisco Capital の柔軟な支払いソリューションにより、ハードウェア、ソフトウェア、サービス、補完的なサードパーティ製機器を、お手軽で予測可能な支払い方法で取得することができます。詳細はこちら

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

C78-740772-01JA 19.06