

Cisco Webex Control Hub

(管理と分析)

目次

管理と分析の概要	3
ユーザ管理、アイデンティティ管理、およびアクセス管理	3
デバイス管理とサービス管理	8
コンテンツ管理設定	10
分析	11
Cisco Capital	13

管理と分析の概要

Cisco Webex® Control Hub は、Cisco Webex サービスおよび Webex ハイブリッド サービス（ハイブリッド コール サービス、ハイブリッド カレンダー サービス、ハイブリッド ディレクトリ サービス、ビデオ メッシュ など）のプロビジョニングと管理を直感的な操作で一括で行える、Web ベースの管理ポータルです。

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（セキュリティ、コンプライアンス、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。このサービスへのアクセスは、高度な機能が必要なユーザ（情報セキュリティ プロフェッショナルやコンプライアンス担当者、ビジネス アナリストなど）に対して特別に提供することができます。

Pro Pack は、有償オプションです。従来の Webex サイト管理ツールを利用している場合、Webex Control Hub の分析を利用するためには、管理している Webex サイトと Webex Control Hub をひもづける設定、サイト リンクが必要です。Webex Control Hub でネイティブ管理されているサイトの場合、分析は自動的に利用可能になります。

Webex Control Hub には次の機能があります。

ユーザ管理、アイデンティティ管理、およびアクセス管理

ユーザ管理

アイデンティティとアクセス管理サービスでは、Cisco Webex プラットフォームのセキュリティ保護における柱の 1 つが提供されます。サービスに対するユーザのプロビジョニング、認証、および承認の機能、さらに適切なスペースは、Webex プラットフォームで使用される業界をリードするセキュリティ モデルの基礎となっています。正常に認証され、スペースやミーティングへの参加が承認されたユーザのみに、キー管理サービス (KMS) から一意のキーが付与され、該当するスペースでコンテンツを暗号化または復号できるようになります。

Webex Control Hub を使用すると、ユーザのオンボーディングが簡単になります。顧客とパートナーは、作成、更新、および削除のプロセスでアイデンティティを管理できます。これは、Active Directory 同期ツールを使用してコンマ区切り値 (CSV) をアップロードして手動で行うか¹、業界標準の System for Cross-Domain Identity Management (SCIM) に準拠した API を使用して行います。また、ユーザ変換フローも用意され、すでに無料の Cisco Webex Teams アカウントを持っているユーザを有料の Webex 組織に含めて、顧客による管理対象にすることができます。今日のセキュリティを意識した環境では、必要な時にユーザを削除しアクセスできないようにする機能が不可欠です。これらの各メカニズムを使用して、ユーザまたはデバイスのアクセスを削除できます。

SCIM

System for Cross-Domain
Identity Management

ユーザが追加されたら、Webex Control Hub からすべてのユーザ設定を簡単に管理することができます。Webex プラットフォームでプロビジョニングされた各ユーザのすべてのサービス設定は、Control Hub のユーザの詳細ペインから管理できます。

¹ 組織のオンプレミスの Microsoft Active Directory を Cisco Webex プラットフォームと同期できます。このディレクトリ同期によりユーザが自動的に追加および削除され、複数のディレクトリ データベースを管理する必要がなくなります。

ライセンスの自動指定

ライセンスの自動指定により、Webex Control Hub に追加されたユーザは自身に割り当てられたサービスの使用を自動的に開始できます。管理者は Webex Control Hub の新規ユーザにライセンスを自動的に割り当てるためにライセンス テンプレートを作成することができます。これを行うには、Active Directory 同期ツール、Messenger Sync、手動による追加、People API、SCIM を介したサードパーティ ID プロバイダー、Webex サイト リンク、CSV ファイルのアップロード、サイドボーディング、またはコンシューマから企業組織へのユーザの変換を使用します。オンボーディング レポートを使用してユーザのオンボード履歴と傾向を表示できるため、管理者の利便性が確保されます。

ロールベース アクセス コントロール

Cisco Webex Control Hub ではロール ベースのアクセスが提供されるため、顧客やパートナーに対して異なるレベルの管理者アクセス権を設定できます。表 1 に、現在 Webex Control Hub で使用可能なロールを示します。

表 1. ロールと権限

ロール	権限
ユーザとデバイスの管理者	ユーザ、エンドユーザ デバイス、共有デバイスを管理します。
デバイス管理者	エンド ユーザ デバイス、共有デバイスを管理します。
フルアクセス権を持つ管理者	ユーザ、エンドユーザ デバイス、共有デバイス、ボット、スペース、会社のポリシーとテンプレート、分析とレポート、サポートのメトリックと通知、ライセンス、およびアップグレードを管理します。また、ユーザに管理者ロールを割り当てます。
読み取り専用権限の管理者	ポータルを読み取り専用表示。変更は一切受け付けられません。
ヘルプデスク サポート (パートナーのみ)	ヘルプ デスク サポート ツールにアクセスできます。
コンプライアンス管理者	コンプライアンス担当者は、検索を実行して訴訟をサポートするコンテンツを抽出したり、規制要件に対応したりできます。
営業管理者 (パートナーのみ)	トライアル、顧客およびその組織を管理します (概要やレポートを含む)。
サポート管理者	プラットフォームの可用性とトラブルシューティングのツールにアクセスします。

シングル サインオン

Webex Control Hub では、顧客がシングル サインオン (SSO) を有効にすると、そのユーザは IT 部門が承認したパスワードを入力して Cisco Webex に確実にアクセスできるようになります。Security Assertion Markup Language (SAML) v2 フェデレーションを使用した SSO 統合が、Microsoft Active Directory Federation Services (ADFS) または Azure Active Directory (Azure AD)、Okta、Ping Identity、ForgeRock、またはその他の業界をリードするアイデンティティ プロバイダーでサポートされています。

Cisco Webex プラットフォームにユーザがプロビジョニングされたら、このプラットフォームへの認証は簡単です。管理者レベルでの選択に応じて、ユーザは Webex プラットフォームに保存されているユーザ名とパスワードで認証するか、別の ID プロバイダーで認証して、SAML 2.0 プロトコルを介し、フェデレーション認証を使用してアクセス権を得ることができます。フェデレーテッド SSO では Webex プラットフォームにユーザのパスワードを保存しないため、顧客の利便性とセキュリティが向上します。フェデレーテッド SSO では、管理者の作業時間が減少し、パスワードを忘れてしまったために生じるパスワード リセットやロックアウト イベントに関するヘルプ デスクへの問い合わせ数が削減されるため、企業の総所有コストが削減されます。

Webex では、多要素認証 (MFA) メカニズムをサポートする SAML v2 ID プロバイダーとの統合により、MFA が提供されます。多くの組織では、すべてのサービスまたは認証時に特別な追加要素 (既知のもの (パスワード など) と所有しているもの (x509 証明書など)、HMAC ベースのワンタイム パスワード (HOTP)、時間ベースのワンタイム パスワード (TOTP)、デバイス フィンガープリンティング、または ID プロバイダーがサポートするその他のメカニズム) を必要とするサービスに対して企業全体で MFA メカニズムを導入しているため、この機能は必要不可欠です。



Webex プラットフォームでは、OAuth 2.0 プロトコルを使用して複数のサービスにわたって認可を提供しています。これにより、長時間持続するユーザ セッションを実現し、API にアクセスするときの固有のセキュリティが強化されます。OAuth 2.0 の実装により、デバイスで使用される API のセキュリティが提供され、サードパーティ API、ボット、インテグレーションが統合されます。この必要不可欠なプロトコルにより、Cisco Webex Depot および Cisco Webex の開発者は Webex プラットフォームを拡張することができ、Box、IFTTT、Salesforce、Github、およびその他の多くのボットやインテグレーションなどの追加サービスを使用できます。

表 2 では、企業でユーザ、認証、認可を管理するために使用できる Webex Control Hub の機能を要約しています。

表 2. アイデンティティ管理とアクセス管理の機能とメリット

機能	標準オファー/ Pro Pack が必要	メリット
ユーザ プロビジョニング	標準オファー	複数の方法でユーザを Webex プラットフォームにプロビジョニングできます。ユーザは、手動で入力するか、Webex Control Hub に CSV をアップロードして作成できます。Webex Directory Connector を介してもユーザを作成できます。これは、オンプレミスの Active Directory からユーザを同期します。
SCIM	標準オファー	ユーザのプロビジョニングは、SCIM v1 プロトコルをサポートする多くのエンタープライズ ID プロバイダーからも実行できます。これにより、企業の管理者は短時間でユーザをプロビジョニングでき、さらに重要なことに、ユーザがサービスにアクセスできなくなるようにユーザをデプロビジョニングできます。
Webex Directory Connector と Active Directory (AD) の同期	標準オファー	このソフトウェアを仮想マシンまたはベアメタル Windows マシンで使用して、企業の要件を満たす同期スケジュールに基づいてユーザをプロビジョニングおよびデプロビジョニングします。複数の AD コンテナから選択して Lightweight Directory Access Protocol (LDAP) フィルタを使用し、ユーザの小さなグループを選択してコンセプトの実証を速やかに開始します。次に、組織全体に導入する準備ができたなら拡張します。
AD 同期 Webex Directory Connector を使用したマルチドメインとマルチフォレスト	標準オファー	複数のフォレストまたは複数のドメインにわたってユーザが存在する組織は、Webex AD Connector を使用してユーザをクラウドに同期できます。

機能	標準オファー/ Pro Pack が必要	メリット
ルーム同期	標準オファー	AD に存在しているルームを使用できれば、Webex Board などのデバイスの管理または Webex ルーム デバイスを含むルームでのミーティングのスケジュールリングがはるかに簡単になります。Webex Directory Connector を使用してルームをクラウドに同期します。
プロフィール写真の同期	標準オファー	Webex Directory Connector を使用してプロフィール写真をクラウドに同期します。ユーザは Cisco Webex Teams スペースに招待している人やディレクトリ内で検索している人を確認できます。Webex プラットフォームでは、AD からインポートされたいかなるユーザ属性もエンドユーザが変更することはできません。
Basic 認証	標準オファー	Webex では、ユーザ名（電子メール）とパスワードによる認証がサポートされています。
パスワード ポリシーの施行	標準オファー	デフォルトのパスワード ポリシーでは、ユーザは 1 つの大文字、1 つの数字、1 つの特殊文字の入力が求められます。また、パスワードは 8 文字である必要があります。また、エントロピーのある強力なパスワードの作成に一般的な名前や語句が使用された場合、これらは受け付けられません。
SAML 2.0 フェデレーテッド SSO	標準オファー	Webex では、SAML 2.0 プロトコルを使用したフェデレーテッド SSO がサポートされています。Webex プラットフォームと ID プロバイダーが、これらの中で信頼の輪を作るメタデータを交換した後は、Webex のテナント内のユーザのすべての認証は認証用の ID プロバイダーにリダイレクトされます。これにより、ユーザに対して適切であり、業界のセキュリティ要件を満たす認証方式を自由に定義できるようになります。
多要素認証 (MFA)	標準オファー	Webex では、SAML 2.0 フェデレーテッド SSO による MFA がサポートされます。この機能を要求する場合、通常は 2 つ以上のアプリケーションに対してこれを要求します。したがって、ID プロバイダーを通してこの機能をサポートすることで、複数のアプリケーションにわたって MFA を適用でき、その結果コストが削減されて、セキュリティが強化されます。
認可 (OAuth 2.0)	標準オファー	Webex では OAuth 2.0 がサポートされ、ユーザは認証後に業界標準の OAuth 2.0 トークンを受け取ります。このトークンは、ロール、ライセンス、およびユーザが Webex プラットフォーム上でアクセスするマイクロサービスに対して適切なスコープを持ちます。この機能は、デバイス、ボット、およびインテグレーションが Webex プラットフォームに必要な機能を提供するために適切な API とマイクロサービスにアクセスすることを許可します。
ロールベース アクセス コントロール (RBAC)	標準オファー	Webex Control Hub は RBAC を使用して、管理者が自分のロールで求められる Webex サービス管理を行うための適切な機能セットへのアクセス権を確実に持つようにします。Webex では、フルアクセス権を持つ管理者、ユーザとデバイスの管理者、デバイス管理者、読み取り専用管理者、サポート管理者、およびコンプライアンス担当者の各ロールがサポートされます。

Webex Directory Connector

企業環境でのユーザのプロビジョニングとデプロビジョニングは、特に大規模な組織でのアクセスの管理に不可欠です。このような場合、Webex ディレクトリ コネクタは、ユーザ情報を 1 時間ごと、毎日、または週単位で同期できます。さらに、管理者はディレクトリ プロフィール画像やルーム オブジェクトなどの属性を同期して、デバイスを管理したりミーティングのスケジューリングを効率化したりできます。また、Webex Directory Connector は、Active Directory のマルチ ドメインとマルチフォレストの実装もサポートします。

認証と認可のフロー

図 1 は、SAML ID プロバイダーによる認証と認可によるフェデレーテッド SSO を実現するために Webex Teams を構成した場合の、Webex Teams アプリケーション上のユーザ、Webex Teams サービス、および使用しているアイデンティティ プロバイダー (IdP) 間のフローを示しています。これは、SSO 認証で多く使用される業界標準です。

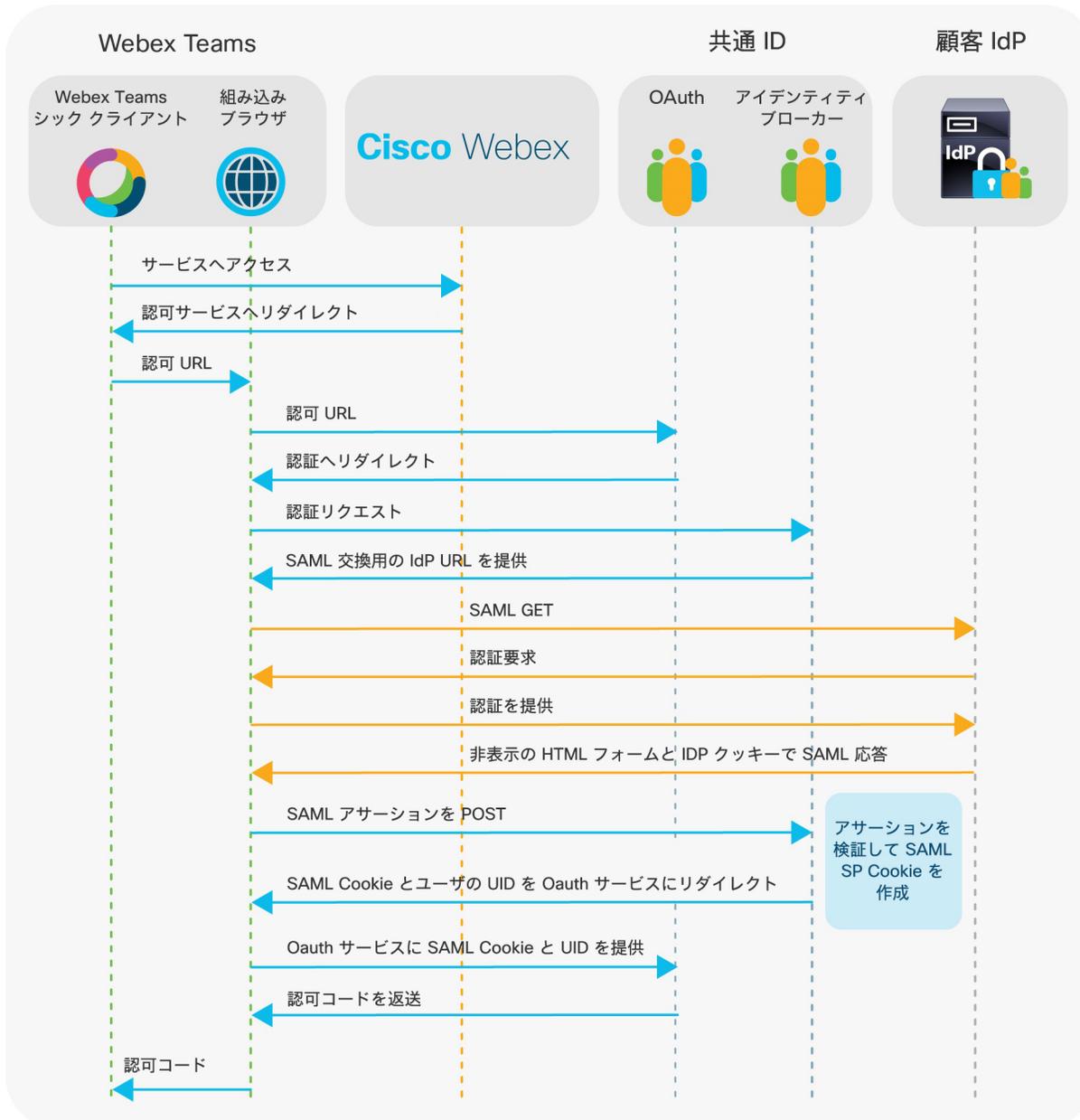


図 1. Cisco Webex Teams プラットフォームを使用した認証と認可のフロー

図 1 に示すように、ユーザは認証および認可が正常に行われると Webex サービスへのアクセス権を取得します。管理者は、従業員のライフサイクルに応じたユースケースを考慮して、Webex サービスの全体的なセキュリティを維持する必要があります。Webex Control Hub、Webex Directory Connector、または SCIM API による手動削除などの機能を使用してユーザを確実にデプロビジョニングして、人事イベント後にアクセス権を取り消すことができます。

Cisco Webex アイデンティティ管理パートナー

シスコは、SAML v2 フェデレーテッド SSO を実現するために、オンプレミスと Identity-as-a-Service 統合の両方の市場で業界をリードする ID プロバイダー各社と協力してきました。

シスコは、以下のパートナー用に、統合ガイドまたは確定した顧客統合を作成しました。

オンプレミスの ID プロバイダー (IdP)

- Microsoft ADFS
- Oracle Access Manager
- Ping Identity
- OpenAM
- IBM Security Access Manager
- CA Siteminder
- F5 - BigIP
- Shibboleth

Identity-as-a-Service ベンダー

- Okta
- PingOne
- Salesforce
- Microsoft Azure
- Oracle Identity Cloud Service
- Centrify
- OneLogin

デバイス管理とサービス管理

デバイス管理

Cisco Webex Control Hub には、Cisco Webex の個人用と共有のデバイスをオンボードおよび有効化するためのシンプルなインターフェイスが用意されています。デバイスのオンボードは、Webex Control Hub で生成された 16 桁のアクティベーション コードまたは QR コードを使用して簡単に行うことができます。デバイスのオンボードが完了したら、管理者はこれらのデバイスの詳細情報と状態を表示して確認することができ、選択した構成設定（設定ロックをオンにして、エンドユーザがタッチパネルを使用してルームのシステム設定を変更することを防ぐ、など）を Webex Control Hub から更新できます。デバイスに注意が必要な問題（ケーブルが外れている、アップグレードが必要など）がある場合、管理者は、それらの問題を Webex Control Hub の該当デバイスの詳細パネルでリスト形式で確認できます。

サービス管理、グローバル設定、および [自社 (My Company)] ページ

Webex Control Hub には、組織がサインアップした Webex サービスを、それがトライアルの状態であるか購入済みであるかに関係なく管理するためのインターフェイスが用意されています。このインターフェイスでは、Cisco Webex ハイブリッド サービスの設定と管理が可能です。たとえば、管理者は、ハイブリッド サービスコネクタを登録し、これらのコネクタ ソフトウェアのアップグレードをスケジュールできます。

表 3 に、Webex Control Hub で管理可能な Webex サービスと、各サービスの高度な管理機能を示します。

表 3. Control Hub で利用可能な Webex サービス

サービス名	管理機能
Cisco Webex Calling	サービスのセットアップ、設定の構成
Cisco Webex Teams	サービスのセットアップ、設定の構成
Cisco Webex Meetings	新規注文の場合、サービスのセットアップと設定の構成。既存のサイトの場合、サイト リンクによる特定の設定の管理
Cisco Webex ハイブリッド コール サービス	コネクタの登録または登録解除、リソースの表示、ソフトウェア アップグレードのスケジュール設定、サービスまたはリソースのエラーの表示、証明書のアップロード、SIP ドメインの確認、サービスの非アクティブ化
Cisco Webex ハイブリッド カレンダー サービス	Google カレンダーまたは Microsoft Exchange のサービスの有効化、コネクタの登録または登録解除、リソースの表示、ソフトウェア アップグレードのスケジュール設定、サービスまたはリソースのエラーの表示、サービスの非アクティブ化
Cisco Webex Video Mesh	ハイブリッド メディア サーバのオンボードまたは削除、リソースの表示、サービスまたはリソースのエラーの表示、オンプレミス ミーティングのビデオ品質の設定、アップグレードのスケジュール設定、サービスの非アクティブ化
Cisco Webex Hybrid Data Security	コンテンツやサービスの暗号化に使用されるキーの管理と保存。キーは、検索インデックス ハッシュの生成に必要です
Cisco Webex Context Service	コネクタの登録または登録解除、リソースの表示、サービスの非アクティブ化
オンプレミス リソース (ハイブリッド サービス)	単一ロケーションからのすべてのリソースの表示、クラスタ レベルの設定 (タイムゾーンの設定やリソース グループの定義など)

サービスの設定は特定の Webex サービスにのみ適用されますが、管理者は組織全体に影響する設定の有効化と管理も可能です。たとえば、管理者はセキュリティとプライバシーの設定、SIP ドメイン、およびブランディングの設定を変更する必要がある場合があります。管理者は、ディレクトリ同期と SSO の設定も管理でき、SSO を有効化または無効化できます。

表 4 に、Webex Control Hub で管理者が編集できるグローバル設定を示します。

表 4. Webex Control Hub で可能なグローバル設定

設定名	管理機能
セキュリティ	ロック画面で保護されているモバイル デバイスの Webex Teams アプリの起動をロックする
ファイル共有制御	Webex Teams アプリとボットの内部ユーザに対してダウンロードとプレビューの制限を設定する

設定名	管理機能
プライバシー	シスコ サポートに読み取り専用モードでのポータルへのアクセスを設定し、デバイスの自動クラッシュ レポートがシスコ サポートにアップロードされるようにする
ドメイン数	SIP ドメインの追加と確認
Webex SIP アドレス	Webex サービスの SIP アドレス サブドメインを設定する
ディレクトリ同期	ディレクトリ同期を有効または無効にする
認証	SSO を有効または無効にする
共有リンクのプレビュー	Webex Teams クライアントでリンク プレビューを表示するかどうかを制御する
E メール	シスコが招待電子メールをエンド ユーザに送信するかどうかを制御する
アニメーションされた GIF を共有する	GIPHY の統合の制御。Webex Teams クライアントで GIF オプションを制御する
サポート	組織のサポート パラメータを設定する

Webex Control Hub では、管理者が組織のサブスクリプションを簡単に管理するためのインターフェイスが用意されています。[会社(My Company)]のページでは、組織の現在のサブスクリプションおよびライセンスへのアクセスが可能です。また、各サブスクリプションの使用状況を表示して確認できます。このページでは、アカウントの詳細(会社名、アカウント番号など)に加え、詳細な注文履歴が表示されます。

コンテンツ管理設定

Cisco Webex Control Hub 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** をコンテンツ管理プラットフォーム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。

ユーザごとのコンテンツ管理：

- IT 管理者は、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
- 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
- IT 管理者が、ユーザのサブセットまたは組織全体に対する ECM 権限付与を有効または無効にできるようにします

ヘルプ デスク

ヘルプ デスク機能により、IT ヘルプ デスク管理者ロールを持つ IT サポート担当者は、組織で有効化されているユーザ、デバイスおよびサービスを検索して、選択した設定を読み取り専用モードで表示できます。この情報を使用して、IT サポート担当者はエンドユーザの問題をトラブルシューティングできます。たとえば、デバイスが Webex プラットフォームに登録されているかどうか、特定のユーザに対してサービスが適切に有効化されているかどうかなどを調査できます。

パートナーは、ヘルプ デスク機能を追加で使用して、顧客のユーザ ベースに Tier 1 サポートを提供できます。検索結果では、関連する詳細情報を一目で確認することができ、顧客の Webex Control Hub を読み取り専用モードで表示する機能も提供されます（顧客がこの機能にオプトインしている場合）。パートナーは、顧客の注文を検索してそのステータスを確認し、顧客からの問い合わせに対応することができます。注文検索ツールを使用するには、ユーザに注文管理者ロールが割り当てられている必要があります。

パートナー ポータル（顧客トライアルと顧客管理用）

Cisco Webex サービスのトライアルでは、パートナーは Webex Control Hub を介して潜在顧客に対し 30 日、60 日、および 90 日の無償トライアルを作成して、簡単に Webex のビジネス価値を実際に示すことができます。トライアルでは、Webex で提供されるサービスのコラボレーション スイートをすべて使用できます。これには、Webex Meetings、Messaging、および Calling（公衆電話交換網（PSTN）サービスを含む）が含まれます。

パートナーは、Webex Control Hub で課金中の顧客と顧客トライアルを表示して管理できます。パートナーの管理者は、顧客リストを使用して顧客のサービスとアカウントのステータス、および顧客が購入したライセンス数を簡単に確認できます。パートナーの管理者は、[顧客のセットアップ（Set Up Customer）] ボタンを使用して顧客の設定を管理できるほか、トライアル期間の変更やサービスの追加など、トライアルの条件を編集できます。

監査管理者のアクティビティ

管理者のアクティビティ ログは、問い合わせへの対応やアーカイブのために提供されます。管理者による操作のログは、コンプライアンスの要件として多くの組織、業界で必要とされています。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のアクティビティのログを使用して、管理者によって実行された重要な操作（ORG 設定の変更など）を表示できます。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操作を検索したり、特定の操作または特定の管理者を検索して検索結果を絞り込んだりできます。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。

分析

Cisco Webex Control Hub の分析では、使用状況の傾向および価値のある洞察が提供されます。これを戦略の参考にして、チーム間の導入を促進および最適化できます。高度な分析機能が、Webex Control Hub の一部として統合されています。顧客は、組織全体で各種サービスがどのように使用されているかを理解することができ、サービスの導入を拡大させて生産性を最大限に向上させることができます。管理者は容量とパフォーマンスをモニタリングことができ、プロアクティブな管理の一環としてリソース使用率を最適化できます。管理者または IT ヘルプデスク スタッフは、診断の実行や、問題解決までの時間短縮が可能です。

直感的なグラフィカル インターフェイスにより、管理者は使用状況、導入状況、およびその他の重要な情報にアクセスできます。データがインタラクティブに可視化され、指定したパラメータにリアルタイムで自動的に順応するため、データを詳しく調査することができます。

標準で、過去 90 日間の履歴データにアクセスできます。データは集約され、複数のレポートで表示されます。管理者は、Webex Control Hub 内でこれらのレポートにいつでもアクセスできます。

Pro Pack for Webex Control Hub は、最大 1 年分のデータをサポートします。さらに、会議ごと、参加者ごとのより詳細な情報を提供します。これは、詳細なデータをエクスポートする機能と同様に、より深いデータの探索および洞察に利用できます。

表 5 に、Webex の分析機能を要約します。

表 5. Webex Teams の分析機能

機能	標準オファア/ Pro Pack が必要	説明
柔軟な履歴レポート	標準オファア	Webex Meetings、Webex Teams、ハイブリッド メディア サービス、およびデバイスについて、最大 90 日間の日次集約メトリックが要約レポートで視覚化されます。エンゲージメントと品質のレポートを取得できます。
ドリルダウン	Pro Pack が必要	個別のセッションおよびユーザレベルのメトリックを取得できます。月次レポートから個別のミーティングレコードにズームインできます。
1 年分のデータ	Pro Pack が必要	最大 365 日間の履歴データにアクセスできます。
マルチディメンションピボットとデータ探索	標準オファア	拡張された分析エンジンにより、ユーザはレポートのインターフェイスを介して、リアルタイムでデータを操作することができます。任意のデータセットを選択すると、関連するすべてのレポートが更新されます。
ミーティングのトラブルシューティング	標準オファア	過去 30 日間の Webex ミーティングの詳細をリアルタイム検索します。ホストの電子メールまたはミーティング ID を検索して、ミーティングおよび参加者の詳細を特定します。

柔軟な履歴レポート

履歴レポートは Webex Control Hub の標準機能です。レポートは、日次、週次、および月次の形式で取得できます。最大 90 日間の日次集約メトリックには、フルアクセス権を持つ管理者または読み取り専用アクセス権を持つユーザがアクセスできます。管理者は、Webex Teams、Webex Meetings、Webex Video Mesh、および Webex デバイス（それぞれ展開された構成で該当する場合）のさまざまな種類のレポートを表示できます。

- Webex Meetings レポートには、ミーティングや音声の使用状況、ミーティングの平均参加時間、およびメディア品質が含まれます。
- Webex Teams レポートには、スペース使用率、アクティブ ユーザ、および共有ファイルが含まれます。
- Webex Video Mesh レポートには、通話総数、リソース使用率、およびクラスタ ステータスが含まれます。
- Webex デバイスの使用率レポートには、使用状況、使用頻度が最も多いデバイスと最も少ないデバイスが含まれます。

過去の傾向を使用して繰り返し発生する異常を識別します。エンゲージメント、品質、および診断の各データは、簡単に取得できます。システムの概要を一目で把握できるように、上位のメトリックを簡単に識別できます。傾向分析と可視化により、重要なパターンが明確になります。

ドリルダウン

Pro Pack for Webex Control Hub を使用すると、Webex ミーティング セッションやユーザ レベルの詳細情報を取得できます。管理者は、月次のミーティング使用状況の合計から個別の通話の詳細情報までワンクリックでドリルダウンできます。この機能では、管理者は不要なデータを除外することができ、最も意味がある情報に注目できます。

データ探索

高度な分析データ アーキテクチャにより、内部データモデル内にデータが取り込まれ、リアルタイムで瞬時にデータを探索できます。データ セットを操作または選択することで、関連するすべてのレポートが自動的に更新されます。マルチディメンション ピボットにより情報の視覚化方法が変わり、リアルタイムで多種多様な方法でデータを操作できます。

ミーティングのトラブルシューティング

Webex Control Hub では、Webex ミーティングのトラブルシューティング機能も提供されます。技術スタッフは、迅速にサポート要求を解決することができ、リクエストの発生時にリアルタイムでのミーティングを検索できます。ホストの電子メール アドレス、会議 ID、およびミーティング ID は有効な検索条件です。会議を検索し、30 日前までに診断できます。ミーティングが特定されたら、開始時刻、継続時間、ミーティング名、参加者数、およびステータスが報告されます。

通話全体を通じて、IT 管理者はミーティング参加時間 (JMT) や通話中の音声およびビデオ品質を含む、参加者ごとのサービス品質を確認できます。

API

Webex 環境を管理するために Cisco Webex Control Hub 以外の独自のツールを使用する必要がある管理対象 サービス プロバイダーと企業は、Cisco Webex for Developers APIs を使用して独自のツールに Webex 管理機能を統合することができます。たとえば、Webex People API および Licenses API を介して、ユーザやユーザ ライセンスの機能を使用できます。

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に支援します。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](#)

©2019 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。

本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(1502R)

この資料の記載内容は2019年6月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



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>

お問い合わせ先