ポリシー エディタ（Policy Editor）

- 概要，1 ページ
- ポリシー エディタ（Policy Editor），2 ページ
- 暗号化レベル，12 ページ

概要

Cisco WebEx には、グループのポリシーを定義して適用できるポリシー エディタがあります。ポリシーは、ファイル転送、デスクトップ共有、IM セッションのアーカイブ、Cisco WebEx の自動アップグレードなどの機能を有効化または無効化するために使用できます。ポリシーは、Cisco WebEx 組織内の全ユーザまたは特定のユーザ グループに適用できます。

個人にポリシーを適用することはできません。

ポリシーおよびポリシー アクション

ポリシーは、ユーザのグループまたは Cisco WebEx 組織全体が使用可能な Cisco WebEx 機能を決定するアクションを含む一連のルールです。そのため、ポリシーには、有効、無効、または詳細設定で使用可能な複数のアクションを含めることができます。たとえば、新規従業員に対して Cisco WebEx の特定の機能を制限したいお客様は、新規従業員ポリシーという名前のポリシーを作成して、さまざまなアクションを関連付けることができます。

アクションは、ポリシーによって制限可能な Cisco WebEx の機能です。たとえば、外部ファイル転送アクションは、Cisco WebEx 組織の外部のユーザとのファイル交換機能に対応しています。

ポリシーの定義と適用

組織レベルのポリシーとグループレベルのポリシーの違いを理解することが重要です。

Cisco WebEx 組織に新規ユーザを作成した場合、そのユーザはデフォルトではいずれのグループにも属していません。そのため、すべてのデフォルトのポリシー アクションが Cisco WebEx 組織

全体に適用されます。これは、通常プロビジョニング時に作成される最上位グループには、Cisco WebEx 組織のすべてのユーザが含まれるためです。

組織管理者がグループを作成し、それらのグループに特定のポリシーを適用する場合、グループレベルのポリシーによって組織レベルのポリシーがオーバーライドされます。それらのグループに属しているユーザは、組織レベルのポリシーではなくグループレベルのポリシーによって支配されます。たとえば、組織管理者が特定のグループに対して外部VoIP通信を禁止するポリシーを適用すると、そのグループのユーザはVoIPを使用して通信できなくなります。ただし、組織内の他のすべてのユーザに対しては、外部 VoIP 通信が引き続き有効な場合があります。

ポリシーは、組織レベルで、または特定のグループに対して適用できます。ただし、組織レベルとグループレベル（または親グループとそのサブグループ）の間でポリシーの設定に競合がある場合、最も限定的なアクションが有効になります。たとえば、組織レベルでVoIP機能がオン（[有効（Enabled）]）になっていて、グループレベルでオフ（[無効（Disabled）]）になっている場合、そのグループ内のすべてのユーザの VoIP 機能が無効になります。ただし、組織レベルで VoIP 機能がオフになっている場合、グループレベルで有効にしても、そのグループのユーザのVoIP機能は無効なままです。

ポリシー エディタ（Policy Editor）

ポリシーを設定するには、Cisco WebEx管理ツールを使用します。グループごとに異なるポリシーを設定でき、ポリシーはいつでも変更できます。Cisco WebEx 組織が新しくプロビジョニングされると、デフォルトですべてのユーザに対してすべての機能が有効になります。ただし、ユーザが AES 暗号化を使用しなければならない機能は除きます。

（注） ポリシーを変更または更新した場合、更新されたポリシーを適用するには、Cisco WebEx からログアウトしてから再度ログインする必要があります。

グループにポリシーを適用する方法については、グループへのポリシーの割り当てを参照してください。

ポリシーの追加

手順

ステップ 1 [ポリシー エディタ（Policy Editor）]タブを選択します。
[ポリシー（Policy）]画面の左側に [ポリシー リスト（Policy List）]、右側に [アクション リスト（Action List）] が表示されます。

ステップ 2 [ポリシー リスト（Policy List）]で [追加（Add）] を選択します。
既存のポリシーのリストの最上部に新しいポリシーが表示されます。

ステップ 3 ポリシーの一意の名前を入力します。

次の作業

このポリシーにアクションを追加するには、次を参照してください。 ポリシーへのアクションの追加, （3 ページ）

ポリシーへのアクションの追加

手順

ステップ 1 [ポリシー エディタ（Policy Editor）]タブを選択します。
[ポリシー エディタ（Policy Editor）]画面の左側に [ポリシー リスト（Policy List）]、右側に [アクション リスト（Action List）] が表示されます。

ステップ 2 [ポリシー名（Policy Name）]で、アクションを追加するポリシーを選択します。

ステップ 3 アクションを追加するには、画面の右側の [アクション リスト（Action List）]の下にある [追加（Add）] を選択します。
[アクション エディタ（Action Editor）]画面が表示されます。

ステップ 4 [アクション タグ名（Action Tag Name）]リストからポリシー アクションを選択します。
これらのアクションの詳細については、次を参照してください。 ポリシーおよびポリシー アクション, （1 ページ）

ステップ 5 [保存（Save）]を選択します。

ステップ 6 すべてのポリシーにアクションが割り当てられるまで、ステップ 3 ～ 5 を繰り返します。

Cisco WebEx で使用可能なポリシー アクション

ここでは、Cisco WebEx で使用可能なポリシー アクションについて説明します。説明には、ポリシー アクションを制御する機能への影響に関する情報も含まれています。このため、管理するグループに対して最適なポリシーを設定することができます。ポリシー アクションの確認および設定方法の詳細については、ポリシーへのアクションの追加, （3 ページ）を参照してください。

デフォルトでは、新規にプロビジョニングされた Cisco WebEx の組織に対し、ユーザに付与されたすべての機能が備えられています。これは、デフォルトのポリシー アクションでは、すべてのユーザが Cisco WebEx の全機能を使用できることを意味します。

（注） デフォルトでは、エンドツーエンドの暗号化ポリシーのみ有効になっていません。組織管理者はこのポリシーを明示的に有効にする必要があります。その後、管理者は、すべてのユーザまたは特定のユーザ グループに対して特定の機能を無効にする場合のみ、ポリシーを作成する必要があります。

ポリシー アクションは、サードパーティ製の XMPP IM アプリケーションを使用しているユーザには適用できません。

VoIP 会議の参加者が 10 人未満の場合、同じ VoIP 会議に同時に接続できます。

外部ユーザとは、Cisco WebEx 組織に属していないユーザですが、外部ユーザも Cisco WebEx を使用して、Cisco WebEx 組織に属しているユーザと通信することができます。

ポリシー アクション	説明	影響	デフォルト値
外部ファイル転送（External File Transfer）	組織のユーザと組織外のユーザ間の IM セッションでのファイル転送を制御します。	このポリシー アクションを [無効（Disabled）]に設定すると、少なくとも 1 人の外部ユーザがいるマルチパーティ IM セッションを含む、組織内ユーザと外部ユーザ間のすべてのファイル転送が停止します。	[有効（Enabled）]
内部ファイル転送（Internal File Transfer）	組織内のユーザ間の IM セッションでのファイル転送を制御します。	このポリシー アクションを [無効（Disabled）]に設定すると、すべての内部ファイル転送が停止します。 このポリシー アクションが明示的に [無効（Disabled）]に設定されていない場合、組織内のすべてのユーザが内部ユーザとファイル交換することができます。	[有効（Enabled）]
外部 IM（External IM）	組織内のユーザと組織外のユーザ間の IM セッションを制御します。	このポリシー アクションを [無効（Disabled）]に設定すると、組織内のユーザと組織外のユーザ間のすべての IM セッションが停止します。この場合、音声、ビデオ、VoIP などの依存関係にあるサービスもすべて停止します。	[有効（Enabled）]
外部 VoIP（External VOIP）	組織内のユーザと組織外のユーザ間の IM セッションでの VoIP 通信を制御します。	このポリシー アクションを [無効（Disabled）]に設定すると、組織内のユーザと組織外のユーザ間の IM セッションでのすべての VoIP 通信が停止します。ただし、テキストベースの IM セッションやファイル転送などの他のサービスは使用できます。	[有効（Enabled）]

ポリシー アクション	説明	影響	デフォルト値
内部 VoIP（Internal VOIP）	組織内のユーザ間の IM セッションでの VoIP 通信を制御します。	このポリシー アクションを [無効（Disabled）]に設定すると、組織内のユーザ間の IM セッションでのすべての VoIP 通信が停止します。ただし、テキストベースの IM セッションやファイル転送などの他のサービスは使用できます。 このポリシー アクションが明示的に [無効（Disabled）]に設定されていない場合、組織内のすべてのユーザが IM セッションで VoIP 通信を行うことができます。	[有効（Enabled）]
外部ビデオ（External Video）	組織内のユーザと組織外のユーザ間の IM セッションでのビデオサービスを制御します。	このポリシー アクションを [無効（Disabled）]に設定すると、組織内のユーザと組織外のユーザ間のIMセッションでのすべてのビデオサービスが停止します。ただし、テキストベースのIMセッションやファイル転送などの他のサービスは使用できます。	[有効（Enabled）]
内部ビデオ（Internal Video）	組織内のユーザ間の IM セッションでのビデオサービスを制御します。	このポリシー アクションを [無効（Disabled）]に設定すると、組織内のユーザ間の IM セッションでのすべてのビデオサービスが停止します。ただし、テキストベースの IM セッションやファイル転送などの他のサービスは使用できます。 このポリシー アクションが明示的に [無効（Disabled）]に設定されていない場合、組織内のすべてのユーザが IM セッションでビデオコミュニケーションを行うことができます。	[有効（Enabled）]

ポリシー アクション	説明	影響	デフォルト値
ローカル アーカイブ（Local Archive）	ユーザがローカルで IM テキストメッセージをアーカイブする機能を制御します。	バージョン7.1のアプリケーション以降、このポリシーを [無効（Disabled）]に設定すると、保存されていたローカル履歴は削除されます。 Cisco WebEx アプリケーションでは、次のオプションは無効になっています。[編集（Edit）] > [設定（Settings）] > [一般 GM（General IM）] > [メッセージ アーカイブ（Message Archive）]。 Cisco WebEx バージョン 5.x から 6.x にアップグレードすると、ユーザのローカルコンピュータに保存されていたチャット履歴のアーカイブは削除され、回復することはできません。組織管理者はCisco WebEx組織のすべてのユーザにこの点を連絡することを推奨します。さらに、ユーザは、Cisco WebExが新しいバージョンにアップグレードされる前に、個人のチャットアーカイブをバックアップする必要があります。 7.1 以降、このポリシーが [無効（Disabled）]に設定されている場合、ローカル履歴は削除されます。	[有効（Enabled）]
ワークスペースへの参加（Join Workspace）			[有効（Enabled）]
外部ワークスペースへの参加（Join External Workspace）			[有効（Enabled）]

ポリシー アクション	説明	影響	デフォルト値
外部デスクトップ共有（External Desktop Share）	組織内のユーザが自身のデスクトップを組織外のユーザと共有する機能を制御します。	このポリシー アクションを [無効（Disabled）]に設定すると、組織内のユーザは自身の（ローカル）デスクトップを組織外のユーザと共有できなくなります。 このポリシー アクションが明示的に [無効（Disabled）]に設定されていない場合、ユーザは自身の（ローカル）デスクトップを組織外のユーザと共有できます。	[有効（Enabled）]
内部デスクトップ共有（Internal Desktop share）	組織内のユーザが自身のデスクトップを組織内の他のユーザと共有する機能を制御します。	このポリシー アクションをオフにすると、組織内のユーザは自身のデスクトップを組織内の他のユーザと共有できなくなります。 このポリシー アクションが明示的に [無効（Disabled）]に設定されていない場合、ユーザは自身のデスクトップを組織内の他のユーザと共有できます。	[有効（Enabled）]
ワークスペース機能（Workspace Feature）			[有効（Enabled）]
ユーザをワークスペースに招待する（Invite Users to Workspace）			[有効（Enabled）]

ポリシー アクション	説明	影響	デフォルト値
ユーザを外部ワークスペースに招待する（Invite Users External Workspace）			[有効（Enabled）]
IM のエンドツーエンドの暗号化のサポート（Support End-to-End Encryption For IM）	ユーザが IM セッションのエンドツーエンドの暗号化のサポートを指定できます。	このアクション ポリシーを [有効（Enabled）]に設定すると、IM セッションのエンドツーエンドの暗号化をサポートできます。 ユーザがログに記録されるように指定されている場合、エンドツーエンドの暗号化ポリシーの設定はオーバーライドされて False になります。エンドツーエンドの暗号化は、ログに記録されたユーザに対してはサポートされません。詳細については、IM ログ記録とアーカイブの概要を参照してください。	無効
符号化されていない IM のサポート（Support NO Encoding For IM）	エンドツーエンドの暗号化に対応しているアプリケーションが、エンドツーエンドの暗号化に対応していないアプリケーションやエンドツーエンドの暗号化をサポートしていないサードパーティ製アプリケーションとの IM セッションを開始できるかどうかを制御します。	このポリシーを [無効（Disabled）]に設定すると、エンドツーエンドの暗号化に対応しているアプリケーションが、エンドツーエンドの暗号化に対応していないアプリケーションやエンドツーエンドの暗号化をサポートしていないサードパーティ製アプリケーションとの IM セッションを開始できなくなります。 （注） [IM のエンドツーエンドの暗号化のサポート（Support End-to-End Encryption For IM）] を [有効（Enabled）]に設定すると、ネゴシエートされる暗号化レベルは、相手側がサポートする最高のレベルになります。暗号化レベルの詳細については、暗号化レベル，（12 ページ）を参照してください。	[有効（Enabled）]

ポリシー アクション	説明	影響	デフォルト値
内部 IM（ホワイト リストに記載されたドメインを含む）（Internal IM（including White Listed domains））	組織内のユーザとホワイトリスト上の特定ドメイン間の IM 通信を制御します。	このポリシー アクションを [無効（Disabled）]に設定すると、組織内のユーザはホワイトリストに指定されたドメイン内の IM ユーザになれなくなります。ただし、ドメイン内のユーザは互いに IM を続けることができます。このポリシー アクションを [無効（Disabled）] に設定すると、VoIP、ビデオ、ファイル転送などの依存関係にある他のサービスも無効になります。	[有効（Enabled）]
アップロード ウィジェット（Upload Widgets）			[有効（Enabled）]
ユーザによるプロファイルの編集を許可（Allow user to edit profile）	ユーザの自身のプロファイル情報の編集機能を制御します。	このポリシー アクションを [無効（Disabled）]に設定すると、ユーザは自身のプロファイル情報を編集できなくなります。 このポリシー アクションは、[設定（Configuration）]タブの下にある [プロファイルの設定（Profile Settings）] 画面の設定に影響します。	[有効（Enabled）]

ポリシー アクション	説明	影響	デフォルト値
ユーザによる表示プロファイル設定の編集を許可（Allow user to edit the view profile setting）	ユーザのグループが、ユーザプロファイルの表示設定の変更を制限できる機能を制御します。	このポリシー アクションを [無効（Disabled）]に設定すると、ユーザはユーザプロファイルの表示設定の変更できなくなります。 このポリシー アクションは、[設定（Configuration）]タブの下にある [プロファイルの設定（Profile Settings）] 画面の [ユーザによるプロファイル表示設定の変更を許可（Allow users to change their profile view settings）] チェックボックスに影響します。 このポリシー アクションを [無効（Disabled）]に設定すると、[ユーザによるプロファイル表示設定の変更を許可（Allow users to change their profile view settings）] チェックボックスは、選択している場合でも無意味になります。	[有効（Enabled）]
内部スクリーンキャプチャ（Internal Screen Capture）	組織内のユーザのスクリーンキャプチャ送信機能を制御します。	このポリシー アクションを [無効（Disabled）]に設定すると、組織内のユーザが組織内でスクリーンキャプチャを送信できなくなります。	[有効（Enabled）]
外部スクリーンキャプチャ（External Screen Capture）	ユーザが組織外のユーザにスクリーンキャプチャを送信する機能を制御します。	このポリシー アクションを [無効（Disabled）]に設定すると、組織内のユーザが組織外でスクリーンキャプチャを送信できなくなります。	[有効（Enabled）]

ポリシー アクション	説明	影響	デフォルト値
内部ブロードキャストメッセージの送信（Send Internal Broadcast Message）	ユーザが組織内のユーザにブロードキャストメッセージを送信する機能を制御します。	このポリシー アクションを [無効（Disabled）]に設定すると、組織内のユーザが組織内でブロードキャストメッセージを送信できなくなります。	[有効（Enabled）]
外部ブロードキャストメッセージの送信（Send External Broadcast Message）	ユーザが組織外のユーザにブロードキャストメッセージを送信する機能を制御します。	このポリシー アクションを [無効（Disabled）]に設定すると、組織内のユーザが組織外でブロードキャストメッセージを送信できなくなります。	[有効（Enabled）]
ユーザによるディレクトリ グループへのブロードキャストの送信を許可（Allow user to send broadcast to a directory group）	ユーザが組織内のディレクトリ グループにブロードキャストメッセージを送信する機能を制御します。	このポリシー アクションを [無効（Disabled）]に設定すると、組織内のユーザが組織内のディレクトリ グループにブロードキャストメッセージを送信できなくなります。	[有効（Enabled）]

ポリシー アクション	説明	影響	デフォルト値
HD ビデオ（HD Video）	外部ビデオポリシーまたは内部ビデオポリシーが有効になっている場合に、コンピュータ コールに対するコンピュータ上の HD ビデオ機能を制御します。	このポリシー アクションを [無効（Disabled）]に設定すると、コンピュータ コールに対するすべてのコンピュータの HD ビデオが停止します。	[有効（Enabled）]

すべてのユーザに対して以下のポリシー アクションを無効にする組織管理者は、各値を False に設定する必要があります。

- 内部 VoIP（Internal VoIP）
- 外部 VoIP（External VoIP）
- 内部ビデオ（Internal Video）
- 外部ビデオ（External Video）
- 内部ファイル転送（Internal File Transfer）
- 外部ファイル転送（External File Transfer）
- 内部デスクトップ共有（Internal Desktop Share）
- 外部デスクトップ共有（External Desktop Share）

暗号化レベル

通常、Cisco WebEx アプリケーション間で行われるすべての IM 通信は、Cisco WebEx 組織内および組織外の両方で暗号化されます。IM 通信は発信元の Cisco WebEx アプリケーションで暗号化され、宛先のアプリケーションで復号化されます。この暗号化は、テキスト、デスクトップ（およびアプリケーション）共有、ファイル転送、VoIP、およびビデオを含むすべての IM 通信の形態に適用されます。

Cisco WebEx には 3 つのレベルの暗号化が用意されています。

- **256 ビット Advanced Encryption Standard（AES）/エンドツーエンドの暗号化**：追加のセキュリティ層を提供します。データはアプリケーションで AES を使用して暗号化され、その宛先でのみ復号化されます。
- **128 ビット セキュア ソケット レイヤ（SSL）**：アプリケーションとデータセンターの SSL ターミネーション ポイント間の接続が暗号化されます。Cisco WebEx バージョン 6 以降では、Cisco WebEx アプリケーションは常に SSL（セキュア ソケット レイヤ）を使用して Cisco WebEx データセンターに接続します。

- **暗号化なし**：データは暗号化されませんが、接続は SSL で行われることがあります（Cisco WebEx バージョン 5.x の場合）。Cisco WebEx バージョン 6 以降では、常に SSL で接続します。

  暗号化のレベルは、組織管理者が設定しているポリシーによって異なります。組織管理者は、Cisco WebEx 組織全体または特定のグループに対して暗号化ポリシーを適用できます。

  Cisco WebEx アプリケーションは、そのアプリケーションにログインしているユーザに適用可能なポリシーから自動的に暗号化レベルを判断します。したがって、Cisco WebEx 組織のポリシー設定により特定の暗号化レベルが許可されない場合、IMセッションは許可されず、適切なエラー メッセージがその IM セッション内のすべてのアプリケーションに表示されます。

  （注） グループ IM のシナリオでは、最初の招待の送信時にすべてのユーザ間で暗号化レベルがネゴシエートされます。IM セッションが確立されると、後続の出席者は、参加するためにはネゴシエートされた暗号化レベルをサポートしている必要があります。

  次の例は、IM セッションの一般的な暗号化ポリシーを示しています。

  エンドツーエンドの暗号化の導入を選択する組織は、次のポリシー オプションから選択できます。

- エンドツーエンドの暗号化のみ許可。IMのログを記録する必要があるユーザがいる場合、エンドツーエンドの暗号化を排他的に設定しないでください。これは、IM ログ記録がエンドツーエンドの暗号化より優先されるためです。
- エンドツーエンドの暗号化と SSL 暗号化の両方を許可。このオプションは、Cisco WebEx バージョン 5.x を使用している場合に適用されます。
- エンドツーエンドの暗号化、SSL 暗号化を許可、および暗号化なし。

  アクション エディタで、選択したポリシー オプションに基づき各暗号化レベルを [有効（Enabled）]または [無効（Disabled）] に設定する必要があります。

次の表に、これらのポリシー オプションの影響を示します。

アプリケーション A のポリシー	**アプリケーション B の暗号化レベル**		
	エンドツーエンド暗号化	**SSL**	**SSL**
エンドツーエンドの暗号化のみ	エンドツーエンド暗号化	許可しないでください	許可しないでください

アプリケーション**A**のポリシー	アプリケーション**B**の暗号化レベル		
エンドツーエンドの暗号化または SSL	エンドツーエンド暗号化	SSL	許可しないでください
エンドツーエンドの暗号化、SSL、または暗号化なし	エンドツーエンド暗号化	SSL	暗号化なし

アクションエディタで、選択したポリシーオプションに基づき各暗号化レベルを [有効（Enabled）] または [無効（Disabled）] に設定する必要があります。