CHAPTER 11

Cisco Unified MeetingPlace Express に対するセキュリティ機能の設定

改訂：2006 年 10 月 18 日、OL-12185-01-J

この章では、システムのセキュリティを強化する方法を説明します。

この項の内容は、次のとおりです。

この章の内容は、次の場合に適用されます。

- Cisco Unified MeetingPlace Express システムを所有している場合。
- Cisco Unified MeetingPlace Express VT システムを所有している場合。

システムのセキュリティに関する推奨事項

企業によっては、コンピュータ システムへのアクセス制限に関するガイドラインがすでに定められていることもありますが、表 11-1 に示すタスクも実行することをお勧めします。

表 11-1　Cisco Unified MeetingPlace Express のセキュリティに関する推奨事項

セキュリティに関する推奨事項	説明
サーバの物理的な設置場所の安全を確保します。権限のない者がシステムにアクセスできないようにするために、鍵またはカード キー システムで保護されたエリアにサーバを置きます。	—
データベースを最新の状態に維持します。退職した従業員のユーザ プロファイルを、非アクティブ化または削除します。	ユーザ プロファイルのアクティブ、非アクティブ、およびロック状態について（P. 8-24）
事前設定されている管理者プロファイルのデフォルト パスワードを変更します。	管理者プロファイルのパスワードの変更（P. 1-3）
ユーザ構成に応じて、該当するセキュリティ関連のタスクをすべて実行します。	システムの安全を確保する方法（P. 11-3）

関連項目

- 電話ハッカー侵入阻止のオプションについて（P. 11-2）

電話ハッカー侵入阻止のオプションについて

Cisco Unified MeetingPlace Express では、次の作業を行うことで、電話ハッカー侵入を監視し、防止できます。

- 特定のユーザだけにダイヤルアウト特権を持たせるために、次のタスクを実行します。
  - ゲスト ユーザのダイヤルアウト特権の制限（P. 11-8）
  - プロファイル ユーザのダイヤルアウト特権の制限（P. 11-9）
- ダイヤルアウトの利用状況を監視するために、次のタスクを実行します。
  - ポートの使用状況についてのレポートの実行（P. 10-13）
  - 発信コールについての情報のエクスポート（P. 10-16）
  - 会議についての情報のエクスポート（P. 10-8）

関連項目

- システムのセキュリティに関する推奨事項（P. 11-2）

システムの安全を確保する方法

この項では、システムのセキュリティを強化するのに役立つタスクを示します。この項の内容は、次のとおりです。

ユーザ パスワード要件の設定

Cisco Unified MeetingPlace Express システムのセキュリティを強化するには、次の操作を実行します。

- 長いユーザ パスワードを設定する。
- ユーザ パスワードを変更する頻度を増やす。

手順

ステップ 1　Cisco Unified MeetingPlace Express にログインします。

ステップ 2　ページの上部にある［管理］をクリックします。

ステップ 3　ページの左側で次の操作を実行します。

a. [System Configuration] をクリックします。

b. [Usage Configuration] をクリックします。

ステップ 4　[Usage Configuration] ページで、次のフィールドを設定します。

- Minimum profile password length（P. C-160）：値が大きいほど、セキュリティが強化されます。
- Change profile password (days)（P. C-160）：値が小さいほど、セキュリティが強化されます。
- Minimum user password length（P. C-160）：値が大きいほど、セキュリティが強化されます。
- Change user password (days)（P. C-160）：値が小さいほど、セキュリティが強化されます。

ステップ 5　[Save] をクリックします。

ヒント

長いパスワードと、頻繁なパスワード変更を義務づけると、ユーザがフラストレーションを感じる可能性があります。パスワードに関する要件は、社内ですでに使用されている要件に合わせるようにしてください。

関連項目

- システムのセキュリティに関する推奨事項（P. 11-2）
- 概要：使用状況の設定（P. C-159）

ユーザ ログイン失敗回数の制限

この項では、1 回のセッションで Cisco Unified MeetingPlace Express へのログインを何回試行できるかを設定する方法を説明します。この回数に達するとユーザ プロファイルは「ロック」され、ログインできなくなります。

始める前に

- 事前設定されている管理者プロファイルはロックされません。
- 最大ログイン試行回数に達する前にユーザが次のいずれかを実行すると、ログイン失敗回数のカウンタがリセットされます。
  - ブラウザを閉じてから新たに開き、ログイン試行を続行する。
  - Cisco Unified MeetingPlace Express へのコールを終了して、新しいコールを開始し、ログイン試行を続行する。
- Cisco Unified MeetingPlace Express と Cisco Unified CallManager リリース 4.x との統合のために SIP トランクを使用する場合は、アテンダントへのコールはサポートされません。

手順

ステップ 1　Cisco Unified MeetingPlace Express にログインします。

ステップ 2　ページの上部にある［管理］をクリックします。

ステップ 3　ページの左側で次の操作を実行します。

a. [System Configuration] をクリックします。

b. [Usage Configuration] をクリックします。

ステップ 4　[Usage Configuration] ページで、次のフィールドを設定します。

- Maximum profile login attempts（P. C-161）：値が小さいほど、セキュリティが強化されます。

ステップ 5　[Save] をクリックします。

関連項目

- SIP 環境での統合の Cisco Unified CallManager の制約事項（P. 7-41）
- システムのセキュリティに関する推奨事項（P. 11-2）
- ユーザ プロファイルのアクティブ、非アクティブ、およびロック状態について（P. 8-24）
- 概要：使用状況の設定（P. C-159）
- 管理者プロファイルについて（P. 8-21）

会議パスワードに関する要件の設定

Cisco Unified MeetingPlace Express システムのセキュリティを強化するには、次のことを行います。

- 特定のユーザまたはすべてのユーザに対して、そのユーザがスケジュールする会議のパスワードを必須にする。
- 長い会議パスワードを設定する。

会議パスワードを設定すると、招待されていない人は会議に参加できなくなります。

手順

ステップ 1　Cisco Unified MeetingPlace Express にログインします。

ステップ 2　ページの上部にある［管理］をクリックします。

ステップ 3　ページ左側の [Meeting Configuration] をクリックします。

ステップ 4　[Meeting Configuration] ページで、次のフィールドを設定します。

- Minimum meeting password length（P. C-112）：値が大きいほど、セキュリティが強化されます。

ステップ 5　[Save] をクリックします。

ステップ 6　ページ左側の [User Configuration] をクリックします。

ステップ 7　次のいずれかを実行します。

- ユーザ グループの設定を行うには、[User Group Management] をクリックします。
- 個人のユーザ プロファイルを設定するには、[User Profile Management] をクリックします。

ステップ 8　次のいずれかを実行します。

- 既存のユーザ プロファイルを設定するには、[Edit] をクリックします。
- 新しいユーザ プロファイルを設定するには、[Add New] をクリックします。必須のフィールド（アスタリスク（*）が付いています）を設定します。

ステップ 9　次のいずれかのフィールドを設定します。

- Password required（P. C-13）（ユーザ グループ）：[Yes] を選択します。
- Password required（P. C-26）（ユーザ プロファイル）：[Yes] を選択します。

ステップ 10　[Save] をクリックします。

ステップ 11　会議のパスワードを必須にするすべてのユーザ グループおよびユーザ プロファイルについて、ステップ 6 からステップ 10 までを繰り返します。

ヒント

会議招待者が会議に参加できるように、パスワードを必ず通知してください。

- 電子メールによる通知にパスワードが記載されるように、ユーザ グループとユーザ プロファイルを設定します。「ユーザ グループの電子メール通知設定の設定」（P. 14-7）を参照してください。
- 会議招待者の中に電子メール通知を受信しない人がいる場合は、会議スケジュール担当者または別の主催者が手動で会議パスワードを通知する必要があります。

関連項目

- システムのセキュリティに関する推奨事項（P. 11-2）
- 概要：会議の設定（P. C-109）
- 概要：ユーザ グループの追加（P. C-11）
- 概要：ユーザ プロファイルの追加（P. C-18）

スケジュールされた会議および記録へのアクセスの制限

この項では、プロファイルを持たないユーザが次のアクションを実行できないようにする方法を説明します。

- 特定のユーザまたは任意のユーザによってスケジュールされた会議に参加すること。
- 特定のユーザまたは任意のユーザによって記録された会議を再生すること。

手順

ステップ 1　Cisco Unified MeetingPlace Express にログインします。

ステップ 2　ページの上部にある［管理］をクリックします。

ステップ 3　ページ左側の [User Configuration] をクリックします。

ステップ 4　次のいずれかを実行します。

- ユーザ グループを設定するには、[User Group Management] をクリックします。
- 個人のユーザ プロファイルを設定するには、[User Profile Management] をクリックします。

ステップ 5　次のいずれかを実行します。

- 既存のユーザ プロファイルを設定するには、[Edit] をクリックします。
- 新しいユーザ プロファイルを設定するには、[Add New] をクリックします。必須のフィールド（アスタリスク（*）が付いています）を設定します。

ステップ 6　会議への参加と会議記録へのアクセスをプロファイル ユーザのみに限定するには、次のいずれかのフィールドを「Users with Cisco Unified MeetingPlace Express profiles only」に設定します。

- Who can attend（P. C-13）（ユーザ グループ）
- Who can attend（P. C-26）（ユーザ プロファイル）

ステップ 7　[Save] をクリックします。

ステップ 8　会議へのアクセスをプロファイル ユーザのみに制限するすべてのユーザ グループおよびユーザ プロファイルについて、ステップ 3 からステップ 7 までを繰り返します。

ヒント

- 会議への参加がプロファイル ユーザのみに制限されている場合は、プロファイルを持たない外部ユーザ（会社の顧客やビジネス パートナーなど）や、プロファイルがロックされているユーザは参加できなくなります。
- 同様に、会議記録へのアクセスがプロファイル ユーザのみに制限されている場合は、プロファイルを持たない外部ユーザ（会社の顧客やビジネス パートナーなど）や、プロファイルがロックされているユーザは、会議記録にアクセスできなくなります。

関連項目

- システムのセキュリティに関する推奨事項（P. 11-2）
- 概要：ユーザ グループの追加（P. C-11）
- 概要：ユーザ プロファイルの追加（P. C-18）

単純な会議 ID の使用の制限

Cisco Unified MeetingPlace Express のデフォルトでは、会議スケジュール担当者が特定の会議 ID、たとえば、暗記しやすいもの（12345）や、単語のつづりに一致するもの（24726 または CISCO）を要求できます。ただし、招待を受けていない人でも、Cisco Unified MeetingPlace Express サーバの電話番号を知っていれば、よく使われる会議 ID を推測して、参加する権限のない会議に参加できてしまいます。

この項では、権限のない者が会議に参加することを防ぐために、会議スケジュール作成時にバニティ会議 ID（ユーザが選択した ID）を要求できないようにする方法を説明します。このようにすると、スケジュールされる会議すべてに、ランダムに生成された一意の ID が割り当てられます。割り当てられた会議 ID をユーザが変更することはできません。

手順

ステップ 1　Cisco Unified MeetingPlace Express にログインします。

ステップ 2　ページの上部にある［管理］をクリックします。

ステップ 3　ページ左側の [Meeting Configuration] をクリックします。

ステップ 4　[Meeting Configuration] ページで、次のフィールドを設定します。

- Allow vanity meeting IDs（P. C-113）：[No] を選択します。

ステップ 5　[Save] をクリックします。

関連項目

- システムのセキュリティに関する推奨事項（P. 11-2）
- 概要：会議の設定（P. C-109）

次の操作

権限のない者が会議に参加することを防ぐには、次の方法もあります。

- 会議パスワードを必須にする。「会議パスワードに関する要件の設定」（P. 11-5）を参照してください。
- スケジュールされた会議への参加をプロファイル ユーザのみに制限する。「スケジュールされた会議および記録へのアクセスの制限」（P. 11-6）を参照してください。

予約不要の会議を第三者が開始することの禁止

この項では、会議所有者だけが予約不要の会議を開始できるようにシステムを設定する方法を説明します。

手順

ステップ 1　Cisco Unified MeetingPlace Express にログインします。

ステップ 2　ページの上部にある［管理］をクリックします。

ステップ 3　ページの左側で次の操作を実行します。

a. [System Configuration] をクリックします。

b. [System Configuration] をクリックします。

ステップ 4　[Meeting Configuration] ページで、次のフィールドを設定します。

- Reservationless: Allow 3rd party initiate（P. C-113）：[No] を選択します。

ステップ 5　[Save] をクリックします。

関連項目

- 予約不要の会議についての情報（P. 5-7）
- システムのセキュリティに関する推奨事項（P. 11-2）
- ユーザ プロファイルのアクティブ、非アクティブ、およびロック状態について（P. 8-24）
- 概要：使用状況の設定（P. C-159）

ゲスト ユーザのダイヤルアウト特権の制限

この項では、ゲストによるダイヤルアウトを禁止する方法を説明します。このタスクが完了すると、Cisco Unified MeetingPlace Express に正しくログインしたプロファイル ユーザだけがダイヤルアウトできるようになります。このように制限することで、電話ハッカー侵入の危険性を抑えます。

手順

ステップ 1　Cisco Unified MeetingPlace Express にログインします。

ステップ 2　ページの上部にある［管理］をクリックします。

ステップ 3　ページの左側で次の操作を実行します。

a. [System Configuration] をクリックします。

b. [Usage Configuration] をクリックします。

ステップ 4　[Usage Configuration] ページの [Allow guest outdials] フィールドを [No] に設定します。

ステップ 5　[Save] をクリックします。

関連項目

- システムのセキュリティに関する推奨事項（P. 11-2）
- ダイヤルアウト機能および音声プロンプト言語（P. 8-11）
- 電話ハッカー侵入阻止のオプションについて（P. 11-2）
- プロファイル ユーザのダイヤルアウト特権の制限（P. 11-9）
- 発信コールについての情報のエクスポート（P. 10-16）
- 概要：ユーザ グループの管理（P. C-167）
- 概要：ユーザ プロファイルの管理（P. C-169）

次の操作

システムでのダイヤルアウト特権をさらに制限するには、「プロファイル ユーザのダイヤルアウト特権の制限」（P. 11-9）に進みます。

プロファイル ユーザのダイヤルアウト特権の制限

この項では、特定のユーザ グループおよびユーザ プロファイルだけがダイヤルアウト特権を持つように制限する方法を説明します。このようにダイヤルアウト特権を制限することで、電話ハッカー侵入の危険性が低下します。

手順

ステップ 1　Cisco Unified MeetingPlace Express にログインします。

ステップ 2　ページの上部にある［管理］をクリックします。

ステップ 3　ページ左側の [User Configuration] をクリックします。

ステップ 4　特定のユーザ グループのダイヤルアウト特権を制限するには、次の手順を実行します。

a. [User Group Management] をクリックします。

b. [User Group Management] ページで、ユーザ グループを選択して、同じ行にある [Edit] をクリックします。[Edit User Groups Details] ページが表示されます。

c. ダイヤルアウト特権を制限するには、次のフィールドを設定します。

- Can call out of meetings：[No] に設定します。
- Ask for profile password：[Yes] に設定します。

d. [Save] をクリックします。

e. ダイヤルアウト特権を制限するすべてのユーザ グループについて、ステップ 4 を繰り返します。

ステップ 5　特定のユーザ プロファイルのダイヤルアウト特権を制限するには、次の手順を実行します。

a. [User Profile Management] をクリックします。

b. [User Profile Management] ページで、ユーザ プロファイルを選択して、同じ行にある [Edit] をクリックします。[Edit user profiles details] ページが表示されます。

c. ダイヤルアウト特権を制限するには、次のフィールドを設定します。

- Can call out of meetings：[No] に設定します。
- Ask for profile password：[Yes] に設定します。

d. [Save] をクリックします。

e. ダイヤルアウト特権を制限するすべてのユーザ プロファイルについて、ステップ 5 を繰り返します。

関連項目

- システムのセキュリティに関する推奨事項（P. 11-2）
- ダイヤルアウト機能および音声プロンプト言語（P. 8-11）
- 電話ハッカー侵入阻止のオプションについて（P. 11-2）
- ゲスト ユーザのダイヤルアウト特権の制限（P. 11-8）
- 発信コールについての情報のエクスポート（P. 10-16）
- 概要：ユーザ グループの管理（P. C-167）
- 概要：ユーザ プロファイルの管理（P. C-169）