IM and Presence Service 向けの Microsoft Outlook カレンダー連携、リリース 15 および SU

最終更新：2026 年 6 月 22 日

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：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

© 2023–2026 Cisco Systems, Inc. All rights reserved.

目 次

第 1 章 はじめに 1

はじめに 1

対象読者 1

書籍の構成 1

表記法 2

マニュアルの入手方法およびサービスリクエストの送信方法 3

第 2 章 新規および変更情報 5

新規および変更情報 5

第 3 章 に関する概要 7

概要 7

導入 7

Exchange Web Services 7

IM and Presence Service の Microsoft Outlook カレンダリングステータス 8

制約事項と制限 8

第 4 章 カレンダー統合を計画する 11

Microsoft Outlook とのカレンダー統合の前提条件 11

構成に関する考慮事項 11

Exchange Web Services を介した Microsoft Exchange Server との統合 12

Exchange Server における管理者の役割と権限 12

Exchange Server 統合のためのプレゼンスゲートウェイ構成 13

Exchange Web Services 統合に関する既知の問題 14

セキュリティに関する考慮事項 14
Windows セキュリティポリシー設定 14

第 5 章 カレンダー連携に向けて Microsoft Exchange を構成する 15
Exchange Web Services 経由の Microsoft Exchange 2007 の構成 15
Windows セキュリティポリシー設定 16
Windows セキュリティ設定の確認 16
ユーザーにサービスアカウントへのサインイン権限ローカルで付与する... 17
Windows Server 2003 上で Microsoft Exchange 2007 を構成する 17
Windows Server 2008 上で Microsoft Exchange 2007 を構成する 18
サーバーレベルでのなりすまし権限を設定する 18
サービスアカウントの Active Directory サービス拡張権限を設定する 19
サービスアカウントとユーザメールボックスへの「代理送信」権限の付与 20
サービスアカウントとユーザーメールボックスになりすまし権限を付与する 21
Microsoft Exchange 2007 アカウントのアクセス許可を確認する 22
Exchange Web Services を介した Microsoft Exchange 2016 および 2019 の構成 23
Windows セキュリティポリシー設定 23
Windows セキュリティ設定の確認 24
Exchange 2010 で特定のユーザーまたはグループに対して Exchange のなりすまし権限を設定する 24
Exchange 2016 または 2019 の特定のユーザーまたはグループになりすまし権限を設定する 26
Microsoft Exchange 2010 アカウントの権限を確認する 27
Microsoft Exchange 2016 または 2019 アカウントで権限を確認する 29
Exchange 仮想ディレクトリで認証を有効にする 30
Windows Server 2003 上で動作する Exchange 2007 での認証の有効化 30
Windows Server 2016 で実行されている Exchange 2016 または 2019 で認証を有効にする 31

第 6 章 Microsoft Exchange を構成する 33
Microsoft Exchange のカレンダー統合構成 33
Microsoft Exchange 2016 および 2019 の構成タスクフロー 33

Windows のセキュリティ設定を確認する 34
Exchange 2016 または 2019 の特定のユーザーまたはグループになりすまし権限を設定する 35
Microsoft Exchange 2016 または 2019 アカウントで権限を確認する 36
Windows Server 2016 で実行されている Exchange 2016 または 2019 で認証を有効にする 38
SAN およびワイルドカード証明書のサポート 39
Exchange Server の証明書構成タスクフロー 39
Windows Server 2008 に CA をインストールする 40
CSR を生成する – Windows Server 2008 での操作 41
CA サーバ/認証局への CSR の送信 42
署名済み証明書のダウンロード 44
署名済み証明書をアップロードする – Windows 2008 での操作 45
ルート証明書のダウンロード 46
IM およびプレゼンスサービスノードにルート証明書をアップロードします。 46

第 7 章 **IM and Presence Service でカレンダー連携を構成する 49**
カレンダー連携の概要 49
IM and Presence カレンダー連携タスクフロー 50
IM and Presence Service に Microsoft 証明書をアップロードする 51
プレゼンスゲートウェイの設定 51
認証向け Office 365 構成 53
Office 365 統合のためのプル間隔の設定 54
カレンダーの不在情報を設定する 54
Exchange 統合のためのサービスパラメータの設定 55
Cisco Presence Engine を再起動してください。 56
初期 LDAP 同期中にカレンダー機能を有効にする 57
機能グループテンプレートにカレンダー統合を追加する 58
LDAP 同期に機能グループテンプレートを追加する 58
カレンダー連携を一括で有効化する 59
ユーザのカレンダー連携を有効にする 60

第 8 章 IM and Presence Service をカレンダー統合向けに構成する 61

Microsoft Exchange との統合にむけて Presence Gateway を構成する 61

Exchange Web Services を介してプレゼンス ゲートウェイとして Exchange 2007、2010、または 2013 を構成する 62

SAN およびワイルドカード証明書のサポート 64

IM and Presence Service と Microsoft Exchange の間にセキュリティで保護された証明書交換を構成する 64

Certificate Authority サービスをインストールする方法 64

Windows Server 2003 に CA をインストールする 65

Windows Server 2008 に CA をインストールする 66

Microsoft Exchange Server の IIS 上で CSR を生成する 67

CSR を生成する – Windows Server 2003 での操作 67

CSR を生成する – Windows Server 2008 での操作 68

CA サーバ/認証局への CSR の送信 69

署名済み証明書のダウンロード 70

Exchange IIS への署名済み証明書のアップロード 71

署名済み証明書をアップロードする – Windows 2003 での操作 71

署名済み証明書をアップロードする – Windows 2008 での操作 72

ルート証明書のダウンロード 73

IM およびプレゼンスサービスノードにルート証明書をアップロードします。 74

カレンダー統合を有効にする 76

個人ユーザ向けカレンダー統合の有効化 77

カレンダー連携を一括で有効化する 77

[オプション] Exchange Web Service 経由で送信される Exchange カレンダー通知送信頻度を構成する 78

[オプション] Microsoft Exchange 通知ポートの設定 79

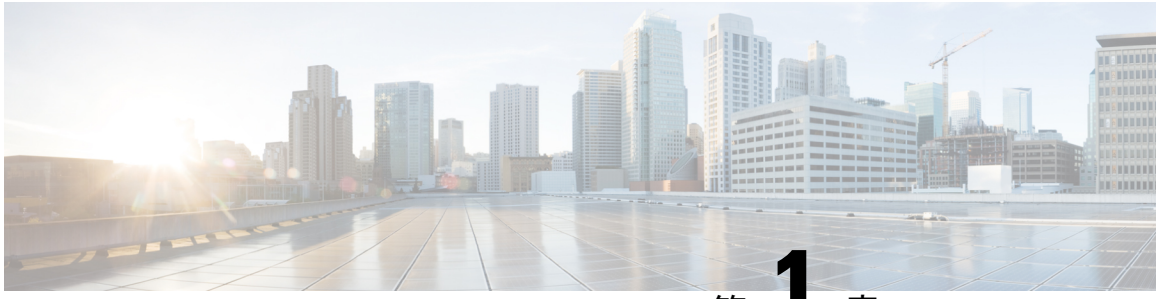
[オプション] Microsoft Exchange カレンダー通知の期間範囲の設定 80

その他の Microsoft Exchange カレンダーパラメータ 81

外出中プレゼンスステータス 81

第 9 章 Exchange 予定表統合のトラブルシューティング 83

Exchange Server の接続状態のトラブルシューティング 83
SSL 接続証明書の状態に関するトラブルシューティング 84
Microsoft Exchange との統合に影響を与えることが知られている問題 87
カレンダー統合における規模の制限 87
ユーザが Microsoft Exchange サーバ間を移動した場合、カレンダーの状態が更新されない。 88
LDAP ユーザの削除は、IM およびプレゼンスサービスに反映されるまでに少なくとも 24 時間かかります。 88
Microsoft Exchange Server URL にカレンダー向けにローカライズされた単語が含まれていることを確認する 89



第 1 章

はじめに

- はじめに （1 ページ）
- 対象読者 （1 ページ）
- 書籍の構成 （1 ページ）
- 表記法 （2 ページ）
- マニュアルの入手方法およびサービスリクエストの送信方法 （3 ページ）

はじめに

IM and Presence Service とのカレンダー連携により、ユーザーは、Microsoft Outlook のカレンダーとミーティングのステータスを IM and Presence Service の空き状況のステータスと連携できるようになります。

対象読者

この資料は、Microsoft Exchange と IM and Presence Service との統合を構成および保守する経験豊富なユーザーを対象としています。

書籍の構成

このガイドには以下の章が含まれています。

第 1 章	タイトル	説明
1	はじめに （1 ページ）	この章では、本書の構成、対象読者、および本書の目的について説明します。
2	に関する概要 （7 ページ）	この章では、IM and Presence Service 向けの Microsoft Outlook カレンダー統合機能について説明します。

第 1 章	タイトル	説明
4	カレンダー統合を計画する（11 ページ）	この章では、カレンダー統合を計画するために必要な前提条件について説明します。
5	Microsoft Exchange を構成する（33 ページ）	Outlook カレンダーとの連携のためにオンプレミスの Microsoft Exchange サーバに接続する場合にのみ、この章を参照してください。 この章では、Exchange サーバを統合用に構成する方法について説明します。
7	IM and Presence Service でカレンダー連携を構成する （49 ページ）	Outlook カレンダー連携に向けて IM and Presence Service を設定する方法については、この章を参照してください。 オンプレミスの Exchange Server に接続する場合も、クラウドホスト型の Office 365 サーバーに接続する場合も、この章を参照します。
8	Exchange 予定表統合のトラブルシューティング （83 ページ）	この章では、よくある問題のトラブルシューティング手順と解決策について説明します。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	表示
太字 フォント	コマンド、キーワード、およびユーザーが入力したテキストは、**太字**フォントで表示されます。
斜体 フォント	文書のタイトル、新規用語または強調された用語、および値を指定する引数は、斜体フォントで表示されます。
`Courier` フォント	端末セッションとシステムが表示する情報は、`courier` フォントで表示されます。

（注） 「注釈」です。 注記には、マニュアルに記載されていない役立つヒントや資料への参照が含まれています。

ヒント 次の情報が問題の解決に役立つことを意味します。 ヒントの情報は、トラブルシューティングや具体的な対処法ではないかもしれませんが、時間短縮に役立つ情報など、有用な情報である可能性があります。

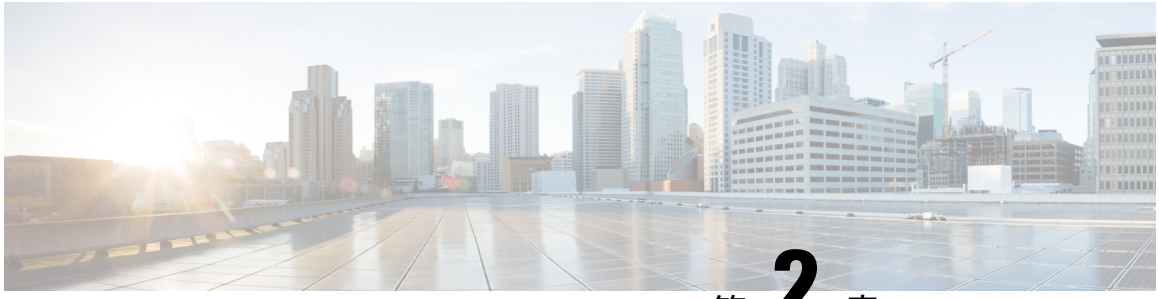
注意 「要注意」の意味です。 このような状況では、機器の損傷やデータの損失につながる可能性のある行動を行う可能性があります。

マニュアルの入手方法およびサービスリクエストの送信方法

ドキュメントの入手方法、サービスリクエストの送信、追加情報の収集については、月次『*Cisco Product Documentation* の新機能』を参照してください。これには、新規および改訂されたすべての Cisco 技術ドキュメントも一覧表示されています。入手先は以下のとおりです。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*Cisco Product Documentation* の新機能』は、Really Simple Syndication (RSS) フィードとしてサブスクライブでき、リーダーアプリケーションを使用すると、お使いのデスクトップに直接コンテンツを配信されるように設定できます。 RSS フィードは、無料のサービスで、Cisco は現在 RSS バージョン 2.0 をサポートしています。



第 2 章

新規および変更情報

- 新規および変更情報 （5 ページ）

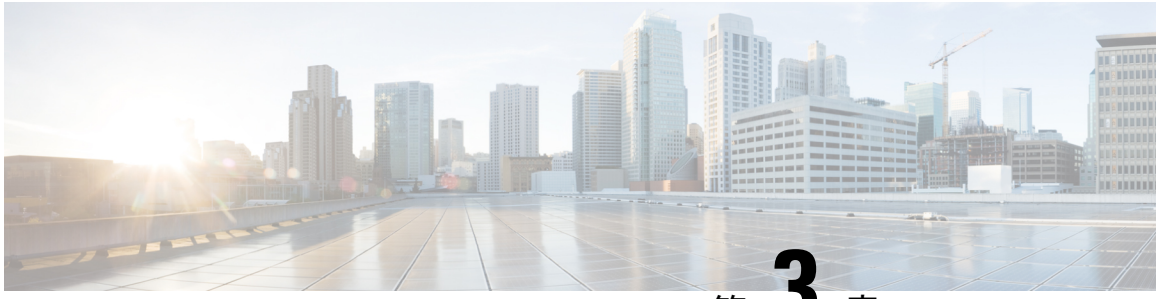
新規および変更情報

次の表は、この最新リリースに関するこのガイドでの機能に対する大幅な変更の概要を示したものです。ただし、このリリースに関するガイドの変更点や新機能のなかには、この表に記載されていないものもあります。

表 *1 : Unified Communications Manager* と *IM and Presence Service* での新機能と変更された動作

日付（Date）	説明	参照先
2026 年 2 月 5 日	カレンダーの不在情報を設定する手順を追加しました。	カレンダーの不在情報を設定する （54 ページ）
2024 年 10 月 01 日	「プレゼンスゲートウェイの構成」機能に、政府機関の URL に対する Office 365 のサポートを構成する手順を追加しました。	Presence Gateway を構成する
2024 年 10 月 01 日	TLS 1.3 の最小バージョンに関する注記を追加しました。	Presence Gateway を構成する

新規および変更情報



第 3 章

に関する概要

- 概要 （7 ページ）
- 導入 （7 ページ）
- IM and Presence Service の Microsoft Outlook カレンダリングステータス （8 ページ）
- 制約事項と制限 （8 ページ）

概要

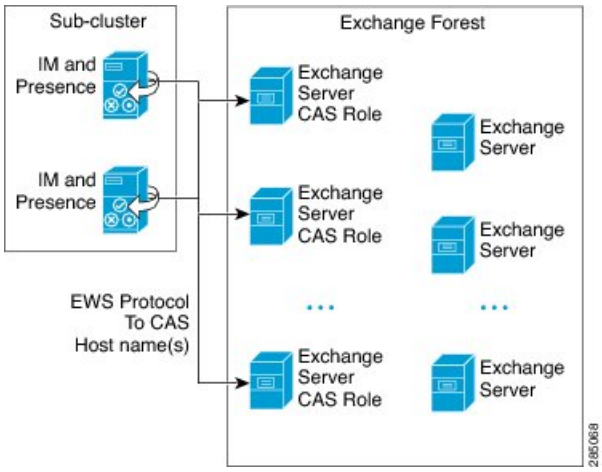
Microsoft Outlook カレンダーと IM and Presence Service の統合により、ユーザーは、Microsoft Outlook のカレンダーとミーティングのステータスを IM and Presence Service の空き状況のステータスと連携できるようになります。 この統合は、IM and Presence Service をオンプレミスの Microsoft Exchange Server またはホスト型 Office 365 サーバーに接続することで実現できます。

導入

Exchange Web Services

Exchange Web Services (EWS) を使用すると、HTTP を介して Microsoft Exchange のメールボックスおよびコンテンツとやり取りできます。 EWS は、Microsoft Outlook を通じて利用できるデータの多くへのアクセスを提供します。 EWS は、クライアントコンピュータからサーバへいくつかの責任を移管します。

図 *1 : EWS* で *Microsoft Exchange* と *IM and Presence Service* を統合する



IM and Presence Service の Microsoft Outlook カレンダリングステータス

Microsoft Outlook を Microsoft Exchange または Office 365 経由で IM and Presence Service と統合することで、ユーザーは、Microsoft Outlook のカレンダー/ミーティングステータスを IM and Presence Service の空き状況のステータスに組み込むことができます。 以下の表は、到達可能性のマッピングと、IM and Presence Service がミーティングのステータス (Microsoft Outlook カレンダーに表示されるもの) を、IM and Presence Service のユーザーの空き状況のステータスとどのように関連付けるかを示しています。

表 *2 :* カレンダー状態に基づく集計された可用性状態

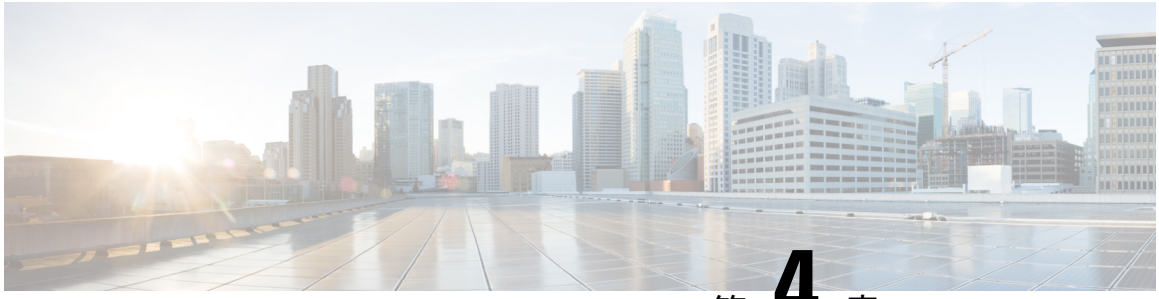
Microsoft Outlook の状態	IM およびプレゼンスサービスの状態
空き/一時	利用可能
ビジー	ミーティング中
外出中	不在
不在	不在

制約事項と制限

以下は、IM and Presence Service と Microsoft Exchange を統合する際の制限事項です。

- EWS サーバーは、上限なく 1 台または複数台を追加、更新、削除できます。 ただし、[プレゼンス ゲートウェイ構成] ウィンドウの [トラブルシューター] は、構成した最初の 10 台の EWS サーバの状態を確認して報告するように設計されています。
- この IM and Presence Service のリリースは、Exchange 自動検出サービスをサポートしていません。 自動検出サービスは、クライアントアクセスサーバ（CAS）または複数のサーバ間で既に負荷分散メカニズムが実装されていることを前提としています。
- Exchange サーバーまたは Office 365 サーバーを Presence Gateway として構成したら、ローカルの Outlook から会議を受信したときに、Jabber クライアントは、**[会議中]** 状態に設定できなくなります。 **[会議中]** 状態は、Presence Gateway 経由でのみ設定されます。 プレゼンスゲートウェイが何らかの理由でダウンした場合、クライアントは **会議中** ステータスを設定できません。

（注） **[会議中]** 状態に設定するには、Presence Gateway 向けサービスをリストアする必要があります。



第 4 章

カレンダー統合を計画する

- Microsoft Outlook とのカレンダー統合の前提条件 （11 ページ）
- 構成に関する考慮事項 （11 ページ）
- セキュリティに関する考慮事項 （14 ページ）

Microsoft Outlook とのカレンダー統合の前提条件

IM およびプレゼンス サービスは、オンプレミスの Exchange Server とクラウドホスト型 Exchange Online の両方との Microsoft Outlook カレンダーの統合をサポートします。 サポートされている構成の詳細については、次の表を参照してください。

表 *3*: カレンダー連携のサポート情報

コンポーネント	互換バージョンのインストール
カレンダーサーバ	• Exchange Server サブスクリプション エディション (SE) • Microsoft 365 (旧 Office 365) の Exchange Online
証明書サーバ	• Windows Server に組み込まれた Microsoft 証明書サーバ • サードパーティの CA サーバ （注） IM and Presence Service を使用した Microsoft Exchange の統合サービスは、RSA 1024 または 2048 ビットキーと SHA1 および SHA256 署名アルゴリズムを使用した証明書をサポートしています。

構成に関する考慮事項

本書には、オンプレミスの Microsoft Exchange 導入またはホスト型の Office 365 導入において、IM and Presence Service と Microsoft Outlook 間のカレンダー連携を構成する方法を説明する構成タスクが含まれています。 以下の表を参考に、展開に使用する章を決定してください。

表 *4 : Microsoft* 展開のための構成タスク

Microsoft 展開	これらの設定章を一読してください...
Microsoft Exchange (2016、2019)	• Microsoft Exchange 2016 および 2019 の構成タスクフロー （33 ページ） • IM and Presence カレンダー連携タスクフロー （50 ページ）
Microsoft Office 365	• IM and Presence カレンダー連携タスクフロー （50 ページ）

Exchange Web Services を介した Microsoft Exchange Server との統合

Microsoft Exchange Server は、カレンダリング連携に向けて Exchange Server への SOAP (Simple Object Access Protocol) に類似したインターフェースを使用する Exchange Web Services (EWS) を導入しました。

Cisco Unified CM IM and Presence Service Administration のユーザインターフェイスで Exchange 統合用の EWS Presence Gateway を設定する際は、以下の点に注意してください。

- EWS サーバーは、上限なく 1 台または複数台を追加、更新、削除できます。 ただし、**[Presence Gateway構成]** ウィンドウのトラブルシューティングツールは、構成した最初の 10 の EWS サーバーのステータスのみを検証して報告します。
- EWS サーバゲートウェイは、最初の EWS サーバゲートウェイ用に設定した認証情報（アカウント名とパスワード）を共有します。 1 つの EWS サーバゲートウェイの認証情報を変更すると、設定されているすべての EWS ゲートウェイの認証情報もそれに応じて変更されます。
- 1 つ以上の EWS サーバを追加、更新、または削除した後は、設定変更を有効にするために Cisco Presence Engine を再起動する必要があります。 複数の EWS サーバを順次追加する場合、Cisco Presence Engine を一度再起動するだけで、すべての変更を同時に反映させることができます。

Exchange Server における管理者の役割と権限

Exchange Web Services (EWS) では、すべてのユーザのカレンダー情報にアクセスできるようにするために、特別なアカウントが必要です。 このアカウントは、なりすましアカウントと呼ばれます。

Microsoft Exchange Server 2007

Exchange Server 2007 で発信者が他のユーザーのメールアカウントにアクセスする場合、EWS 統合で、なりすまし権限を持つアカウントが必要です。 発信者は、発信者のアカウントに関連

付けられている権限ではなく、なりすましアカウントに関連付けられている権限を使用して、指定されたユーザーアカウントになりすます。

なりすましアカウントには、Exchange 2007 で実行中の Client Access Server (CAS) で **ms-Exch-EPI-Impersonation** 権限を付与する必要があります。これにより発信者はCAS を使用してユーザーメールアカウントになりすます権限が付与されます。 さらに発信者には、メールボックスデータベースまたはディレクトリの個別のユーザーオブジェクトのいずれかに対する **ms-Exch-EPI-MayImpersonate** 権限を付与する必要があります。

個々のユーザのアクセス制御リスト（ACL）は、メールボックスデータベースの設定よりも優先されるため、発信者に対してデータベース内のすべてのメールボックスへのアクセスを許可しつつ、必要に応じて、そのデータベース内の特定のメールボックスへのアクセスを拒否することができます。

Microsoft Exchange Server

Microsoft Exchange Server は、ロールベースのアクセス制御 (RBAC) を使用して、なりすましアカウントに権限を割り当て、ユーザーが組織内での役割に固有のタスクを実行できるようにします。 ユーザが管理者、スーパーユーザ、エンドユーザのいずれであるかによって、RBAC 権限を適用する主な方法は 2 つあります。

- 管理ロールグループ — Microsoft は、Exchange セットアッププロセス中に、グループのロールに応じた関連する権限が付与された 11 のデフォルト管理ロールグループを提供します。 例えば、受信者管理やヘルプデスクは、組み込みの役割グループです。 通常、特定のタスクを実行する必要のあるスーパーユーザーは、関連する管理役割グループに割り当てられ、関連する権限を継承します。 例えば、Exchange 組織全体のあらゆるユーザの連絡先情報を変更する必要のある製品サポート担当者は、ヘルプデスク管理ロールグループのメンバーとして割り当てられる場合があります。
- 管理ロール割り当てポリシー—管理者やスーパーユーザーではない一般ユーザーの場合、管理ロール割り当てポリシーが、該当するユーザーが修正できる具体的なメールボックスを制御します。 **ApplicationImpersonation** ロールは、 **New-ManagementRoleAssignment** コマンドレットを使用してユーザに割り当てられると、アカウントが組織内のユーザになりすまして、ユーザに代わってタスクを実行できるようになります。 ロールの割り当ての範囲は、 **New-ManagementScope** コマンドレットを使用して個別に管理され、特定の受信者または特定のサーバーを対象とするようにフィルタリングできます。

Exchange Server 統合のためのプレゼンスゲートウェイ構成

(EWS カレンダー連携が有効になっている) 多数のユーザーをサポートするには、IM and Presence Service は、EWS トラフィックの負荷を複数の Client Access サーバー (CAS) に分散させる必要があります。 IM and Presence Serviceは、EWS 経由で複数の CAS に接続でき、次のラウンドロビン戦略を使用して、受信するトラフィックの負荷を処理します。

- ユーザのカレンダー購読が初めて有効になると、管理者が設定した対象となる CAS ホストのプールから、ユーザに CAS が割り当てられます。
- ユーザは、カレンダーの購読が失敗するまで、その割り当てを保持します。

- ユーザのカレンダーサブスクリプションが失敗した場合、対象となる CAS ホストのプールから再び CAS が割り当てられます。

Exchange Web Services 統合に関する既知の問題

- Exchange Web Services (EWS) の統合に影響を与えることが知られている問題については、このガイドの「Exchange 予定表統合のトラブルシューティング （83 ページ）」章を参照してください。
- Microsoft Exchange との統合に影響を与えることが知られている問題 （87 ページ）を参照してください。

セキュリティに関する考慮事項

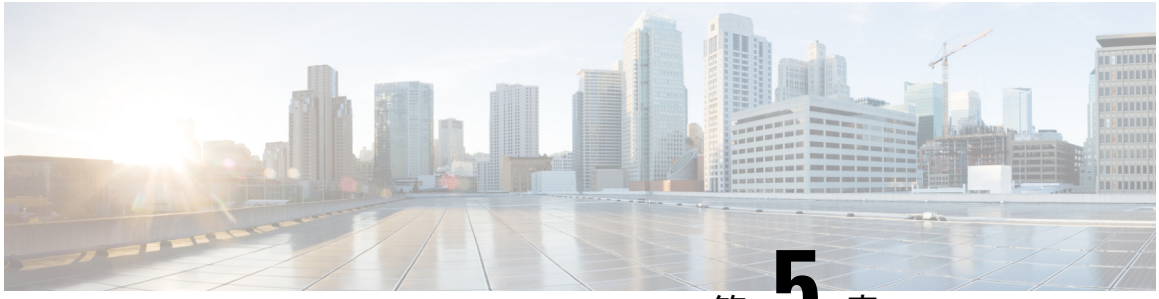
Windows セキュリティポリシー設定

IM and Presence Service と Microsoft Exchange の統合により、Windows 統合認証 (NTLM) を含むさまざまな認証方法がサポートされます。

IM and Presence Service は、NTLMv1 と NTLMv2 の両方の Windows 統合認証をサポートしており、デフォルトで NTLMv2 が使用されます。

[LANマネージャー認証レベル] を **[NTLMv2レスポンスのみを送信]** に構成します。 **Windows ドメイン コントローラーで LM と NTLM** を拒否すると、ドメインで NTLMv2 認証が強制されます。

（注） IM and Presence Service は、NTLMv2 セッションセキュリティをサポートしていません。 メッセージの機密性と完全性は、セキュリティで保護された HTTP (HTTPS) によって確保されます。



第 5 章

カレンダー連携に向けて Microsoft Exchange を構成する

- Exchange Web Services 経由の Microsoft Exchange 2007 の構成 （15 ページ）
- Exchange Web Services を介した Microsoft Exchange 2016 および 2019 の構成 （23 ページ）
- Exchange 仮想ディレクトリで認証を有効にする （30 ページ）

Exchange Web Services 経由の Microsoft Exchange 2007 の構成

事前準備

Exchange Server 2007 を構成するために必要な手順は、Windows Server 2003 を使用するか Windows Server 2008 を使用するかによって異なることに注意してください。

Exchange Server 2007 でメールボックスへのアクセスを構成する際には、以下のタスクを完了する必要があります。詳細な手順については、次の URL にある Exchange Server 2007 のドキュメントを参照してください。http://technet.microsoft.com/en-us/library/bb124558(EXCHG.80).aspx

- Windows セキュリティ設定の確認 （16 ページ）
- ユーザーにサービスアカウントへのサインイン権限ローカルで付与する... （17 ページ）
- サーバーレベルでのなりすまし権限を設定する （18 ページ）
- サービスアカウントとユーザメールボックスへの「代理送信」権限の付与 （20 ページ）
- サービスアカウントとユーザーメールボックスになりすまし権限を付与する （21 ページ）
- Microsoft Exchange 2007 アカウントのアクセス許可を確認する （22 ページ）

ヒント IM and Presence Service では、アカウントに対するなりすまし権限のみが必要で、これにより、Exchange Server に接続する際にアカウントにログインできるようになります。 このアカウントは、通常、メールを受信しないため、容量を確保する必要がないことに注意してください。

Windows セキュリティポリシー設定

IM and Presence Service と Microsoft Exchange の統合により、Windows 統合認証 (NTLM) を含むさまざまな認証方法がサポートされます。

IM and Presence Service は、NTLMv1 と NTLMv2 の両方の Windows 統合認証をサポートしており、デフォルトで NTLMv2 が使用されます。

[LANマネージャー認証レベル] を **[NTLMv2レスポンスのみを送信]** に構成します。 **Windows ドメイン コントローラーで LM と NTLM** を拒否すると、ドメインで NTLMv2 認証が強制されます。

（注） IM and Presence Service は、NTLMv2 セッションセキュリティをサポートしていません。 メッセージの機密性と完全性は、セキュリティで保護された HTTP (HTTPS) によって確保されます。

Windows セキュリティ設定の確認

手順

ステップ 1 Windows ドメインコントローラーと Exchange を実行しているサーバーで、**[開始]** > **[管理ツール]** > **[ローカルセキュリティポリシー]** の順に選択します。

ステップ 2 **[セキュリティ設定]** > **[ローカルポリシー]** > **[セキュリティオプション]** の順に選択します。

ステップ 3 **[ネットワークセキュリティ:セキュリティで保護されたRPCを含むNTLM SSPサーバー向けの最小セッションセキュリティ]**を選択します。

ステップ 4 「NTLMv2 セッション セキュリティを要求する」チェックボックスがオフになっていることを確認してください。

ステップ 5 「NTLMv2 セッション セキュリティを要求する」チェックボックスがオンになっている場合は、以下の手順を実行してください。

a) **[NTLMv2セッションセキュリティが必要]** チェックボックスをオフにします。

b) **OK**をクリックします。

ステップ 6 新しいセキュリティ設定を適用するには、Windows ドメインコントローラーと Exchange を実行しているサーバを再起動してください。

（注）
再起動が必要なのは、セキュリティポリシーの設定変更が行われたサーバのみです。

ユーザーにサービスアカウントへのサインイン権限ローカルで付与する...

以下の手順のいずれかを実行して、ユーザーがサービスアカウントにローカルでログインできるようにします。

はじめる前に

- Exchange のなりすましを機能させるには、すべての Microsoft Exchange Server を Windows Authorization Access Group のメンバーにする必要があります。
- サービスアカウントは、Exchange 管理グループのいずれにも属してはなりません。Exchange は、これらのグループに属するすべてのアカウントについて、なりすましを明確に拒否します。

Windows Server 2003 上で Microsoft Exchange 2007 を構成する

手順

ステップ 1 Exchange Server 2007 のユーザインターフェイスに、Exchange 閲覧専用管理者ロールが委任されたサービスアカウントを使用してログインします。

ステップ 2 左側のペインの [セキュリティ設定] で、**[ローカルポリシー]** > **[ユーザー権限の割り当て]** の順に選択します。

ステップ 3 コンソールの右ペインで、**[ローカルログオンを許可]** をダブルクリックします。

ステップ 4 **[ユーザまたはグループを追加]** を選択し、作成したサービスアカウントに移動して選択します。

ステップ 5 **[名前を確認]** を選択して、指定されたユーザーが正しいことを確認します。

ステップ 6 **OK**をクリックします。

次のタスク

サーバーレベルでのなりすまし権限を設定する （18 ページ）

Windows Server 2008 上で Microsoft Exchange 2007 を構成する

手順

ステップ 1 Exchange View Only Administrator ロールが委任されたサービスアカウントを使用して、Exchange Server 2007 にログインします。

ステップ 2 [開始] を選択します。

ステップ 3 gpmc.msc と入力してください。

ステップ 4 Enter キーを押してください。

ステップ 5 Exchange Server で **[ドメインコントローラセキュリティ設定]** ウィンドウを開きます。

ステップ 6 左側のペインの **[セキュリティ設定]** で、**[ローカルポリシー]** > **[ユーザー権限の割り当て]** の順に選択します。

ステップ 7 コンソールの右ペインで、**[ローカルログオンを許可]** をダブルクリックします。

ステップ 8 **[これらのポリシー設定を定義する]** チェックボックスがオンになっていることを確認します。

ステップ 9 「ユーザまたはグループの追加」を選択し、以前に作成したサービスアカウントに移動して選択します。次に **OK**をクリックします。

ステップ 10 **[名前を確認]** を選択して、指定されたユーザーが正しいことを確認します。 次に、**[OK]** をクリックします。

ステップ 11 **[適用]** をクリックしたら、**[プロパティにローカルでログオンする]**ダイアログボックスで、**[OK]** をクリックします。

ステップ 12 ユーザの SMTP アドレスが *alias@FQDN* であるかどうかを確認します。 そうでない場合は、ユーザプリンシパル名（UPN）を使用してなりすましを行う必要があります。 これは *alias@FQDN* として定義されます。

次のタスク

サーバーレベルでのなりすまし権限を設定する （18 ページ）

サーバーレベルでのなりすまし権限を設定する

以下の手順で示すコマンドを使用すると、サーバーレベルでなりすまし権限を付与できます。データベース、ユーザ、連絡先の各レベルで権限を付与することもできます。

はじめる前に

- サービス アカウントに個々の Microsoft Exchange サーバへのアクセス権限のみを付与する場合は、

  `Get-OrganizationConfig`

  文字列で

  `Get-ExchangeServer -Identity`*`ServerName`*

ここで、 *ServerName* は Exchange サーバの名前です。

例

```
Add-ADPermission -Identity (Get-ExchangeServer -Identity exchangeserver1)。
DistinguishedName -User (Get-User -Identityuser| select-object).identity
-ExtendedRights Send-As
```

- ユーザの SMTP アドレスが alias@FQDN として定義されていることを確認してください。そうでない場合は、User Principal Name (UPN) を使用して、ユーザーアカウントになりすます必要があります。

手順

ステップ 1 コマンドライン入力のために、Exchange Management Shell (EMS) を開きます。

ステップ 2 サーバーになりすまし権限をつかするには、Add-ADPermission コマンドを実行します。

構文

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User -Identity
User| select-object).identity -AccessRights GenericAll -InheritanceType Descendents
```

例

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User -Identity
Ex2007| select-object).identity -AccessRights GenericAll -InheritanceType Descendents
```

次のタスク

サービスアカウントの Active Directory サービス拡張権限を設定する （19 ページ）

サービスアカウントの Active Directory サービス拡張権限を設定する

始める前に

なりすましを実行するサービスアカウントに対して、クライアントアクセスサーバ（CAS）上でこれらの権限を設定する必要があります。

- CAS がロードバランサーの背後に配置されている場合は、ロードバランサー背後のすべての CAS の Microsoft Exchange 2007 アカウントに **ms-Exch-EPI-Impersonation** 権限を付与します。
- メールボックスサーバーが CAS とは異なるマシンに配置されている場合は、すべてのメールボックスサーバーの Exchange 2007 アカウントに **ms-Exch-EPI-Impersonation** 権限を付与します。
- これらの権限は、**[Active Directoryサイトおよびサービス]** または **[Active Directoryユーザーおよびコンピューター]** ユーザーインターフェイス経由でも設定できます。

手順

ステップ 1 Exchange Management Shell (EMS) を開きます。

ステップ 2 EMS で Add-ADPermission コマンドを実行すると、指定されたサービスアカウント (たとえば、Exchange 2007) のサーバーでなりすまし権限を付与できます。

構文

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User -Identity
User| select-object).identity -ExtendedRight ms-Exch-EPI-Impersonation
```

例

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User -IdentityEx2007|
select-object).identity -ExtendedRight ms-Exch-EPI-Impersonation
```

ステップ 3 EMS で Add-ADPermission コマンドを実行すると、そのサービスアカウントがなりすましを行う各メールボックスに対してなりすまし権限を付与できます。

構文

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User -Identity
User| select-object).identity -ExtendedRight ms-Exch-EPI-May-Impersonate
```

例

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User -IdentityEx2007|
select-object).identity -ExtendedRight ms-Exch-EPI-May-Impersonate
```

次のタスク

サービスアカウントとユーザメールボックスへの「代理送信」権限の付与 （20 ページ）

サービスアカウントとユーザメールボックスへの「代理送信」権限の付与

サービスアカウントとユーザメールボックスに「代理送信」権限を付与するには、以下の手順に従ってください。

（注） この手順を完了するために、Microsoft Exchange 管理コンソール (EMC) を使用することはできません。

手順

ステップ 1 Exchange Management Shell (EMS) を開きます。

ステップ 2 EMS で、Add-ADPermission コマンドを実行して、サービスアカウントと関連するすべてのメールボックスストアに Send As 権限を付与します。

構文

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User -IdentityUser|
select-object).identity -ExtendedRights Send-As
```

例

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User -IdentityEx2007|
select-object).identity -ExtendedRights Send-As
```

次のタスク

サービスアカウントとユーザーメールボックスになりすまし権限を付与する （21 ページ）

サービスアカウントとユーザーメールボックスになりすまし権限を付与する

サービスアカウントとユーザメールボックスに偽装権限を付与するには、以下の手順に従ってください。

（注） この手順を完了するために、Microsoft Exchange 管理コンソール (EMC) を使用することはできません。

手順

ステップ 1 Exchange Management Shell (EMS) を開きます。

ステップ 2 EMS で、**Add-ADPermission** コマンドを実行して、サービスアカウントと関連するすべてのメールボックスストアになりすまし権限を付与します。

構文

```
Add-ADPermission -Identity (Get-OrganizationConfig) .DistinguishedName -User (Get-User -Identity
User| select-object) .identity -ExtendedRights Receive-As
```

例

```
Add-ADPermission -Identity (Get-OrganizationConfig) .DistinguishedName -User (Get-User -IdentityEX2007
| select-object) .identity -ExtendedRights Receive-As
```

（注）
IM and Presence Service では、アカウントに対するなりすまし権限のみが必要で、これにより、Exchange Server に接続する際にアカウントにログインできるようになります。 このアカウントは、通常、メールを受信しないため、容量を確保する必要はありません。

次のタスク

Microsoft Exchange 2007 アカウントのアクセス許可を確認する （22 ページ）

Microsoft Exchange 2007 アカウントのアクセス許可を確認する

Exchange 2007 アカウントに権限を割り当てたら、メールボックスレベルで権限が反映され、指定されたユーザーが、メールボックスにアクセスでき、別のユーザーのアカウントになりすますことができることを確認する必要があります。 Exchange 2007 では、アクセス許可がメールボックスに反映されるまでに時間がかかります。

手順

ステップ 1 Exchange Server 2007 の Exchange 管理コンソール (EMC) のコンソールツリーにある **[Active Directoryサイトとサービス]** を右クリックします。

ステップ 2 **[表示]** にカーソルを合わせて、**[サービスノードを表示]** を選択します。

ステップ 3 たとえば、`Services/MS Exchange/First Organization/Admin Group/Exchange Admin Group/Servers` などのサービスノードを展開します。

ステップ 4 選択したサービスノードにクライアントアクセスサーバ（CAS）がリストされていることを確認してください。

ステップ 5 各 CAS の「プロパティ」を表示し、[セキュリティ] タブで次を検証します。

a) サービスアカウントが一覧されます。

b) サービスアカウントに付与された権限 (チェックボックスがオンになっています) は、Exchange Web Services のなりすまし権限がそのアカウントで許可されていることを示します。

（注）
手順 5 で説明したとおりにアカウントまたはなりすまし権限が表示されない場合は、サービスアカウントを再作成し、必要ななりすまし権限がアカウントに付与されていることを確認する必要がある場合があります。

ステップ 6 たとえば、Ex2007 などのサービスアカウントに対して、個人情報の交換、および他のユーザーアカウントとしての Send As と Receive As を実行できるよう、ストレージグループおよびメールボックスストアにおいて Allow Impersonation 権限が付与されていることを確認します。

ステップ 7 変更を有効にするには、Exchange Server を再起動する必要がある場合があります。 これはテスト中に確認できます。

次のタスク

Exchange 仮想ディレクトリで認証を有効にする （30 ページ）

Windows Server 2003 上で動作する Exchange 2007 での認証の有効化 （30 ページ）

Exchange Web Services を介した Microsoft Exchange 2016 および 2019 の構成

Exchange 2016 および 2019 サーバ上のメールボックスへのアクセスを設定する際は、以下の手順に従ってください。

事前準備

Exchange Web Services (EWS) を使用して Exchange 2016 および 2019 サーバーを IM and Presence Serviceと統合する前に、Exchange Server で throttle policy パラメーター値を構成します。 これらは、EWS カレンダリングが IM and Presence Serviceと連携するために必要な値です。

これらは、Exchange Server 2016 および 2019 のコマンドと設定です。

表 *5 : Exchange Server 2016* または *2019* に推奨されるスロットルポリシー設定

パラメータ[1]	推奨構成値 — Exchange Server 2016 および 2019
EwsCutoffBalance	3000000
EwsMaxBurst	300000
EwsMaxConcurrency	**100**
EwsMaxSubscriptions	無制限
EwsRechargeRate	900000

[1] これらは、Exchange Server 2016 または 2019 で変更できる唯一の EWS パラメーターです。

Windows セキュリティポリシー設定

IM and Presence Service と Microsoft Exchange の統合により、Windows 統合認証 (NTLM) を含むさまざまな認証方法がサポートされます。

IM and Presence Service は、NTLMv1 と NTLMv2 の両方の Windows 統合認証をサポートしており、デフォルトで NTLMv2 が使用されます。

[LANマネージャー認証レベル] を **[NTLMv2レスポンスのみを送信]** に構成します。 **Windows ドメイン コントローラーで LM と NTLM** を拒否すると、ドメインで NTLMv2 認証が強制されます。

（注） IM and Presence Service は、NTLMv2 セッションセキュリティをサポートしていません。 メッセージの機密性と完全性は、セキュリティで保護された HTTP (HTTPS) によって確保されます。

Windows セキュリティ設定の確認

手順

ステップ 1 Windows ドメインコントローラーと Exchange を実行しているサーバーで、**[開始]** > **[管理ツール]** > **[ローカルセキュリティポリシー]** の順に選択します。

ステップ 2 **[セキュリティ設定]** > **[ローカルポリシー]** > **[セキュリティオプション]** の順に選択します。

ステップ 3 **[ネットワークセキュリティ:セキュリティで保護されたRPCを含むNTLM SSPサーバー向けの最小セッションセキュリティ]**を選択します。

ステップ 4 「NTLMv2 セッション セキュリティを要求する」チェックボックスがオフになっていることを確認してください。

ステップ 5 「NTLMv2 セッション セキュリティを要求する」チェックボックスがオンになっている場合は、以下の手順を実行してください。

a) **[NTLMv2セッションセキュリティが必要]** チェックボックスをオフにします。

b) **OK**をクリックします。

ステップ 6 新しいセキュリティ設定を適用するには、Windows ドメインコントローラーと Exchange を実行しているサーバを再起動してください。

（注）
再起動が必要なのは、セキュリティポリシーの設定変更が行われたサーバのみです。

Exchange 2010 で特定のユーザーまたはグループに対して Exchange のなりすまし権限を設定する

特定のユーザーまたはユーザグループに対して Exchange のなりすまし権限を設定するには、Microsoft Exchange Management Shell (EMS) を使用して以下の手順を実行します。

これらは Exchange Server 2010 のコマンドと設定です。Exchange Server 2013 を使用している場合は、Exchange 2016 または 2019 の特定のユーザーまたはグループになりすまし権限を設定する （26 ページ） の手順を実行します。

手順

ステップ 1 Active Directory にアカウントを作成します。

ステップ 2 コマンドライン入力のために EMS を開きます。

ステップ 3 EMS で New-ManagementRoleAssignment コマンドを実行して、指定した既存のドメインサービスアカウント（例： *Ex2010*）に他のユーザアカウントを偽装する権限を付与します。

構文

```
New-ManagementRoleAssignment -Name:_suImpersonateRoleAsg -Role:ApplicationImpersonation
-User:user@domain
```

例

```
New-ManagementRoleAssignment -Name:_suImpersonateRoleAsg -Role:ApplicationImpersonation
-User:Ex2010@contoso.com
```

ステップ 4 偽装権限が適用される範囲を定義するには、この New-ManagementRoleAssignment コマンドを実行します。この例では、 *Ex2010* アカウントに、指定された Exchange Server 上のすべてのアカウントになりすます権限が付与されます。

構文

```
New-ManagementScope -Name:_suImpersonateScope -ServerList:server_name
```

例

```
New-ManagementScope -Name:_suImpersonateScope -ServerList:nw066b-227
```

ステップ 5 以下の表に示す推奨値を使用して、New-ThrottlingPolicy コマンドを実行し、新しいスロットリングポリシーを作成します。

構文

```
New-ThrottlingPolicy -Name:Policy_Name -EwsMaxConcurrency:100 -EwsPercentTimeInAD:50
-EwsPercentTimeInCAS:90 -EwsPercentTimeInMailboxRPC:60 -EwsMaxSubscriptions:NULL
-EwsFastSearchTimeoutInSeconds:60 -EwsFindCountLimit:1000
```

例

```
New-ThrottlingPolicy -Name:IM_and_Presence_ThrottlingPolicy -EwsMaxConcurrency:100
-EwsPercentTimeInAD:50 -EwsPercentTimeInCAS:90 -EwsPercentTimeInMailboxRPC:60 -EwsMaxSubscriptions:NULL
-EwsFastSearchTimeoutInSeconds:60 -EwsFindCountLimit:1000
```

注: サポートされている Exchange SP1 でのみ利用可能です。

ステップ 6 Set-ThrottlingPolicyAssociation コマンドを実行して、新しいスロットリングポリシーを手順 2 で使用したサービスアカウントに関連付けます。

構文

```
Set-ThrottlingPolicyAssociation -IdentityUsername -ThrottlingPolicyPolicy_Name
```

例

```
Set-ThrottlingPolicyAssociation -IdentityEx2010-ThrottlingPolicy IM_and_Presence_ThrottlingPolicy
```

次のタスク

Microsoft Exchange 2010 アカウントの権限を確認する （27 ページ）

関連トピック

Exchange Server 2010
Exchange Server 2013

Exchange 2016 または 2019 の特定のユーザーまたはグループになりすまし権限を設定する

特定のユーザーまたはユーザグループに対して Exchange のなりすまし権限を設定するには、Microsoft Exchange Management Shell (EMS) を使用して以下の手順を実行します。

これらは、Exchange Server 2016 または 2019向けのコマンドと設定です。

手順

ステップ 1 Active Directory にアカウントを作成します。

ステップ 2 コマンドラインを入力するために EMS を開きます。

ステップ 3 EMS で New-ManagementRoleAssignment コマンドを実行して、指定した既存のドメインサービスアカウント (例: *Ex2016*) に他のユーザーアカウントになりすます権限を付与します。

構文

```
New-ManagementRoleAssignment -Name:_suImpersonateRoleAsg -Role:ApplicationImpersonation
-User:user@domain
```

例

```
New-ManagementRoleAssignment -Name:_suImpersonateRoleAsg -Role:ApplicationImpersonation
-User:Ex2016@contoso.com
```

ステップ 4 偽装権限が適用される範囲を定義するには、この New-ManagementRoleAssignment コマンドを実行します。この例では、*Ex2016*アカウントに、指定された Exchange Server 上のすべてのアカウントになりすます権限が付与されます。

構文

```
New-ManagementScope -Name:_suImpersonateScope -ServerList:server_name
```

例

```
New-ManagementScope -Name:_suImpersonateScope -ServerList:nw066b-227
```

ステップ 5 以下の表で定義されている推奨値を使用して、New-ThrottlingPolicy コマンドを実行し、新しいスロットリングポリシーを作成します。

構文

```
New-ThrottlingPolicy -Name:Policy_Name -EwsMaxConcurrency:100 -EwsMaxSubscriptions:NULL
-EwsCutoffBalance3000000-EwsMaxBurst300000-EwsRechargeRate900000
```

例

```
New-ThrottlingPolicy -Name IMP_ThrottlingPolicy -EwsMaxConcurrency 100 -EwsMaxSubscriptionsunlimited
-EwsCutoffBalance 3000000 -EwsMaxBurst 300000 -EwsRechargeRate 900000
```

表 *6 : Exchange Server 2016* または *2019* に推奨されるスロットルポリシー設定

パラメータ[1]	推奨構成値 — Exchange Server 2016 および 2019
EwsCutoffBalance	3000000
EwsMaxBurst	300000
EwsMaxConcurrency	**100**
EwsMaxSubscriptions	無制限
EwsRechargeRate	900000

[1] これらは、Exchange Server 2016 または 2019 で変更できる唯一の EWS パラメーターです。

（注）
サポートされている Exchange SP1 でのみ利用可能です。

ステップ 6 Set-ThrottlingPolicyAssociation コマンドを実行して、新しいスロットリング ポリシーを手順 2 で使用したサービス アカウントに関連付けます。

構文

```
Set-ThrottlingPolicyAssociation -IdentityUsername -ThrottlingPolicyPolicy_Name
```

例

```
Set-ThrottlingPolicyAssociation -Identity ex2016 -ThrottlingPolicy IMP_ThrottlingPolicy
```

次のタスク

Microsoft Exchange 2016 または 2019 アカウントで権限を確認する （29 ページ）

Microsoft Exchange 2010 アカウントの権限を確認する

Exchange 2010 アカウントに権限を割り当てたら、メールボックスレベルで権限が反映され、指定されたユーザーが、メールボックスにアクセスでき、別のユーザーのアカウントになりす

ますことができることを確認する必要があります。 Exchange 2010 では、アクセス許可がメールボックスに反映されるまでに時間がかかります。

これらは Exchange Server 2010 のコマンドです。Exchange Server 2013 を使用している場合は、Microsoft Exchange 2016 または 2019 アカウントで権限を確認する （29 ページ） の手順に従ってください。

手順

ステップ 1 Active Directory サーバーで、なりすましアカウントが存在することを確認します。

ステップ 2 コマンドライン入力のために、Exchange Management Shell (EMS) を開きます。

ステップ 3 Exchange Server で、サービスアカウントに、必要ななりすまし権限が付与されたことを確認します。

a) EMS で以下のコマンドを実行してください。

```
Get-ManagementRoleAssignment -Role ApplicationImpersonation
```

b) コマンド出力で、次のとおり指定されたアカウントに対して、Role ApplicationImpersonation のロール割り当てが行われていることを確認します。

コマンド出力例

名前 - - - -	Role - - -	Role AssigneeName-	Role AssigneeType-
_suImpersonate RoleAs	アプリケーションのなりすまし	ex2010	ユーザ

ステップ 4 サービスアカウントに適用される管理範囲が正しいことを確認してください。

a) EMS で以下のコマンドを実行してください。

```
Get-ManagementScope _suImpersonateScope
```

b) コマンド出力によって、なりすましアカウント名が次のように返されていることを確認します。

コマンド出力例

名前 - - -	Scope RestrictionType	Exclusive	受信者ルート - -	受信
_suImpersonate スコープ	ServerScope	False	ユーザ	直接

ステップ 5 EMS でこのコマンドを実行して、ThrottlingPolicy パラメータが以下の表で定義されている内容と一致していることを確認してください。

```
Get-ThrottlingPolicy -Identity Policy_Name | findstr ^EWS
```

次のタスク

Exchange 仮想ディレクトリで認証を有効にする （30 ページ）

関連トピック

Exchange Server 2010
Exchange Server 2013

Microsoft Exchange 2016 または 2019 アカウントで権限を確認する

Exchange 2016 または 2019 アカウントに権限を割り当てたら、メールボックスレベルで権限が反映され、指定されたユーザーが、メールボックスにアクセスでき、別のユーザーのアカウントになりすますことができることを確認する必要があります。 権限がメールボックスに反映されるまでには時間がかかります。

手順

ステップ 1 Active Directory サーバーで、なりすましアカウントが存在することを確認します。

ステップ 2 コマンドライン入力のために、Exchange Management Shell (EMS) を開きます。

ステップ 3 Exchange Server で、サービスアカウントに、必要ななりすまし権限が付与されたことを確認します。

a) EMS で以下のコマンドを実行してください。

```
Get-ManagementRoleAssignment -Role ApplicationImpersonation
```

b) コマンド出力で、次のとおり指定されたアカウントに対して、Role ApplicationImpersonation のロール割り当てが行われていることを確認します。

コマンド出力例

名前 - - - -	Role - - -	Role AssigneeName-	Role AssigneeType-	割り当て方法 ---	有効なユーザー名
_suImpersonateRoleAs	アプリケーションのなりすまし	ex2016	ユーザ	直接	ex2016

ステップ 4 サービスアカウントに適用される管理範囲が正しいことを確認してください。

a) EMS で以下のコマンドを実行してください。

```
Get-ManagementScope _suImpersonateScope
```

b) コマンド出力によって、なりすましアカウント名が次のように返されていることを確認します。

コマンド出力例

名前 - - -	Scope RestrictionType	Exclusive	受信者ルート - -	受信者フィルター -	Server Filter- - -
_suImpersonateスコープ	ServerScope	False	ユーザ	直接	識別名

ステップ 5 EMS でこのコマンドを実行して、ThrottlingPolicy パラメータが以下の表で定義されている内容と一致していることを確認してください。

```
Get-ThrottlingPolicy -Identity IMP_ThrottlingPolicy | Format-List | findstr ^Ews
```

表 *7 : Exchange Server 2016* または *2019* に推奨されるスロットルポリシー設定

パラメータ[1]	推奨構成値 — Exchange Server 2016 および 2019
EwsCutoffBalance	3000000
EwsMaxBurst	300000
EwsMaxConcurrency	**100**
EwsMaxSubscriptions	無制限
EwsRechargeRate	900000

[1] これらは、Exchange Server 2016 または 2019 で変更できる唯一の EWS パラメーターです。

ステップ 6 Exchange アカウントに ThrottlingPolicy が関連付けられていることを確認してください。

```
Get-ThrottlingPolicyAssociation -Identity  ex2016
```

Exchange 仮想ディレクトリで認証を有効にする

始める前に

Exchange Web Services (EWS) の統合が正しく機能するためには、Exchange Server 2007、2010、および 2013 の EWS 仮想ディレクトリ (/EWS) で、基本認証、Windows 統合認証、またはその両方を有効にする必要があります。

Windows Server 2003 上で動作する Exchange 2007 での認証の有効化

手順

ステップ 1 管理ツールで、**[インターネット情報サービス]** を開き、サーバーを選択します。

ステップ 2 **[ウェブサイト]**を選択します。

ステップ 3 **[デフォルトのウェブサイト]** を選択します。

ステップ 4 **EWS** directory フォルダを右クリックして、**[プロパティ]** を選択します。

ステップ 5 「ディレクトリ セキュリティ」タブを選択してください。

ステップ 6 「認証とアクセス制御」の下にある「編集」をクリックします。

ステップ 7 「認証方法」の下にある次のチェックボックスがオフになっていることを確認してください。

- 匿名アクセスを有効にする

ステップ 8 **[認証方法認証済みアクセス]** で、以下の 2 つのチェックボックスが両方ともオンになっていることを確認します。

- 統合 **Windows** 認証
- 基本認証（パスワードは平文で送信されます）

ステップ 9 **OK**をクリックします。

次のタスク

Exchange Server の証明書構成タスクフロー　(39 ページ)

Windows Server 2016 で実行されている Exchange 2016 または 2019 で認証を有効にする

手順

ステップ 1 管理ツールで、**[インターネット情報サービス]** を開き、サーバーを選択します。

ステップ 2 **[ウェブサイト]**を選択します。

ステップ 3 **[デフォルトのウェブサイト]** を選択します。

ステップ 4 **[EWS]** を選択します。

ステップ 5 [IIS] セクションで、**[認証]** を選択します。

ステップ 6 以下の認証方法が有効になっていることを確認してください。

- 匿名認証
- **Windows** 認証および/または基本認証

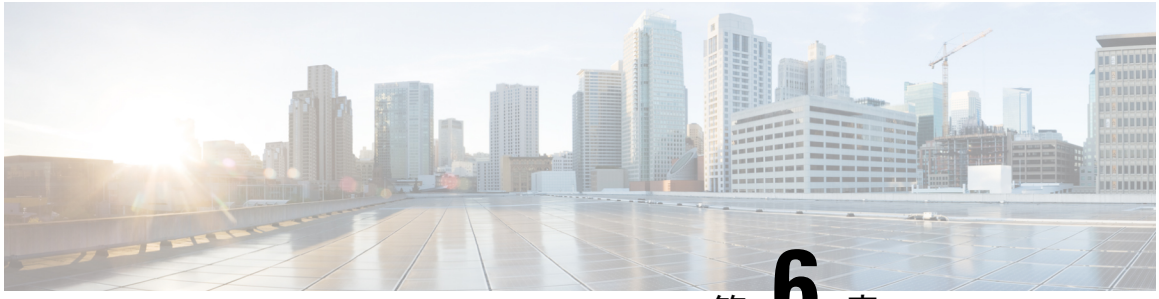
ステップ 7 アクション列の **有効/無効** リンクを使用して、適切に設定してください。

次のタスク

Exchange Server の証明書構成タスクフロー　(39 ページ)

関連トピック

Outlook Web App の仮想ディレクトリの管理
Exchange Web Services 仮想ディレクトリで SSL を有効または無効にする



第 6 章

Microsoft Exchange を構成する

- Microsoft Exchange のカレンダー統合構成 （33 ページ）
- Microsoft Exchange 2016 および 2019 の構成タスクフロー （33 ページ）
- SAN およびワイルドカード証明書のサポート （39 ページ）
- Exchange Server の証明書構成タスクフロー （39 ページ）

Microsoft Exchange のカレンダー統合構成

オンプレミスの Microsoft Exchange Server をデプロイする場合は、この章の手順を実行して、IM and Presence Service と Microsoft Outlook 間のカレンダー連携にむけて Microsoft Exchange を構成します。 IM and Presence Service は、次の各種 Microsoft 導入と統合できます。

表 8 : カレンダーと *IM and Presence Service* の統合に向けた *Microsoft Exchange* 構成

Microsoft Exchange の展開	Microsoft 構成
Microsoft Exchange 2016 または 2019	Microsoft Exchange 2016 および 2019 の構成タスクフロー （33 ページ）

（注） テストは、Microsoft Exchange Server の主要バージョンを使用して実施されます。 このような主要バージョンのそその他の累積更新プログラムについても、互換性が維持されることが期待されています。 例えば、Exchange 2016 について言及する場合、それは IM and Presence Service が Exchange 2016 でリリースされたすべての累積更新プログラム (CU) をサポートしていることを意味します。

Microsoft Exchange 2016 および 2019 の構成タスクフロー

Microsoft Exchange 2016 または 2019 の展開環境において、Outlook カレンダーと IM およびプレゼンス サービスとの統合を構成するには、以下の手順を実行してください。

手順

	コマンドまたはアクション	目的
ステップ 1	Windows のセキュリティ設定を確認する （34 ページ）	Windows 統合認証（NTLM）に関する Windows セキュリティ設定を確認してください。
ステップ 2	リリース用に Exchange の権限を設定します。	• Exchange 2016 または 2019 の特定のユーザーまたはグループになりすまし権限を設定する （26 ページ） 特定のユーザまたはユーザグループに対して、Exchange のなりすまし権限を設定します。
ステップ 3	リリース用の権限を確認します。	• Microsoft Exchange 2016 または 2019 アカウントで権限を確認する （29 ページ） アクセス許可がメールボックスレベルまで伝播し、指定されたユーザがメールボックスにアクセスして他のユーザのアカウントになりすますことができることを確認してください。
ステップ 4	Windows Server 2016 で実行されている Exchange 2016 または 2019 で認証を有効にする （31 ページ）	Exchange Server の EWS 仮想ディレクトリ (/EWS) では、基本認証、Windows 統合認証、またはその両方を有効にする必要があります。
ステップ 5	Exchange Server の証明書構成タスクフロー （39 ページ）	Microsoft Exchange 導入の証明書を構成するには、このタスクフローを完了します。

Windows のセキュリティ設定を確認する

手順

ステップ 1 Windows ドメインコントローラーと Exchange を実行しているサーバーで、**[開始]** > **[管理ツール]** > **[ローカルセキュリティポリシー]** の順に選択します。

ステップ 2 **[セキュリティ設定]** > **[ローカルポリシー]** > **[セキュリティオプション]** の順に選択します。

ステップ 3 **[ネットワークセキュリティ:セキュリティで保護されたRPCを含むNTLM SSPサーバー向けの最小セッションセキュリティ]**を選択します。

ステップ 4 「NTLMv2 セッション セキュリティを要求する」チェックボックスがオフになっていることを確認してください。

ステップ 5 「NTLMv2 セッション セキュリティを要求する」チェックボックスがオンになっている場合は、以下の手順を実行してください。

a) **[NTLMv2セッションセキュリティが必要]** チェックボックスをオフにします。
b) **OK**をクリックします。

ステップ 6 新しいセキュリティ設定を適用するには、Windows ドメインコントローラーと Exchange を実行しているサーバを再起動してください。

（注）
再起動が必要なのは、セキュリティポリシーの設定変更が行われたサーバのみです。

Exchange 2016 または 2019 の特定のユーザーまたはグループになりすまし権限を設定する

特定のユーザーまたはユーザグループに対して Exchange のなりすまし権限を設定するには、Microsoft Exchange Management Shell (EMS) を使用して以下の手順を実行します。

これらは、Exchange Server 2016 または 2019向けのコマンドと設定です。

手順

ステップ 1 Active Directory にアカウントを作成します。

ステップ 2 コマンドラインを入力するために EMS を開きます。

ステップ 3 EMS で New-ManagementRoleAssignment コマンドを実行して、指定した既存のドメインサービスアカウント (例: *Ex2016*) に他のユーザーアカウントになりすます権限を付与します。

構文

```
New-ManagementRoleAssignment -Name:_suImpersonateRoleAsg -Role:ApplicationImpersonation
-User:user@domain
```

例

```
New-ManagementRoleAssignment -Name:_suImpersonateRoleAsg -Role:ApplicationImpersonation
-User:Ex2016@contoso.com
```

ステップ 4 偽装権限が適用される範囲を定義するには、この New-ManagementRoleAssignment コマンドを実行します。この例では、*Ex2016*アカウントに、指定された Exchange Server 上のすべてのアカウントになりすます権限が付与されます。

構文

```
New-ManagementScope -Name:_suImpersonateScope -ServerList:server_name
```

例

```
New-ManagementScope -Name:_suImpersonateScope -ServerList:nw066b-227
```

ステップ 5 以下の表で定義されている推奨値を使用して、New-ThrottlingPolicy コマンドを実行し、新しいスロットリングポリシーを作成します。

構文

```
New-ThrottlingPolicy -Name:Policy_Name -EwsMaxConcurrency:100 -EwsMaxSubscriptions:NULL
-EwsCutoffBalance3000000-EwsMaxBurst300000-EwsRechargeRate900000
```

例

```
New-ThrottlingPolicy -Name IMP_ThrottlingPolicy -EwsMaxConcurrency 100 -EwsMaxSubscriptionsunlimited
-EwsCutoffBalance 3000000 -EwsMaxBurst 300000 -EwsRechargeRate 900000
```

表 *9 : Exchange Server 2016* または *2019* に推奨されるスロットルポリシー設定

パラメータ[1]	推奨構成値 — Exchange Server 2016 および 2019
EwsCutoffBalance	3000000
EwsMaxBurst	300000
EwsMaxConcurrency	**100**
EwsMaxSubscriptions	無制限
EwsRechargeRate	900000

[1] これらは、Exchange Server 2016 または 2019 で変更できる唯一の EWS パラメーターです。

（注）
サポートされている Exchange SP1 でのみ利用可能です。

ステップ 6 Set-ThrottlingPolicyAssociation コマンドを実行して、新しいスロットリング ポリシーを手順 2 で使用したサービス アカウントに関連付けます。

構文

```
Set-ThrottlingPolicyAssociation -IdentityUsername -ThrottlingPolicyPolicy_Name
```

例

```
Set-ThrottlingPolicyAssociation -Identity ex2016 -ThrottlingPolicy IMP_ThrottlingPolicy
```

次のタスク

Microsoft Exchange 2016 または 2019 アカウントで権限を確認する （29 ページ）

Microsoft Exchange 2016 または 2019 アカウントで権限を確認する

Exchange 2016 または 2019 アカウントに権限を割り当てたら、メールボックスレベルで権限が反映され、指定されたユーザーが、メールボックスにアクセスでき、別のユーザーのアカウントになりすますことができることを確認する必要があります。 権限がメールボックスに反映されるまでには時間がかかります。

手順

ステップ 1 Active Directory サーバーで、なりすましアカウントが存在することを確認します。

ステップ 2 コマンドライン入力のために、Exchange Management Shell (EMS) を開きます。

ステップ 3 Exchange Server で、サービスアカウントに、必要ななりすまし権限が付与されたことを確認します。

a) EMS で以下のコマンドを実行してください。

```
Get-ManagementRoleAssignment -Role ApplicationImpersonation
```

b) コマンド出力で、次のとおり指定されたアカウントに対して、Role ApplicationImpersonation のロール割り当てが行われていることを確認します。

コマンド出力例

名前 - - - -	Role - - -	Role AssigneeName-	Role AssigneeType-	割り当て方法 ---	有効なユーザー名
_suImpersonateRoleAs	アプリケーションのなりすまし	ex2016	ユーザ	直接	ex2016

ステップ 4 サービスアカウントに適用される管理範囲が正しいことを確認してください。

a) EMS で以下のコマンドを実行してください。

```
Get-ManagementScope _suImpersonateScope
```

b) コマンド出力によって、なりすましアカウント名が次のように返されていることを確認します。

コマンド出力例

名前 - - -	Scope RestrictionType	Exclusive	受信者ルート - -	受信者フィルター -	Server Filter- - -
_suImpersonateスコープ	ServerScope	False	ユーザ	直接	識別名

ステップ 5 EMS でこのコマンドを実行して、ThrottlingPolicy パラメータが以下の表で定義されている内容と一致していることを確認してください。

```
Get-ThrottlingPolicy -Identity IMP_ThrottlingPolicy | Format-List | findstr ^Ews
```

表 *10 : Exchange Server 2016* または *2019* に推奨されるスロットルポリシー設定

パラメータ[1]	推奨構成値 — Exchange Server 2016 および 2019
EwsCutoffBalance	3000000
EwsMaxBurst	300000
EwsMaxConcurrency	**100**

パラメータ[1]	推奨構成値 — Exchange Server 2016 および 2019
EwsMaxSubscriptions	無制限
EwsRechargeRate	900000
[1] これらは、Exchange Server 2016 または 2019 で変更できる唯一の EWS パラメーターです。	

ステップ 6 Exchange アカウントに ThrottlingPolicy が関連付けられていることを確認してください。

```
Get-ThrottlingPolicyAssociation -Identity  ex2016
```

Windows Server 2016 で実行されている Exchange 2016 または 2019 で認証を有効にする

手順

ステップ 1 管理ツールで、**[インターネット情報サービス]** を開き、サーバーを選択します。

ステップ 2 **[ウェブサイト]**を選択します。

ステップ 3 **[デフォルトのウェブサイト]** を選択します。

ステップ 4 **[EWS]** を選択します。

ステップ 5 [IIS] セクションで、**[認証]** を選択します。

ステップ 6 以下の認証方法が有効になっていることを確認してください。

- **匿名認証**
- **Windows 認証および/または基本認証**

ステップ 7 アクション列の **有効/無効** リンクを使用して、適切に設定してください。

次のタスク

Exchange Server の証明書構成タスクフロー （39 ページ）

関連トピック

Outlook Web App の仮想ディレクトリの管理

Exchange Web Services 仮想ディレクトリで SSL を有効または無効にする

SAN およびワイルドカード証明書のサポート

IM and Presence Service は、Microsoft Exchange との安全なカレンダリング統合に向けて、X.509 証明書を使用します。 IM and Presence Service は、標準証明書に加えて、SAN とワイルドカード証明書をサポートしています。

SAN 証明書を使用すると、X509v3 のサブジェクト代替名フィールドにホスト名、IP アドレス、またはその両方のリストを指定することで、単一の証明書で複数のホスト名と IP アドレスを保護できます。

ワイルドカード証明書を使用すると、ドメイン名にアスタリスク（*）を指定することで、ドメインと無制限のサブドメインを表現できます。名前にはワイルドカード文字「*」を含めることができ、これはドメイン名の任意の単一コンポーネントに一致するものとみなされます。例えば、*.a.com は foo.a.com には一致しますが、bar.foo.a.com には一致しません。

（注） SAN 証明書の場合、保護対象のホストは、サブジェクト代替名フィールドのホスト名/IP アドレスのリストに含まれている必要があります。 Presence Gateway を構成する際は、[Presence Gateway] フィールドは、[サブジェクト代替名] フィールドに一覧されている保護対象ホスト名と完全に一致している必要があります。

ワイルドカードは、標準証明書の場合は共通名（CN）フィールドに、SAN 証明書の場合はサブジェクト代替名フィールドに指定できます。

Exchange Server の証明書構成タスクフロー

Microsoft Exchange 展開用の証明書を構成するには、以下の手順を実行してください。

手順

	コマンドまたはアクション	目的
ステップ 1	お使いの Windows Server のバージョンに認証局（CA）をインストールしてください。 • Windows Server 2003 に CA をインストールする（65 ページ） • Windows Server 2008 に CA をインストールする（40 ページ）	Certificate Authority (CA) は、Exchange Server で実行できますが、CA として別の Windows Server を使用して、サードパーティ証明書交換に拡張されたセキュリティを提供することをお勧めします。
ステップ 2	お使いの Windows Server のバージョンに対応する CSR を生成してください。 • CSR を生成する – Windows Server 2003 での操作（67 ページ）	Exchange 用の証明書署名要求 (CSR) を IIS サーバ上で生成する必要があり、その後、CA サーバによって署名されます。

	コマンドまたはアクション	目的
	• CSR を生成する – Windows Server 2008 での操作 （41 ページ）	
ステップ 3	CA サーバ/認証局への CSR の送信 （42 ページ）	IIS の Exchange 向けに生成されたデフォルトの SSL 証明書は、Exchange Server の完全修飾ドメイン名を使用し、IM and Presence Service が信頼する Certificate Authority によって署名されているはずです。 この手順を実行すると、CA は、Exchange IIS から CSR に署名できるようになります。
ステップ 4	署名済み証明書のダウンロード （44 ページ）	署名済みの証明書のコピーをダウンロードしてください。
ステップ 5	署名済みの証明書を、お使いのバージョンの Windows Server にアップロードしてください。 • 署名済み証明書をアップロードする – Windows 2003 での操作 （71 ページ） • 署名済み証明書をアップロードする – Windows 2008 での操作 （45 ページ）	この手順では、署名済みの CSR を取得し、IIS にアップロードします。
ステップ 6	ルート証明書のダウンロード （46 ページ）	CA サーバからルート証明書をダウンロードしてください。
ステップ 7	IM およびプレゼンスサービスノードにルート証明書をアップロードします。 （46 ページ）	IM and Presence Service にルート証明書をアップロードします。

Windows Server 2008 に CA をインストールする

手順

ステップ 1 **[開始]** > **[管理ツール]** > **[サーバーマネージャ]** の順に選択します。

ステップ 2 コンソールツリーで、 **役割**を選択します。

ステップ 3 **[アクション]** > **[ロールを追加]** の順に選択します。

ステップ 4 **[ロールを追加]** ウィザードを入力します。

a) **[開始する前に]** ウィンドウで、一覧されている前提条件を満たしていることを確認してから、**[次へ]** をクリックします。

b) **[サーバーロールを選択]** ウィンドウで、**[Active Directory証明書サービス]** チェックボックスをオンにして、**[次へ]** をクリックします。

c) **[概要] ウィンドウ**で、**[次へ]** をクリックします。

d) **[ロールサービスを選択]** ウィンドウで、これらのチェックボックスをオンにして、**[次へ]** をクリックします。

- 認証機関
- 認証局ウェブ登録
- オンラインレスポンダー

e) **[セットアップの種類を指定]** ウィンドウで、**[スタンドアロン]** をクリックします。

f) 「CA タイプの指定」ウィンドウで、「ルート CA」をクリックします。

g) 「秘密鍵の設定」ウィンドウで、「新しい秘密鍵の作成」をクリックします。

h) 「CA の暗号化の構成」ウィンドウで、デフォルトの暗号化サービスプロバイダを選択します。

i) 「CA 名の構成」ウィンドウで、CA を識別するための共通名を入力します。

j) **[有効期間を設定]** ウィンドウで、CA 用に生成された証明書の有効期間を設定します。

（注）
認証局は、お客様が指定した有効期限までの有効な証明書のみを発行します。

k) **[証明書データベースを構成]** ウィンドウで、デフォルトの証明書データベースロケーションを選択します。

l) **[インストールの選択肢を確認]** ウィンドウで、**[インストール]** をクリックします。

m) **[インストール結果]** ウィンドウで、すべてのコンポーネントに対して、**「インストール成功」**メッセージが表示されていることを確認したら、**[閉じる]** をクリックします。

（注）
Active Directory証明書サービスが、サーバーマネージャのロールの 1 つとして一覧されていることを確認します。

次のタスク

CSR を生成する – Windows Server 2008 での操作 （41 ページ）

CSR を生成する – Windows Server 2008 での操作

Exchange 用の証明書署名要求 (CSR) を IIS サーバーで生成する必要があります。これは、後で CA サーバーが署名します。

手順

ステップ 1 管理ツールで、**[インターネット情報サービス(IIS)マネージャー]** ウィンドウを開きます。

ステップ 2 IIS マネージャーの左側のペインにある [接続] で、[Exchangeサーバー] を選択します。

ステップ 3 **[サーバー証明書]** をダブルクリックします。

ステップ 4 IIS マネージャーの右ペインにある [アクション] で、**[証明書要求を作成する]** を選択します。

ステップ 5 **[証明書を要求する]** ウィザードを入力します。

a) 「識別名プロパティ」ウィンドウで、次の情報を入力します。

- 「共通名」フィールドに、Exchange Server のホスト名または IP アドレスを入力します。
- **[組織]** フィールドに、自分の会社名を入力します。
- 「組織単位」フィールドに、貴社が所属する組織単位を入力してください。

b) 地理情報を以下のように入力し、**[次へ]** をクリックします。

- 都市/地域
- 州 / 県
- 国 / 地域

（注）
入力する IIS 証明書の共通名は、IM and Presence Service の Presence Gateway の構成に使用され、到達するホスト (URI または IP アドレス) と同一である必要があります。

c) 「暗号化サービスプロバイダのプロパティ」ウィンドウで、既定の暗号化サービスプロバイダを受け入れ、ビット長として「2048」を選択し、「次へ」をクリックします。

d) 「証明書要求ファイル名」ウィンドウで、証明書要求に適したファイル名を入力し、「次へ」をクリックします。

（注）
CSR は拡張子 (.txt など) を付けずに保存します。後でこの CSR を見つける必要があるため、保存場所を覚えておきます。 ファイルを開く際は、メモ帳のみを使用してください。

e) 「リクエスト ファイルの概要」ウィンドウで、情報が正しいことを確認し、「次へ」をクリックします。

f) **[証明書要求を完了する]** ウィンドウで、**[完了]** をクリックします。

次のタスク

CA サーバ/認証局への CSR の送信 （42 ページ）

CA サーバ/認証局への CSR の送信

IIS の Exchange 向けに生成されたデフォルトの SSL 証明書は、Exchange Server の完全修飾ドメイン名を使用し、IM and Presence Service が信頼する Certificate Authority によって署名されているはずです。 この手順を実行すると、CA は、Exchange IIS から CSR に署名できるようになります。 CA サーバーで次の手順を実行し、次の場所で Exchange Server の FQDN を構成します。

- Exchange 証明書。
- **Cisco Unified CM IM およびプレゼンス管理**の Exchange Presence Gateway の [Presence Gateway] フィールド。

始める前に

Exchange Server の IIS 上で CSR を生成します。

手順

ステップ 1 証明書要求ファイルを CA サーバにコピーしてください。

ステップ 2 以下のいずれかの URL を開いてください。

- Windows 2003 または Windows 2008: http://*locall_server*/certserv

または

- Windows 2003: http://127.0.0.1/certserv
- Windows 2008: http://127.0.0.1/certsrv

ステップ 3 **[証明書を要求]** を選択します。

ステップ 4 **[高度な証明書要求]** を選択します。

ステップ 5 **[base-64でエンコードされたCMCまたはPKCS #10ファイルを使用して証明書要求を送信する]** を選択するか、**base-64 でエンコードされた PKCS #7 ファイルを使用して更新要求を送信します。**

ステップ 6 メモ帳などのテキストエディタを使用して、生成した CSR を開きます。

ステップ 7 以下の範囲の情報をコピーします

-----BEGIN CERTIFICATE REQUEST

から以下まで

END CERTIFICATE REQUEST-----

ステップ 8 CSR の内容を証明書要求テキストボックスに貼り付けてください。

ステップ 9 (オプション) デフォルトでは、[証明書テンプレート] ドロップダウンメニューに、管理者テンプレートが設定されていますが、これは、サーバーを認証するために適した有効な署名済み証明書を生成するとは限りません。 エンタープライズルート CA をお持ちの場合は、証明書テンプレートのドロップダウンリストから Web サーバ証明書テンプレートを選択してください。 Web Server certificate テンプレートは表示されない場合があるため、CA 構成をすでに変更済みの場合は、この手順を実行する必要が無い場合があります。

ステップ 10 [送信（Submit）]をクリックします。

ステップ 11 **[管理ツール]** ウィンドウで、**[開始]** > **[管理ツール]** > **[証明書]** > **[認証局]** > **[CA名]** > **[保留中の要求]** の順に選択し、**[証明書認証局]** ウィンドウを開きます。 **[Certificate Authority]** ウィンドウには、[保留中の要求] で送信した要求が表示されます。

ステップ 12 リクエストを右クリックして、以下の操作を実行してください。

- **[すべてのタスク]** に移動します。
- **[問題]** を選択します。

ステップ 13 **[発行済み証明書]** を選択して、証明書が発行されていることを確認します。

次のタスク

署名済み証明書のダウンロード （44 ページ）

署名済み証明書のダウンロード

始める前に

- [自己署名証明書] 証明書署名要求 (CSR) を CA サーバに送信します。
- [サードパーティ証明書] Certificate Authority に CSR を要求します。

手順

ステップ 1 管理ツールで、認証局を開きます。 発行した証明書要求は、[発行済み要求] 領域に表示されます。

ステップ 2 リクエストを右クリックして「開く」を選択します。

ステップ 3 **[詳細]** タブを選択します。

ステップ 4 「ファイルにコピー」を選択してください。

ステップ 5 **[証明書エクスポート]** ウィザードが表示されたら、**[次へ]** をクリックします。

ステップ 6 **[証明書エクスポート]** ウィザードを入力します。

a) **[ファイル形式をエクスポート]** ウィンドウで、**[Base-64でエンコードされたX.509]** を選択し、**[次へ]** をクリックします。

b) **[エクスポートするファイル]** ウィンドウで、証明書を保存する場所を入力し、証明書名に cert.cer を使用し、`c:\cert.cer` を選択します。

c) 「証明書のエクスポート ウィザードの完了」ウィンドウで、概要情報を確認し、エクスポートが成功したことを確認してから、「完了」をクリックします。

ステップ 7 IM and Presence Service を管理するために使用するコンピューターに cert.cer をコピーするか FTP で転送します。

次のタスク

Exchange IIS への署名済み証明書のアップロード （71 ページ）

サーバーの種類に応じた署名済み証明書をアップロードします。

- 署名済み証明書をアップロードする – Windows 2003 での操作 （71 ページ）
- 署名済み証明書をアップロードする – Windows 2008 での操作 （45 ページ）

署名済み証明書をアップロードする – Windows 2008 での操作

この手順では、署名済みの CSR を取得し、IIS にアップロードします。 署名済みの証明書をアップロードするには、IM and Presence Service の管理に使用するコンピューターで次の手順を実行します。

始める前に

【自己署名証明書】署名済みの証明書をダウンロードしてください。

[サードパーティ証明書] Certificate Authority が署名済みの証明書を提供します。

手順

ステップ 1 管理ツールで、**[インターネット情報サービス(IIS)マネージャー]** ウィンドウを開きます。

ステップ 2 IIS マネージャーの左側のペインにある [接続] で、[Exchangeサーバー] を選択します。

ステップ 3 **[サーバー証明書]** をダブルクリックします。

ステップ 4 IIS マネージャーの右ペインにある [アクション] で、**[証明書要求を入力する]** を選択します。

ステップ 5 **[Certificate Authorityのレスポンスを指定する]** ウィンドウで、以下の操作を実行します。

a) 証明書を探すには、省略記号 [...] を選択してください。
b) 正しいパスとファイル名に移動してください。
c) 証明書に分かりやすい名前を入力してください。
d) [OK]をクリックします。 完了した証明書は、証明書一覧に表示されます。

ステップ 6 **[インターネット情報サービス]** ウィンドウで、次の手順を実行して証明書をバインドします。

a) **[デフォルトのウェブサイト]** を選択します。
b) IIS マネージャーの右ペインの [アクション] で、[バインディング] を選択します。

ステップ 7 **[サイトバインディング]** ウィンドウで、次の手順を実行します。

a) **[https]** を選択します。
b) [Edit]を選択します。

ステップ 8 **[サイトバインディングを編集]** ウィンドウで、次の手順を実行します。

a) SSL 証明書のドロップダウンリストから、先ほど作成した証明書を選択してください。 証明書に設定した名前が表示されます。
b) 「OK」をクリックしてください 。

次のタスク

ルート証明書のダウンロード （46 ページ）

ルート証明書のダウンロード

始める前に

署名済み証明書を Exchange IIS にアップロードします。

手順

ステップ 1 CA サーバのユーザインターフェースにログインし、Web ブラウザを開いてください。

ステップ 2 お使いの Windows プラットフォームの種類に応じた URL を開いてください。

a) Windows Server 2008 – https://127.0.0.1/certsrv

ステップ 3 **[CA証明書、証明書チェーンまたはCRLをダウンロード]** を選択します。

ステップ 4 エンコード方式には、 **Base 64**を選択してください。

ステップ 5 **[CA証明書をダウンロード]** をクリックします。

ステップ 6 証明書 **certnew.cer**をローカルディスクに保存します。

ヒント

ルート証明書のサブジェクト共通名 (CN) がわからない場合は、外部の Certificate Management ツールを使用して共通名を検索します。 Windows オペレーティングシステムでは、拡張子が.cer の証明書ファイルを右クリックし、証明書のプロパティを開きます。

次のタスク

IM およびプレゼンスサービスノードにルート証明書をアップロードします。 （46 ページ）

IMおよびプレゼンスサービスノードにルート証明書をアップロードします。

始める前に

- 【自己署名証明書】ルート証明書をダウンロードしてください。
- [サードパーティ証明書] Certificate Authority からルート証明書を要求します。 サードパーティ CA 署名済み Exchange Server 証明書をお持ちの場合、証明書チェーンのすべての CA 証明書を、CiscoUnified Presence Trust 証明書 (cup-trust) として IM and Presence Service にアップロードする必要があります。

手順

ステップ 1 **Cisco Unified CM IM およびプレゼンス管理** で証明書インポートツールを使用して証明書をアップロードします。

以下を経由して証明書をアップロードする:	アクション
Cisco Unified CM IM およびプレゼンス管理の証明書インポートツール。 証明書インポートツールは、 IM およびプレゼンスサービスに信頼証明書をインストールするプロセスを簡素化し、証明書交換の主要な方法です。 このツールを使用すると、Exchange サーバのホスト名とポート番号を指定でき、サーバから証明書チェーンをダウンロードしようと試みます。 承認すると、ツールが欠落している証明書を自動的にインストールします。 （注） この手順では、**Cisco Unified CM IM およびプレゼンス管理**で証明書インポートツールにアクセスする方法と構成する方法の一例について説明します。 カレンダリング統合の特定の種類に向けて Exchange Presence Gateway を構成する際は、**Cisco Unified CM IM およびプレゼンス管理**で証明書インポートツールのカスタマイズバージョンを確認することができます (**Cisco Unified CM IM およびプレゼンス管理**にログインして、**[プレゼンス]** > **[ゲートウェイ]** の順に選択)。	**1.** **[Cisco Unified CM IM およびプレゼンス管理]** ユーザーインタ グインします。 **2.** **[システム]** > **[セキュリティ]** > **[証明書インポートツール]** の順 **3.** 証明書をインストールする証明書信頼ストアとして **[IM and Trust]** を選択します。 これは、Exchange との統合に必要なフ ンの信頼証明書を保存します。 **4.** Exchange Server に接続するには、以下のいずれかの値を入力 • IP アドレス • ホスト名 • FQDN この [ピアサーバー] フィールドに入力する値は、Exchange S ス、ホスト名または FQDN と完全に一致する必要があります **5.** Exchange Server との通信に使用するポート番号を入力してく は、Exchange Server で使用可能なポートと一致している必要 **6.** [送信（Submit）]をクリックします。 ツールの処理が完了すな ついて以下の状態が報告されます。 • Peer Server 到達の可能性ステータス — IM and Presence Se Server に到達 (ping) できるかどうかを示します。 Exchang 態のトラブルシューティング （83 ページ）を参照してく • SSL 接続/証明書検証ステータス — 証明書インポートツー ピアサーバから証明書のダウンロードに成功したかどう よびプレゼンスサービス とリモートサーバとの間に安全 れたかどうかを示します。 SSL 接続証明書の状態に関する ティング （84 ページ）を参照してください。

ステップ 2 証明書インポートツールが、証明書が見つからないことを示している場合 (通常は、Microsoft サーバーで CA 証明書が見つからないことを示します)、**[Cisco Unified OS Admin Certificate Management]** ウィンドウを使用して、CA 証明書を手動でアップロードします。

以下を経由して証明書をアップロードする:	アクション
Cisco Unified IM およびプレゼンス オペレーティング システムの管理 Exchange Server が SSL/TLS ハンドシェイク中に CA 証明書を提供しない場合、証明書インポートツールを使用してそれらの証明書をインポートすることはできません。 この場合、証明書管理ツールを使用して手動で欠落している証明書をインポートする必要があります（[Cisco Unified IM and Presence オペレーティング システム Administration]にログインします。 **[セキュリティ]** > **[Certificate Management]** の順に選択します)。	**1.** **certnew.cer** 証明書ファイルを IM and Presence Service ノードの管るコンピューターにコピーするか、FTP で転送します。 **2.** **Cisco Unified IM and Presence オペレーティング システムのアドレーション**のユーザーインターフェイスにログインします。 **3.** **[セキュリティ（Security）]** > **[証明書管理（Certificate Managem**択します。 **4.** **[証明書リスト]** ウィンドウで、**[証明書をアップロード/証明書チ**択します。 **5.** **[証明書をアップロード/証明書チェーン]** ダイアログボックスが開次の操作を実行します。 • 証明書名のドロップダウンリストから、 **cup-trust**を選択し • 拡張子を付けずにルート証明書名を入力してください。 **6.** **[参照]** をクリックして、**[certnew.cer]** を選択します。 **7.** [ファイルのアップロード（Upload File）]をクリックします。

ステップ 3 証明書インポートツール（ステップ 1 （47 ページ））に戻り、すべてのステータステストが成功したことを確認してください。

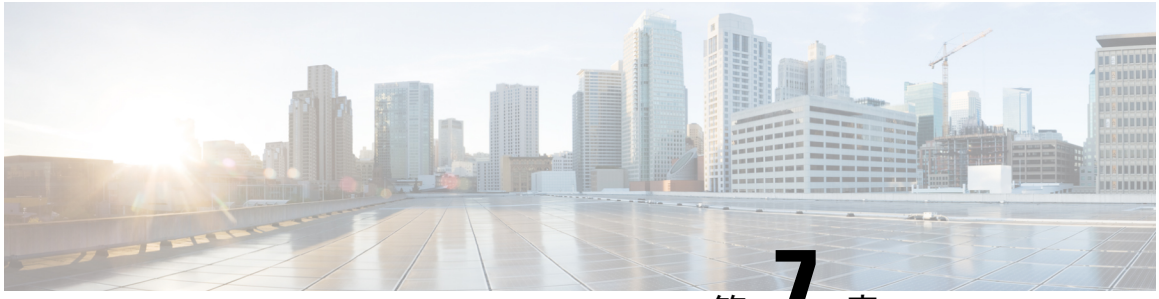
ステップ 4 Exchange の信頼証明書をすべてアップロードしたら、Cisco IM and Presence Engine と SIP プロキシサービスを再起動します。 **Cisco Unified IM and Presence Serviceability** のユーザーインターフェイスにログインします。 **[ツール（Tools）]** > **[コントロール センター - 機能サービス（Control Center - Feature Services）]** の順に選択します。

ヒント

IM and Presence Service では、サブジェクト共通名 (CN) の有無にかかわらず Exchange Server の信頼証明書をアップロードできます。

次のタスク

IM and Presence カレンダー連携タスクフロー （50 ページ）



第 7 章

IM and Presence Service でカレンダー連携を構成する

- カレンダー連携の概要 （49 ページ）
- IM and Presence カレンダー連携タスクフロー （50 ページ）

カレンダー連携の概要

カレンダー連携向けの Microsoft Exchange

IM およびプレゼンスサービスの Microsoft Exchange カレンダー統合機能を使用すると、ユーザの Microsoft Exchange カレンダーと Cisco コラボレーションクライアント（Cisco Jabber など）におけるプレゼンスステータスとの間でシームレスな同期が可能になります。 この連携により、ユーザの空き状況がカレンダーの予定に自動的に反映され、組織全体の同僚にリアルタイムのプレゼンス情報を提供できるようになります。

検証およびサポートは、Microsoft Exchange Server の主要バージョンを使用して実行されます。このような主要バージョンのそその他の累積更新プログラムについても、互換性が維持されることが期待されています。 例えば、Exchange 2016 について言及する場合、それは IM and Presence Service が Exchange 2016 でリリースされたすべての累積更新プログラム (CU) をサポートしていることを意味します。

カレンダー連携向け Microsoft Office 365

IM and Presence Service は、Office 365 がホストする Microsoft Outlook からユーザーカレンダー情報をプルし、それを IM and Presence Service ユーザーのプレゼンスステータスの一部として表示します。

1 つの IM and Presence Service サーバーインスタンスでは、同時進行するカレンダー予定において、最大 7,500 件のプレゼンスステータスの更新がサポートされます。

IM and Presence カレンダー連携タスクフロー

IM and Presence Service でこれらのタスクを完了して、以下の Microsoft 導入のいずれかで、カレンダーと Microsoft Outlook の統合をセットアップします。

- オンプレミスの Microsoft Exchange Server
- ホスト型 Microsoft Office 365 サーバ

手順

	コマンドまたはアクション	目的
ステップ 1	IM and Presence Service に Microsoft 証明書をアップロードする （51 ページ）	IM およびプレゼンスサービスとの統合に必要な Microsoft 証明書をダウンロードしてください。
ステップ 2	プレゼンスゲートウェイの設定 （51 ページ）	IM およびプレゼンスサーバ上で、Exchange サーバまたは Office 365 サーバをプレゼンスゲートウェイとして構成します。
ステップ 3	認証向け Office 365 構成 （53 ページ）	（Office 365 のみ）この手順を使用して、プレゼンスゲートウェイの認証タイプ（現在は OAuth）を設定します。
ステップ 4	Office 365 統合のためのプル間隔の設定 （54 ページ）	（Office 365 のみ）IM およびプレゼンスサービスが Office 365 からカレンダー情報を取得する間隔スケジュールを設定します。デフォルト値は60分です。
ステップ 5	カレンダーの不在情報を設定する （54 ページ）	(オプション)外出中情報を構成して、[外出中] ステータスを表示します。 この設定は、カレンダーサービスが有効になっているかどうかにかかわらず、すべてのユーザに適用されます。 デフォルトは、[外出中の空き状況を表示しない] です。
ステップ 6	Exchange 統合のためのサービスパラメータの設定 （55 ページ）	（Exchange のみ）Microsoft Exchange Server とのカレンダー同期のやり取りを規定するオプションのサービスパラメーターを設定します。
ステップ 7	Cisco Presence Engine を再起動してください。 （56 ページ）	サービスパラメータを編集した場合は、Cisco Presence Engine サービスを再起動してください。
ステップ 8	以下の手順のいずれかを実行して、ユーザーに対してカレンダリングを有効にします。 • 初期 LDAP 同期中にカレンダー機能を有効にする （57 ページ）	ご自分のニーズに適した手順を選択します。 • LDAP 同期がまだ完了していない場合は、LDAP 同期経由でカレンダリングを有効にします。

	コマンドまたはアクション	目的
	• カレンダー連携を一括で有効化する （59 ページ） • ユーザのカレンダー連携を有効にする （60ページ）	• それ以外の場合は、一括管理ツールを使用して、複数のユーザーに対してカレンダリングを構成します。 • または、ユーザーごとにこの機能を有効にします。

IM and Presence Service に Microsoft 証明書をアップロードする

IM and Presence Service と Office 365 の展開環境が通信できるようにするには、IM and Presence Service に Microsoft 証明書をインストールする必要があります。

手順

ステップ 1 Office 365 のルート証明書と中間証明書をダウンロードしてください。

- 以下のサイトには、Office 365 がサポートするすべてのルート証明書と中間証明書の一覧が掲載されています。 https://support.office.com/en-us/article/office-365-certificate-chains-0c03e6b3-e73f-4316-9e2b-bf4091ae96bb

ステップ 2 すべての証明書を、IM and Presence Service の **cup-trust** および **tomcat-trust** ストアにアップロードします。

（注） IM and Presence Service における証明書の詳細については、『*IM and Presence Service* の構成および管理ガイド』の「IM and Presence Service のセキュリティ構成」章を参照してください。

次のタスク

IM and Presence カレンダー連携タスクフロー （50 ページ）

プレゼンスゲートウェイの設定

この手順を使用してプレゼンスゲートウェイを構成し、Microsoft Outlook とのカレンダー統合を設定します。 Presence Gateway として Microsoft Exchange Server または Microsoft Office 365 サーバーのいずれかを割り当てることができます。

手順

ステップ 1 Cisco Unified CM IM and Presence Administration から、以下を選択します。 **[プレゼンス]** > **[ゲートウェイ]**。

ステップ 2 [新規追加] をクリックします。

ステップ 3 **[Presence Gatewayの種類]** フィールドで、次のオプションのいずれかを選択します。

a) オンプレミス Exchange Server と統合する場合は、**[Exchange - - EWS サーバー]** を選択します。

b) ホスト型 Office 365 サーバーと統合する場合は、**[Office 365 サーバー]** を選択します。

[Office 365サーバー] を選択した場合は、デフォルトで、**[認証タイプ]** が、**[OAuth]** になります。

（注）
- **アプリケーション (クライアント) ID**、 **ディレクトリ (テナント) ID**、および **クライアント シークレット** のフィールドは、Office 365 Server にのみ適用されます。

アプリケーション(クライアント)ID、**ディレクトリ(テナント)ID**、および**クライアント シークレット** の値は、Office 365 Server で構成されている値と一致する必要があります。

ステップ 4 **[説明]** フィールドに、Presence Gateway インスタンスを区別するために分かりやすい説明を入力します。

ステップ 5 **[Presence Gateway]** フィールドに、Presence Gateway サーバーの 完全修飾ドメイン名または IP アドレスを入力します。 この値は、サーバ証明書の**サブジェクト共通名（CN）** または**サブジェクト代替名** フィールドに表示されているサーバアドレスと一致する必要があります。

ステップ 6 **[アカウント名]** フィールドに、サーバーにアクセスするアカウント名を入力します。

ステップ 7 **[アカウントパスワード]** および **[確認用パスワード]** フィールドに、サーバーにアクセスするためにアカウントが使用するパスワードを入力します。

ステップ 8 **[Presence Gatewayポート]** フィールドに、カレンダリングサービスに接続するために使用するポートを入力します。 デフォルト ポートは 443 です。

ステップ 9 (Office 365 のみ) **[Presence Gatewayの種類]** が、**[Office 365サーバー]** で、IM and Presence Service に Office 365 サーバーへのアクセス許可がない場合は、**[HTTP/HTTPSプロキシURL]** フィールドに、HTTP/HTTPS プロキシサーバーの詳細を割り当てます。

ステップ 10 (Office 365 のみ) **[HTTP/HTTPSプロキシユーザー名]** フィールドに、HTTP/HTTPS プロキシサーバーにアクセスするユーザー名を入力します。

ステップ 11 (Office 365 のみ) **[HTTP/HTTPSプロキシパスワード]** フィールドに、HTTP/HTTPS プロキシサーバーに対して指定されているユーザー名のパスワードを入力します。

（注）
手順 12 および 13 の設定オプションは、リリース 15SU2 以降で利用可能です。

ステップ 12 (Office 365 のみ) **[AD認証エンドポイント]** フィールドのデフォルト URL は、*https://login.microsoftonline.com* です。 カスタム URL を入力したい場合は、編集アイコンをクリックしてください。

ステップ 13 (Office 365 のみ) **[リソースURI]** フィールドのデフォルト URL は、https://outlook.office365.com です。 リリース 15SU4 以降では、デフォルトの URL は https://graph.microsoft.comです。 カスタム URL を入力したい場合は、編集アイコンをクリックしてください。

ステップ 14 **[保存]** をクリックします。

（注）
セキュアな HTTP 接続を確立するために使用される TLS バージョンの制限を設定する方法の詳細については、『Cisco Unified Communications Manager 用セキュリティ ガイド』を参照してください。

認証向け Office 365 構成

この手順を使用して、プレゼンスゲートウェイの認証タイプ（現在はOAuth）を設定します。

手順

ステップ 1 Microsoft Azure ポータルにログインしてください: https://portal.azure.com。

ステップ 2 新しいアプリケーションを登録し、 **アプリケーション（クライアント）ID** と **ディレクトリ（テナント）ID** を取得するには、次の手順に従ってください。 https://docs.microsoft.com/en-gb/azure/active-directory/develop/quickstart-register-app#register-a-new-application-using-the-azure-portal。

ステップ 3 **クライアントシークレット**を作成するには、**[管理]** で、**[証明書とシークレット]**、 > **[新しいクライアントシークレット]** の順に選択します。 そして、クライアントシークレットの値を取得します。

（注）
Presence Gateway の種類として、Office 365 Server を選択した場合は、Presence Gateway の設定中に同じ値を使用して、IM and Presence Service の **[アプリケーション(クライアント)ID]**、**[ディレクトリ(テナント)ID]** および **[クライアントシークレット]** フィールドを構成します。

ステップ 4 **[管理]** > **[API権限]** > **[権限を追加]** の順に選択し、**[組織が使用するAPI]** で、**[Office 365 Exchange Online]** を選択します。

ステップ 5 アプリケーション権限を追加するには、 **アプリケーション権限** > **権限**を選択し、 **Calendars.ReadBasic.All** チェックボックスをオンにして、 **権限の追加**をクリックします。

（注）
不在情報を取得するには、 **MailBoxSettings.Read** 権限を付与してください。

ステップ 6 管理者の同意を付与するには、**[管理]** > **[API権限]** の順に選択します。

ステップ 7 **[同意を付与]** で、**[「登録済みAzure Active Directory」に管理者の同意を付与する]**、**[はい]** の順に選択します。

ステップ 8 割り当てられた権限の **ステータス** 列に緑色のチェックマークがあるかどうかを確認してください。

Office 365 統合のためのプル間隔の設定

この手順を実行して、IM and Presence Service が Office 365 からカレンダー情報をプルする間隔を構成します。

始める前に

認証向け Office 365 構成 （53 ページ）

手順

ステップ 1 Cisco Unified CM IM およびプレゼンス管理で、**[システム]** > **[サービスパラメータ]** の順に選択します。

ステップ 2 **[サーバー]** ドロップダウンで、[IM and Presenceパブリッシャノード] を選択します。

ステップ 3 **[サービス]** ドロップダウンで、**[Cisco Presence Engine]** を選択します。

ステップ 4 **Office 365 Calendar Information Pull Interval** サービスパラメータの間隔を分単位で構成します。 デフォルトは 60 分です。

ステップ 5 **[保存]** をクリックします。

（注） IM and Presence Service は、**Office 365 Calendar Information Pull Interval** サービスパラメータが指定したスケジュールされた間隔 (デフォルト値は、60 分) で、Office 365 から情報をプルします。 ただし、Office 365 から IM and Presence Service に情報をプッシュする仕組みはありません。 そのため、Office 365 とスケジュールされたプル (たとえば臨時会議) の間でスケジュールされていない Presence の更新が実行された場合は、その結果は、次にスケジュールされているプルが実行されるまで、IM and Presence Service に登録されません。

カレンダーの不在情報を設定する

始める前に

認証向け Office 365 構成 （53 ページ）

手順

ステップ 1 Cisco Unified CM IM およびプレゼンス管理から、**[システム（System）]** > **[サービスパラメータ（Service Parameters）]** を選択します。

ステップ 2 **[サーバー]** ドロップダウンで、[IM and Presenceパブリッシャノード] を選択します。

ステップ 3 **[サービス]** ドロップダウンで、**[Cisco Presence Engine]** を選択します。

ステップ 4 **Calendar Out of Office information** サービスパラメータで、**[外出中の空き状況を表示]** を選択し、ユーザーが、Microsoft Office 365 または Exchange Server でステータスを [外出中] に設定した際に、Cisco Jabber クライアントのユーザーの空き状況のステータスを [外出中] に更新します。

ステップ 5 **[保存（Save）]**をクリックします。

Exchange 統合のためのサービスパラメータの設定

この任意の手順を実行して、Outlook カレンダーと Microsoft Exchange Server の統合向けの任意のサービスパラメータを構成します。 多くのパラメータについては、デフォルト値で十分な場合があります。

手順

ステップ 1 Cisco Unified CM IM およびプレゼンス管理で、**[システム]** > **[サービスパラメータ]** の順に選択します。

ステップ 2 **[サーバー]** ドロップダウンで、[IM and Presenceパブリッシャノード] を選択します。

ステップ 3 **[サービス]** ドロップダウンで、**[Cisco Presence Engine]** を選択します。

ステップ 4 **[カレンダリング構成]**で、次のパラメータの値を構成します。

表 *11 : Exchange* 統合用サービスパラメータ

サービス パラメータ	説明
Microsoft Exchange 通知ポート（Microsoft Exchange Notification Port）	Presence Engine が Exchange Server から送信される通知をリッスンするためのポート番号。 UDP は WebDAV に使用され、TCP は EWS（Exchange Web Services）に使用されます。 指定可能な値は 1024-65535 で、デフォルト値は 50020 です。
カレンダー処理の秒単位の分散時間	このパラメータは、期間の範囲を秒単位で指定します。 各ユーザーには、ハッシュ値に基づいてオフセット時間が割り当てられます。 この時間は、会議の状態遷移通知が毎分の開始時刻から何秒後に送信されるかを決定します。 ユーザー数が少ない場合は、この時間を短縮できます(ユーザー数を100で割った値が秒数の目安です)。 これは WebDAV および EWS（Exchange Web Services）に使用されます。 値の範囲は 0 ～59 で、デフォルト値は 50 秒です。
Exchange タイムアウト（秒）（Exchange Timeout (seconds)）	このパラメーターは、Exchange サーバへのリクエストがタイムアウトするまでの時間を秒単位で指定します。 この変更には、Cisco Presence Engine の再起動が必要です。 設定可能な値の範囲は 1～20 で、デフォルト値は 3 秒です。

サービス パラメータ	説明
Exchange キュー（Exchange Queue）	このパラメータは、Exchange リクエストキューの最大長を指定します。 リクエストが行われた際にキューの長さを超過した場合、リクエストは失敗し、復旧手順が開始されます。 この変更には、Cisco Presence Engine の再起動が必要です。 設定可能な値は 1～5000 で、デフォルト値は 2200 です。
Exchange スレッド（Exchange Threads）	このパラメータは、Exchange リクエストを処理するために使用されるスレッド数を指定します。 ユーザ数が多い場合（例えば 5000 人）、または Exchange のトランザクション処理に 3 秒以上かかる場合は、この値を増やすことができます。 カレンダー連携を無効にする場合は、このパラメータを 1 に設定してください。 この変更には、Cisco Presence Engine の再起動が必要です。 設定可能な値は 1～100 で、デフォルト値は 60 です。
EWS ステータス確認頻度 (分)	このパラメーターは、EWS（Exchange Web Services）を使用している場合に、Exchange サーバから通知メッセージが送信される頻度を指定します。 時間は分単位で設定します。 設定可能な値は 10～1440 で、デフォルト値は 60 です。
FIPS モードでの Exchange Server 認証	このパラメーターは、プレゼンスエンジンが Exchange サーバとの接続を確立するために使用する認証の種類を指定します。 「自動」に設定すると、プレゼンスエンジンはまず NTLMv2 認証をネゴシエートし、NTLMv2 認証が失敗した場合にのみ基本認証にフォールバックします。 FIPS モードでは NTLMv1 はネゴシエートされません。 [Basic のみ] に設定すると、Presence Engine は、Exchange Server が NTLM および Basic の両方を許可するように構成されていても、常に Basic 認証を使用します。 このパラメータは FIPS モードでのみ適用されます。 このパラメータを変更するには、Cisco Presence Engine を再起動する必要があります。 デフォルト値は [自動] です。

ステップ 5 **[保存（Save）]**をクリックします。

次のタスク

Cisco Presence Engine を再起動してください。 （56 ページ）

Cisco Presence Engine を再起動してください。

カレンダー設定サービスのパラメータの値を変更した場合は、Cisco Presence Engine サービスを再起動してください。

手順

ステップ 1 [Cisco Unified IM and Presenceのサービスアビリティ（Cisco Unified IM and Presence Serviceability）] から、**[ツール（Tools）]** > **[コントロールセンター-機能サービス（Control Center - Feature Services）]** を選択します。

ステップ 2 **[サーバー]** ドロップダウンで、[IM and Presence Service] を選択し、**[移動]** をクリックします。

ステップ 3 [IM and Presence サービス（IM and Presence Services）]で、[Cisco Presence Engine]を選択して、[再起動（Restart）]をクリックします。

次のタスク

IM and Presence Service サーバーに対してカレンダリングを有効にします。 多数のユーザに対して一度にこの機能を有効にするには、ユーザが外部のLDAPディレクトリから同期されている場合はLDAP 同期を使用するか、LDAP 以外のユーザの場合は一括管理ツールを使用できます。 あるいは、ユーザごとに個別にこの機能を有効にすることもできます。

- 初期 LDAP 同期中にカレンダー機能を有効にする （57 ページ）
- カレンダー連携を一括で有効化する （59 ページ）
- ユーザのカレンダー連携を有効にする （60 ページ）

初期 LDAP 同期中にカレンダー機能を有効にする

初回LDAPディレクトリ同期の前に、カレンダー機能を有効にするために、以下のタスクを完了してください。 初期 LDAP 同期プロセス中にカレンダリング機能を有効にすると、LDAP ディレクトリからユーザーがインポートされる際に、すべてのユーザーのカレンダリングサービスが自動でプロビジョニングされます。 この設定は、最初の同期を実行する前に構成する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	機能グループテンプレートにカレンダー統合を追加する （58 ページ）	カレンダリングを機能グループテンプレートに割り当てます。
ステップ 2	LDAP 同期に機能グループテンプレートを追加する （58 ページ）	カレンダー対応機能グループテンプレートを LDAP ディレクトリ同期に割り当て、同期を完了します。

機能グループテンプレートにカレンダー統合を追加する

この手順を実行して、Microsoft Outlook のカレンダリング連携を機能グループテンプレートに割り当てます。 このテンプレートを使用すると、Outlook カレンダー連携を、LDAP ディレクトリから同期されたすべてのユーザーに構成できます。

（注） 同期が完了していないLDAPディレクトリに対してのみ、機能グループテンプレートの設定を追加または編集できます。 ディレクトリが既に同期されている場合は、代わりに カレンダー連携を一括で有効化する （59 ページ） を使用してください。

手順

ステップ 1 Cisco Unified CM Administration で、**[ユーザー管理]** > **[ユーザーの電話機/追加]** > **[機能グループテンプレート]** の順に選択します。

ステップ 2 次のいずれかの手順を実行します。

- [新規追加（Add New）] をクリックして新しいテンプレートを作成します。
- [検索（Find）]をクリックし、既存のテンプレートを選択します。

ステップ 3 **[Unified CM IM and Presence に対してユーザーを有効にする]** チェックボックスをオンにします。

ステップ 4 **[プレゼンスにミーティング情報を含める]** チェックボックスをオンにします。

ステップ 5 **機能グループテンプレート** 設定ウィンドウの残りのフィールドを入力してください。 フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

ステップ 6 **[保存（Save）]**をクリックします。

次のタスク

LDAP 同期に機能グループテンプレートを追加する （58 ページ）

LDAP 同期に機能グループテンプレートを追加する

この手順を実行して、作ほど作成したカレンダリング対応機能グループテンプレートを LDAP ディレクトリ同期に割り当てます。 これにより、この LDAP ディレクトリから同期されるすべてのユーザに対して、Outlook カレンダーとの連携を有効にできます。

（注） 機能グループテンプレートは、まだ同期されていない LDAP ディレクトリにのみ追加できます。 ディレクトリが既に同期されている場合は、 カレンダー連携を一括で有効化する （59 ページ） を使用してください。

始める前に

機能グループテンプレートにカレンダー統合を追加する （58 ページ）

手順

ステップ 1 Cisco Unified CM Administration で、**[システム]** > **[LDAP]** > **[LDAPディレクトリ]** の順に選択します。

ステップ 2 **[検索]** をクリックして、既存の LDAP ディレクトリを選択します。

ステップ 3 **[機能グループテンプレート]** ドロップダウンリスト メニューで、前のタスクで作成したカレンダリング対応機能グループテンプレートを選択します。

ステップ 4 [LDAPディレクトリ（LDAP Directory）]ウィンドウで残りのフィールドを設定します。 フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

ステップ 5 **[保存（Save）]**をクリックします。

ステップ 6 **[Perform Full Sync Now（完全同期を今すぐ実施）]** をクリックします。

カレンダー連携を一括で有効化する

一括管理ツールを使用すると、一回の操作で多数のユーザーのカレンダー連携を有効にできます。

（注） 一括管理ツールを使用してカレンダー連携を有効にすると、大量のシステムリソースを消費します。 この操作は、システムのパフォーマンスおよびユーザエクスペリエンスに影響を与える可能性があります。 業務への影響を最小限に抑え、最適なシステムのパフォーマンスを維持するために、この操作は、営業時間外にスケジュールすることをお勧めします。

手順

ステップ 1 Cisco Unified Communications Manager ノードで、**Cisco Unified CM Administration** ユーザーインターフェイスにログインします。

ステップ 2 カレンダー連携を一括で有効化するには、以下のウィンドウから操作できます。

a) **[一括管理]** > **[ユーザー]** > **[ユーザーを挿入]**。

b) **[一括管理]** > **[ユーザー]** > **[ユーザーを更新]** > **[クエリ]**。

c) **[一括管理]** > **[ユーザー]** > **[ユーザーを更新]** > **[カスタムファイル]**。

（注）
各種更新オプションの詳細については、『*Cisco Unified Communications Manager* 向け一括管理ガイド』を参照してください。

ステップ 3 カレンダー連携を有効にするすべてのエンドユーザについて、以下のエンドユーザ設定オプションがチェックされていることを確認してください。

- **[Unified CM IM and Presence のユーザを有効にする（Enable User for Unified CM IM and Presence）]**
- **[プレゼンスに会議情報を含める(Include meeting information in Presence)]**

ステップ 4 csv ファイルから更新する場合は、該当する [ユーザー] 領域でファイル名を選択します。

（注）
[サンプルファイルを表示] をクリックして、正しいファイル形式を確認します。

ステップ 5 **[今すぐ実行]** または **[後で実行]** をクリックします。

ステップ 6 [送信（Submit）]をクリックします。

ユーザのカレンダー連携を有効にする

この手順を実行して、IM and Presence Service ユーザーのカレンダー連携を有効にします。

手順

ステップ 1 **Cisco Unified CM Administration** ユーザーインターフェイスにログインします。

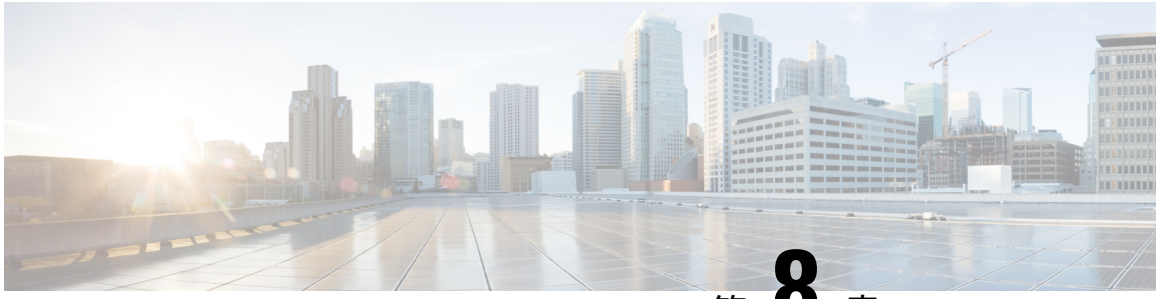
ステップ 2 **[ユーザ管理（User Management）]** > **[エンド ユーザ（End User）]** の順に選択します。

ステップ 3 「検索」をクリックしてエンドユーザを選択します。

ステップ 4 **[Unified CM IM and Presenceに対してユーザーを有効にする]** チェックボックスをオンにします。

ステップ 5 **[プレゼンスにミーティング情報を含める]** チェックボックスをオンにします。

ステップ 6 **[保存（Save）]**をクリックします。



第 8 章

IM and Presence Service をカレンダー統合向けに構成する

- Microsoft Exchange との統合にむけて Presence Gateway を構成する （61 ページ）
- SAN およびワイルドカード証明書のサポート （64 ページ）
- IM and Presence Service と Microsoft Exchange の間にセキュリティで保護された証明書交換を構成する （64 ページ）
- カレンダー統合を有効にする （76 ページ）
- [オプション] Exchange Web Service 経由で送信される Exchange カレンダー通知送信頻度を構成する （78 ページ）
- [オプション] Microsoft Exchange 通知ポートの設定 （79 ページ）
- [オプション] Microsoft Exchange カレンダー通知の期間範囲の設定 （80 ページ）
- その他の Microsoft Exchange カレンダーパラメータ （81 ページ）
- 外出中プレゼンスステータス （81 ページ）

Microsoft Exchange との統合にむけて Presence Gateway を構成する

カレンダー情報の交換を行うには、Exchange Server（Microsoft Outlook）をプレゼンスゲートウェイとして構成する必要があります。 Exchange ゲートウェイを使用すると、IM and Presence Service ノードは、ユーザーごとのユーザーの空き状況情報を反映させます。

プレゼンスゲートウェイを構成する際には、Exchange Server に接続するために以下のいずれかの値を使用できます。

- FQDN (DNS で解決可能)
- IP アドレス

Cisco Unified CM IM およびプレゼンス管理経由で Exchange 連携に向けて Exchange Web Services (EWS) Presence Gateway を構成する際は、次の点に注意します。

- 1 つ以上の EWS サーバを追加、更新、または削除できます。上限はありません。 ただし、[プレゼンス ゲートウェイ構成] ウィンドウのトラブルシューターは、構成した最初の 10 台の EWS サーバの状態を確認して報告するように設計されています。
- EWS サーバゲートウェイは、最初の EWS サーバゲートウェイ用に設定した偽装アカウントの認証情報（アカウント名とパスワード）を共有します。 1 つの EWS サーバゲートウェイの認証情報を変更すると、設定されているすべての EWS ゲートウェイの認証情報もそれに応じて変更されます。
- 1 つ以上の EWS サーバを追加、更新、または削除した後は、設定変更を有効にするために Cisco Presence Engine を再起動する必要があります。 複数の EWS サーバを連続して追加する場合、Cisco Presence Engine を一度再起動するだけで、すべての変更を同時に反映させることができます。

（注）

- SAN 証明書の場合、保護対象のホストは、サブジェクト代替名フィールドのホスト名/IP アドレスのリストに含まれている必要があります。
- Presence Gateway を構成する際は、[Presence Gateway] フィールドは、[サブジェクト代替名]フィールドに一覧されている保護対象ホスト名と完全に一致している必要があります。

Exchange Web Services を介してプレゼンス ゲートウェイとして Exchange 2007、2010、または 2013 を構成する

始める前に

Presence Gateway を構成する前に、IM and Presence Service に有効な証明書チェーンをアップロードする必要があります。

Microsoft Exchanger サーバーに IPv6 経由で接続する場合、enterprise パラメータが IPv6 向けに構成されており、Eth0 が導入環境の各 IM and Presence Service ノードの IPv6 に設定されていることを確認します。 IM and Presence Service で IPv6 を構成する方法については、「*Cisco Unified Communications Manager* での *IM and Presence Service* の構成と管理」を参照してください。

手順

ステップ 1 **[Cisco Unified CM IM およびプレゼンス管理]** ユーザーインターフェイスにログインします。

ステップ 2 **[プレゼンス]** > **[ゲートウェイ]** の順に選択します。

ステップ 3 [新規追加] をクリックします。

ステップ 4 プレゼンスゲートウェイの種類として、 **Exchange -- EWS サーバ** を選択してください。

設定変更を有効にするには、1 つ以上の EWS サーバを追加、更新、または削除した後、Cisco Presence Engine を再起動する必要があります。 複数の EWS サーバを連続して追加する場合、Cisco Presence Engine を一度再起動するだけで、すべての変更を同時に反映させることができます。

ステップ 5 複数の種類のゲートウェイを構成する場合は、Presence Gateway インスタンスの区別がつくような分かりやすい説明を **[説明]** フィールドに入力します。

ステップ 6 [Presence Gateway] フィールドに、Presence Gateway のサーバーロケーションを入力し、これが、サブジェクト共通名 (CN) と一致するか、または Exchange Server 証明書の [サブジェクト代替名] フィールドに入力されていることを確認します。 Exchange Server に接続するには、以下のいずれかの値を使用する必要があります。

- FQDN
- IP アドレス

ワイルドカード証明書で使用するようにプレゼンスゲートウェイを設定するには、指定するノードロケーションの値が、ワイルドカード証明書によって保護されているサブドメインの一部である必要があります。 たとえば、ワイルドカード証明書がサブドメイン `*.imp.cisco.com` を保護する場合は、[Presence Gateway] フィールドに *`server_name`*`.imp.cisco.com` のノード値を入力する必要があります。

（注）
FQDN を入力する場合は、サブジェクト共通名 (CN) と一致するか、証明書チェーンの Exchange Server リーフ証明書の [サブジェクト代替名] フィールドで保護されているホストのいずれかと一致する必要があります。 FQDN は、リクエストを処理し、証明書を使用するアドレスに解決される必要があります。

IPv6 の場合、入力する IPv6 アドレスは、Exchange Server 証明書の SAN フィールドに入力された値と一致している必要があります。

ステップ 7 IM and Presence Service が Exchange Server に接続するために使用するなりすましアカウント名を入力します。これは、ユーザープリンシパル名 (例: user@domain) または下位レベルのログオン名 (例: domain\user) のいずれかの形式で入力します。

ステップ 8 IM and Presence Service に必要な Exchange アカウントパスワードを入力して、Exchange Server に接続します。 確認のためもう一度パスワードを入力します。 この値は、Exchange Server で以前に設定したアカウントのアカウントパスワードと一致している必要があります。

ステップ 9 Exchange Server への接続に使用するポート番号を入力してください。 IM and Presence Service と Exchange は、セキュリティで保護された HTTP 接続経由で統合します。 Cisco は、ポート 443（デフォルトポート）を使用し、他のポートに変更しないことを推奨しています。

ステップ 10 **[保存]** をクリックします。

ステップ 11 以下の項目に対して、Exchange Server のステータスが緑色で表示されていることを確認します。

- **Exchange への到達可能性（ping 可能）**
- **Exchange SSL 接続/証明書の検証**

次のタスク

Exchange Presence Gateway の設定が完了したら、以下の点を確認してください。

- IM and Presence Service と Exchange Server 間で接続が正常に確立されていますか? 「プレゼンス ゲートウェイ構成」ウィンドウの「Exchange Server ステータス」領域には、接続ス

テータスが表示されます。 是正措置が必要な場合は、 Exchange Server の接続状態のトラブルシューティング （83 ページ）を参照してください。

- Exchange SSL 証明書チェーンの状態は正しいですか（検証済みですか）？ **[Presence Gateway 構成]** ウィンドウの Exchange Server ステータスの領域には、証明書サブジェクト CN で不一致があるかどうかが示されます。 是正措置が必要な場合は、 SSL 接続証明書の状態に関するトラブルシューティング （84 ページ）を参照してください。

SAN およびワイルドカード証明書のサポート

IM and Presence Service は、Microsoft Exchange との安全なカレンダリング統合に向けて、X.509 証明書を使用します。 IM and Presence Service は、標準証明書に加えて、SAN とワイルドカード証明書をサポートしています。

SAN 証明書を使用すると、X509v3 のサブジェクト代替名フィールドにホスト名、IP アドレス、またはその両方のリストを指定することで、単一の証明書で複数のホスト名と IP アドレスを保護できます。

ワイルドカード証明書を使用すると、ドメイン名にアスタリスク（*）を指定することで、ドメインと無制限のサブドメインを表現できます。名前にはワイルドカード文字「*」を含めることができ、これはドメイン名の任意の単一コンポーネントに一致するものとみなされます。例えば、*.a.com は foo.a.com には一致しますが、bar.foo.a.com には一致しません。

（注） SAN 証明書の場合、保護対象のホストは、サブジェクト代替名フィールドのホスト名/IP アドレスのリストに含まれている必要があります。 Presence Gateway を構成する際は、[Presence Gateway] フィールドは、[サブジェクト代替名] フィールドに一覧されている保護対象ホスト名と完全に一致している必要があります。

ワイルドカードは、標準証明書の場合は共通名（CN）フィールドに、SAN 証明書の場合はサブジェクト代替名フィールドに指定できます。

IM and Presence Service と Microsoft Exchange の間にセキュリティで保護された証明書交換を構成する

Certificate Authority サービスをインストールする方法

Certificate Authority (CA) は、Exchange Server で実行できますが、CA として別の Windows Server を使用して、サードパーティ証明書交換に拡張されたセキュリティを提供することをお勧めします。

- Windows Server 2003 に CA をインストールする （65 ページ）

• Windows Server 2008 に CA をインストールする （40 ページ）

Windows Server 2003 に CA をインストールする

始める前に

- CA をインストールするには、まず Windows Server 2003 コンピューターにインターネットインフォメーションサービス（IIS）をインストールする必要があります。 IIS は、Windows 2003 のデフォルト インストールではインストールされません。
- Windows Server ディスク 1 と SP1 ディスクが揃っていることを確認してください。

手順

ステップ 1 **[開始]** > **[コントロールパネル]** > **[プログラムの追加と削除]** の順に選択します。

ステップ 2 **[プログラムの追加と削除]** ウィンドウで、**[Windowsコンポーネントの追加と削除]** を選択します。

ステップ 3 **[Windowsコンポーネント]** ウィザードを入力します。

a) **[Windowsコンポーネント]** ウィンドウで、**[証明書サービス]** チェックボックスをオンにし、ドメインのパートナーシップとコンピューターの名前変更制限に関して警告が表示されたら、**[はい]** をクリックします。

b) 「CA タイプ」ウィンドウで「スタンドアロン ルート CA」を選択し、「次へ」をクリックします。

c) **[CA ID情報]** ウィンドウで、CA サーバーの [共通名] フィールドにサーバーの名前を入力します。 DNS がない場合は、IP アドレスを入力して **[次へ]**をクリックします。

（注）
CA は第三者機関であることを覚えておいてください。 CA の共通名は、CSR を生成するために使用された共通名と同じであってはなりません。

d) **[証明書データベース設定]** ウィンドウで、デフォルト設定を許可し、**[次へ]** をクリックします。

ステップ 4 インターネットインフォメーション サービスを停止するように求められたら、「はい」をクリックしてください。

ステップ 5 Active Server Pages (ASP) を有効にするよう求められたら、「はい」をクリックしてください。

ステップ 6 インストールプロセスが完了したら、「完了」をクリックしてください。

次のタスク

CSR を生成する – Windows Server 2003 での操作 （67 ページ）

Windows Server 2008 に CA をインストールする

手順

ステップ 1 **[開始]** > **[管理ツール]** > **[サーバーマネージャ]** の順に選択します。

ステップ 2 コンソールツリーで、 **役割**を選択します。

ステップ 3 **[アクション]** > **[ロールを追加]** の順に選択します。

ステップ 4 **[ロールを追加]** ウィザードを入力します。

a) **[開始する前に]** ウィンドウで、一覧されている前提条件を満たしていることを確認してから、**[次へ]** をクリックします。

b) **[サーバーロールを選択]** ウィンドウで、**[Active Directory証明書サービス]** チェックボックスをオンにして、**[次へ]** をクリックします。

c) **[概要] ウィンドウ**で、**[次へ]** をクリックします。

d) **[ロールサービスを選択]** ウィンドウで、これらのチェックボックスをオンにして、**[次へ]** をクリックします。

- 認証機関
- 認証局ウェブ登録
- オンラインレスポンダー

e) **[セットアップの種類を指定]** ウィンドウで、**[スタンドアロン]** をクリックします。

f) 「CA タイプの指定」ウィンドウで、「ルート CA」をクリックします。

g) 「秘密鍵の設定」ウィンドウで、「新しい秘密鍵の作成」をクリックします。

h) 「CA の暗号化の構成」ウィンドウで、デフォルトの暗号化サービスプロバイダを選択します。

i) 「CA 名の構成」ウィンドウで、CA を識別するための共通名を入力します。

j) **[有効期間を設定]** ウィンドウで、CA 用に生成された証明書の有効期間を設定します。

（注）
認証局は、お客様が指定した有効期限までの有効な証明書のみを発行します。

k) **[証明書データベースを構成]** ウィンドウで、デフォルトの証明書データベースロケーションを選択します。

l) **[インストールの選択肢を確認]** ウィンドウで、**[インストール]** をクリックします。

m) **[インストール結果]** ウィンドウで、すべてのコンポーネントに対して、**「インストール成功」**メッセージが表示されていることを確認したら、**[閉じる]** をクリックします。

（注）
Active Directory証明書サービスが、サーバーマネージャのロールの 1 つとして一覧されていることを確認します。

次のタスク

CSR を生成する – Windows Server 2008 での操作 （41 ページ）

Microsoft Exchange Server の IIS 上で CSR を生成する

CSR を生成する – Windows Server 2003 での操作

Exchange 用の証明書署名要求 (CSR) を IIS サーバーで生成する必要があります。これは、後で CA サーバーが署名します。 証明書にサブジェクト代替名（SAN）フィールドが入力されている場合、それは証明書の共通名（CN）と一致していなければなりません。

始める前に

[自己署名証明書] 必要に応じて証明書 CA サービスをインストールしてください。

手順

ステップ 1 管理ツールで、**[インターネット情報サービス]** を開きます。

a) 右クリック **デフォルトの Web サイト**。

b) **[プロパティ]** を選択します。

ステップ 2 「ディレクトリ セキュリティ」タブを選択してください。

ステップ 3 サーバ証明書を選択してください。

ステップ 4 Web サーバ証明書ウィザードが表示されたら、「次へ」をクリックします。

ステップ 5 サーバ証明書ウィザードを完了してください。

a) **[サーバー証明書]** ウィンドウで、**[新しい証明書を作成]**、**[次へ]** の順に選択します。

b) **[遅延リクエストまたは即時リクエスト]** ウィンドウで、**[リクエストを今すぐ準備するが後で送信する]**、**[次へ]** の順に選択します。

c) **[名前とセキュリティ設定]** ウィンドウで、デフォルトのウェブサイト証明書名を許可し、ビット長として **[1024]** を選択して、**[次へ]** をクリックします。

d) 「組織情報」ウィンドウで、「組織」フィールドに会社名を、「組織単位」フィールドに会社の組織単位を入力し、「次へ」をクリックします。

e) **[サイトの共通名]** ウィンドウで、Exchange Server のホスト名または IP アドレスを入力して、**[次へ]** をクリックします。

（注）
入力する IIS 証明書の共通名は、IM and Presence Service の Presence Gateway の構成に使用され、到達するホスト (URI または IP アドレス) と同一である必要があります。

f) 「地理情報」ウィンドウに、以下のように地理情報を入力し、「次へ」をクリックします。

- 国 / 地域
- 州 / 県

- 市区町村

g) 「証明書要求ファイル名」ウィンドウで、証明書要求に適したファイル名を入力し、CSR を保存するパスとファイル名を指定して、「次へ」をクリックします。

（注）
CSR ファイルは拡張子（.txt など）を付けずに保存し、保存場所を覚えておいてください。後でこの CSR ファイルを見つける必要があるためです。 ファイルを開く際は、メモ帳のみを使用してください。

h) **[リクエストファイルの概要]** ウィンドウで、情報が正しいことを確認し、**[次へ]** をクリックします。

i) 「Web サーバ証明書の完了」ウィンドウで、「完了」をクリックします。

次のタスク

CA サーバ/認証局への CSR の送信 （42 ページ）

CSR を生成する – Windows Server 2008 での操作

Exchange 用の証明書署名要求 (CSR) を IIS サーバーで生成する必要があります。これは、後で CA サーバーが署名します。

手順

ステップ 1 管理ツールで、**[インターネット情報サービス(IIS)マネージャー]** ウィンドウを開きます。

ステップ 2 IIS マネージャーの左側のペインにある [接続] で、[Exchangeサーバー] を選択します。

ステップ 3 **[サーバー証明書]** をダブルクリックします。

ステップ 4 IIS マネージャーの右ペインにある [アクション] で、**[証明書要求を作成する]** を選択します。

ステップ 5 **[証明書を要求する]** ウィザードを入力します。

a) 「識別名プロパティ」ウィンドウで、次の情報を入力します。

- 「共通名」フィールドに、Exchange Server のホスト名または IP アドレスを入力します。
- **[組織]** フィールドに、自分の会社名を入力します。
- 「組織単位」フィールドに、貴社が所属する組織単位を入力してください。

b) 地理情報を以下のように入力し、**[次へ]** をクリックします。

- 都市/地域
- 州 / 県
- 国 / 地域

（注）
入力する IIS 証明書の共通名は、IM and Presence Service の Presence Gateway の構成に使用され、到達するホスト (URI または IP アドレス) と同一である必要があります。

c) 「暗号化サービスプロバイダのプロパティ」ウィンドウで、既定の暗号化サービスプロバイダを受け入れ、ビット長として「2048」を選択し、「次へ」をクリックします。

d) 「証明書要求ファイル名」ウィンドウで、証明書要求に適したファイル名を入力し、「次へ」をクリックします。

（注）
CSR は拡張子 (.txt など) を付けずに保存します。後でこの CSR を見つける必要があるため、保存場所を覚えておきます。 ファイルを開く際は、メモ帳のみを使用してください。

e) 「リクエスト ファイルの概要」ウィンドウで、情報が正しいことを確認し、「次へ」をクリックします。

f) **[証明書要求を完了する]** ウィンドウで、**[完了]** をクリックします。

次のタスク

CA サーバ/認証局への CSR の送信 （42 ページ）

CA サーバ/認証局への CSR の送信

IIS の Exchange 向けに生成されたデフォルトの SSL 証明書は、Exchange Server の完全修飾ドメイン名を使用し、IM and Presence Service が信頼する Certificate Authority によって署名されているはずです。 この手順を実行すると、CA は、Exchange IIS から CSR に署名できるようになります。 CA サーバーで次の手順を実行し、次の場所で Exchange Server の FQDN を構成します。

- Exchange 証明書。
- **Cisco Unified CM IM およびプレゼンス管理**の Exchange Presence Gateway の [Presence Gateway] フィールド。

始める前に

Exchange Server の IIS 上で CSR を生成します。

手順

ステップ 1 証明書要求ファイルを CA サーバにコピーしてください。

ステップ 2 以下のいずれかの URL を開いてください。

- Windows 2003 または Windows 2008: http://*locall_server*/certserv

または

- Windows 2003: http://127.0.0.1/certserv
- Windows 2008: http://127.0.0.1/certsrv

ステップ 3 **[証明書を要求]** を選択します。

ステップ 4 **[高度な証明書要求]** を選択します。

ステップ 5 **[base-64でエンコードされたCMCまたはPKCS #10ファイルを使用して証明書要求を送信する]** を選択するか、**base-64 でエンコードされた PKCS #7 ファイルを使用して更新要求を送信します。**

ステップ 6 メモ帳などのテキストエディタを使用して、生成した CSR を開きます。

ステップ 7 以下の範囲の情報をコピーします

-----BEGIN CERTIFICATE REQUEST

から以下まで

END CERTIFICATE REQUEST-----

ステップ 8 CSR の内容を証明書要求テキストボックスに貼り付けてください。

ステップ 9 (オプション) デフォルトでは、[証明書テンプレート] ドロップダウンメニューに、管理者テンプレートが設定されていますが、これは、サーバーを認証するために適した有効な署名済み証明書を生成するとは限りません。 エンタープライズルート CA をお持ちの場合は、証明書テンプレートのドロップダウンリストから Web サーバ証明書テンプレートを選択してください。 Web Server certificate テンプレートは表示されない場合があるため、CA 構成をすでに変更済みの場合は、この手順を実行する必要が無い場合があります。

ステップ 10 [送信（Submit）]をクリックします。

ステップ 11 **[管理ツール]** ウィンドウで、**[開始]** > **[管理ツール]** > **[証明書]** > **[認証局]** > **[CA名]** > **[保留中の要求]** の順に選択し、**[証明書認証局]** ウィンドウを開きます。 **[Certificate Authority]** ウィンドウには、[保留中の要求] で送信した要求が表示されます。

ステップ 12 リクエストを右クリックして、以下の操作を実行してください。

- **[すべてのタスク]** に移動します。
- **[問題]** を選択します。

ステップ 13 **[発行済み証明書]** を選択して、証明書が発行されていることを確認します。

次のタスク

署名済み証明書のダウンロード （44 ページ）

署名済み証明書のダウンロード

始める前に

- [自己署名証明書] 証明書署名要求 (CSR) を CA サーバに送信します。
- [サードパーティ証明書] Certificate Authority に CSR を要求します。

手順

ステップ 1 管理ツールで、認証局を開きます。 発行した証明書要求は、[発行済み要求] 領域に表示されます。

ステップ 2 リクエストを右クリックして「開く」を選択します。

ステップ 3 **[詳細]** タブを選択します。

ステップ 4 「ファイルにコピー」を選択してください。

ステップ 5 **[証明書エクスポート]** ウィザードが表示されたら、**[次へ]** をクリックします。

ステップ 6 **[証明書エクスポート]** ウィザードを入力します。

a) **[ファイル形式をエクスポート]** ウィンドウで、**[Base-64でエンコードされたX.509]** を選択し、**[次へ]** をクリックします。

b) **[エクスポートするファイル]** ウィンドウで、証明書を保存する場所を入力し、証明書名に cert.cer を使用し、`c:\cert.cer` を選択します。

c) 「証明書のエクスポート ウィザードの完了」ウィンドウで、概要情報を確認し、エクスポートが成功したことを確認してから、「完了」をクリックします。

ステップ 7 IM and Presence Service を管理するために使用するコンピューターに cert.cer をコピーするか FTP で転送します。

次のタスク

Exchange IIS への署名済み証明書のアップロード （71 ページ）

サーバーの種類に応じた署名済み証明書をアップロードします。

- 署名済み証明書をアップロードする – Windows 2003 での操作 （71 ページ）
- 署名済み証明書をアップロードする – Windows 2008 での操作 （45 ページ）

Exchange IIS への署名済み証明書のアップロード

署名済み証明書をアップロードする – Windows 2003 での操作

この手順では、署名済みの CSR を取得し、IIS にアップロードします。 署名済みの証明書をアップロードするには、IM and Presence Service の管理に使用するコンピューターで次の手順を実行します。

始める前に

【自己署名証明書】署名済みの証明書をダウンロードしてください。

[サードパーティ証明書] Certificate Authority が署名済みの証明書を提供します。

手順

ステップ 1 管理ツールから、 **インターネット情報サービス**を開きます。

ステップ 2 **[インターネット情報サービス]** ウィンドウで、次の手順を実行します。

a) **[デフォルトのWebサイト]** を右クリックします。

b) **[プロパティ]** を選択します。

ステップ 3 「既定の Web サイト プロパティ」ウィンドウで、以下の手順を実行します。

a) 「ディレクトリ セキュリティ」タブを選択してください。

b) サーバ証明書を選択してください。

ステップ 4 Web サーバ証明書ウィザードウィンドウが表示されたら、[次へ] をクリックします。

ステップ 5 Web サーバ証明書ウィザードを完了してください。

a) **[保留中の証明書要求]** ウィンドウで、**[保留中の要求を処理して証明書をインストール]** を選択し、**[次へ]** をクリックします。

b) **[保留中の要求を処理]** ウィンドウで、**[参照]** をクリックして、証明書を見つけ、正しいパスとファイル名に移動します。

c) **[SSLポート]** ウィンドウで、SSL ポートに 443 と入力、**[次へ]** をクリックします。

d) **[Webサーバー証明書を完了する]** ウィンドウで、**[完了]** をクリックします。

ヒント

証明書が信頼されている証明書ストアにない場合は、署名済み CSR は信頼されません。 信頼関係を築くために、以下の手順を実行してください。

- **[ディレクトリセキュリティ]** タブで、**[証明書を表示]** をクリックします。
- **[詳細]** > **[ルート証明書を強調表示]** の順に選択し、**[表示]** をクリックします。
- ルート証明書の **[詳細]** タブを選択し、証明書をインストールします。

次のタスク

ルート証明書のダウンロード （46 ページ）

署名済み証明書をアップロードする – Windows 2008 での操作

この手順では、署名済みの CSR を取得し、IIS にアップロードします。 署名済みの証明書をアップロードするには、IM and Presence Service の管理に使用するコンピューターで次の手順を実行します。

始める前に

【自己署名証明書】署名済みの証明書をダウンロードしてください。

[サードパーティ証明書] Certificate Authority が署名済みの証明書を提供します。

手順

ステップ 1 管理ツールで、**[インターネット情報サービス(IIS)マネージャー]** ウィンドウを開きます。

ステップ 2 IIS マネージャーの左側のペインにある [接続] で、[Exchangeサーバー] を選択します。

ステップ 3 **[サーバー証明書]** をダブルクリックします。

ステップ 4 IIS マネージャーの右ペインにある [アクション] で、**[証明書要求を入力する]** を選択します。

ステップ 5 **[Certificate Authorityのレスポンスを指定する]** ウィンドウで、以下の操作を実行します。

a) 証明書を探すには、省略記号 [...] を選択してください。
b) 正しいパスとファイル名に移動してください。
c) 証明書に分かりやすい名前を入力してください。
d) [OK]をクリックします。 完了した証明書は、証明書一覧に表示されます。

ステップ 6 **[インターネット情報サービス]** ウィンドウで、次の手順を実行して証明書をバインドします。

a) **[デフォルトのウェブサイト]** を選択します。
b) IIS マネージャーの右ペインの [アクション] で、[バインディング] を選択します。

ステップ 7 **[サイトバインディング]** ウィンドウで、次の手順を実行します。

a) **[https]** を選択します。
b) [Edit]を選択します。

ステップ 8 **[サイトバインディングを編集]** ウィンドウで、次の手順を実行します。

a) SSL 証明書のドロップダウンリストから、先ほど作成した証明書を選択してください。 証明書に設定した名前が表示されます。
b) 「OK」をクリックしてください 。

次のタスク

ルート証明書のダウンロード （46 ページ）

ルート証明書のダウンロード

始める前に

署名済み証明書を Exchange IIS にアップロードします。

手順

ステップ 1 CA サーバのユーザインターフェースにログインし、Web ブラウザを開いてください。

ステップ 2 お使いの Windows プラットフォームの種類に応じた URL を開いてください。

a) Windows Server 2008 – https://127.0.0.1/certsrv

ステップ 3 **[CA証明書、証明書チェーンまたはCRLをダウンロード]** を選択します。

ステップ 4 エンコード方式には、 **Base 64**を選択してください。

ステップ 5 **[CA証明書をダウンロード]** をクリックします。

ステップ 6 証明書 **certnew.cer**をローカルディスクに保存します。

ヒント

ルート証明書のサブジェクト共通名 (CN) がわからない場合は、外部の Certificate Management ツールを使用して共通名を検索します。 Windows オペレーティングシステムでは、拡張子が.cer の証明書ファイルを右クリックし、証明書のプロパティを開きます。

次のタスク

IM およびプレゼンスサービスノードにルート証明書をアップロードします。 (46 ページ)

IMおよびプレゼンスサービスノードにルート証明書をアップロードします。

始める前に

- 【自己署名証明書】ルート証明書をダウンロードしてください。
- [サードパーティ証明書] Certificate Authority からルート証明書を要求します。 サードパーティ CA 署名済み Exchange Server 証明書をお持ちの場合、証明書チェーンのすべての CA 証明書を、CiscoUnified Presence Trust 証明書 (cup-trust) として IM and Presence Service にアップロードする必要があります。

手順

ステップ 1 **Cisco Unified CM IM およびプレゼンス管理** で証明書インポートツールを使用して証明書をアップロードします。

以下を経由して証明書をアップロードする:	アクション
Cisco Unified CM IM およびプレゼンス管理の証明書インポートツール。 証明書インポートツールは、 IM およびプレゼンスサービスに信頼証明書をインストールするプロセスを簡素化し、証明書交換の主要な方法です。 このツールを使用すると、Exchange サーバのホスト名とポート番号を指定でき、サーバから証明書チェーンをダウンロードしようと試みます。 承認すると、ツールが欠落している証明書を自動的にインストールします。 （注） この手順では、**Cisco Unified CM IM およびプレゼンス管理**で証明書インポートツールにアクセスする方法と構成する方法の一例について説明します。 カレンダリング統合の特定の種類に向けて Exchange Presence Gateway を構成する際は、**Cisco Unified CM IM およびプレゼンス管理**で証明書インポートツールのカスタマイズバージョンを確認することができます (**Cisco Unified CM IM およびプレゼンス管理**にログインして、**[プレゼンス]** > **[ゲートウェイ]** の順に選択)。	**1.** **[Cisco Unified CM IM およびプレゼンス管理]** ユーザーインタ グインします。 **2.** **[システム]** > **[セキュリティ]** > **[証明書インポートツール]** の順 **3.** 証明書をインストールする証明書信頼ストアとして **[IM and Trust]** を選択します。 これは、Exchange との統合に必要なフ ンの信頼証明書を保存します。 **4.** Exchange Server に接続するには、以下のいずれかの値を入力 • IP アドレス • ホスト名 • FQDN この [ピアサーバー] フィールドに入力する値は、Exchange S ス、ホスト名または FQDN と完全に一致する必要があります **5.** Exchange Server との通信に使用するポート番号を入力してく は、Exchange Server で使用可能なポートと一致している必要 **6.** [送信（Submit）]をクリックします。 ツールの処理が完了すな ついて以下の状態が報告されます。 • Peer Server 到達の可能性ステータス — IM and Presence Se Server に到達 (ping) できるかどうかを示します。 Exchang 態のトラブルシューティング （83 ページ）を参照してく • SSL 接続/証明書検証ステータス — 証明書インポートツー ピアサーバから証明書のダウンロードに成功したかどう よびプレゼンスサービス とリモートサーバとの間に安全 れたかどうかを示します。 SSL 接続証明書の状態に関する ティング （84 ページ）を参照してください。

ステップ 2 証明書インポートツールが、証明書が見つからないことを示している場合 (通常は、Microsoft サーバーで CA 証明書が見つからないことを示します)、**[Cisco Unified OS Admin Certificate Management]** ウィンドウを使用して、CA 証明書を手動でアップロードします。

以下を経由して証明書をアップロードする:	アクション
Cisco Unified IM およびプレゼンス オペレーティング システムの管理 Exchange Server が SSL/TLS ハンドシェイク中に CA 証明書を提供しない場合、証明書インポートツールを使用してそれらの証明書をインポートすることはできません。 この場合、証明書管理ツールを使用して手動で欠落している証明書をインポートする必要があります（[Cisco Unified IM and Presence オペレーティング システム Administration]にログインします。 **[セキュリティ]** > **[Certificate Management]** の順に選択します)。	**1.** **certnew.cer** 証明書ファイルを IM and Presence Service ノードの管るコンピューターにコピーするか、FTP で転送します。 **2.** **Cisco Unified IM and Presence オペレーティング システムのアドレーション**のユーザーインターフェイスにログインします。 **3.** **[セキュリティ（Security）]** > **[証明書管理（Certificate Managem**択します。 **4.** **[証明書リスト]** ウィンドウで、**[証明書をアップロード/証明書チ**択します。 **5.** **[証明書をアップロード/証明書チェーン]** ダイアログボックスが開次の操作を実行します。 • 証明書名のドロップダウンリストから、 **cup-trust**を選択し • 拡張子を付けずにルート証明書名を入力してください。 **6.** **[参照]** をクリックして、**[certnew.cer]** を選択します。 **7.** [ファイルのアップロード（Upload File）]をクリックします。

ステップ 3 証明書インポートツール（ステップ 1 （74 ページ））に戻り、すべてのステータステストが成功したことを確認してください。

ステップ 4 Exchange の信頼証明書をすべてアップロードしたら、Cisco IM and Presence Engine と SIP プロキシサービスを再起動します。 **Cisco Unified IM and Presence Serviceability** のユーザーインターフェイスにログインします。 **[ツール（Tools）]** > **[コントロール センター - 機能サービス（Control Center - Feature Services）]** の順に選択します。

ヒント

IM and Presence Service では、サブジェクト共通名 (CN) の有無にかかわらず Exchange Server の信頼証明書をアップロードできます。

次のタスク

IM and Presence カレンダー連携タスクフロー （50 ページ）

カレンダー統合を有効にする

カレンダー連携は、管理者によって個別またはグループ単位で有効化されます。

（注） Cisco Unified Communications Manager で Presence Gateway が設定されていることを確認します。詳細については、Microsoft Exchange との統合にむけて Presence Gateway を構成する （61 ページ） を参照してください。

個人ユーザ向けカレンダー統合の有効化

この手順を使用して、個々のエンドユーザ向けに Microsoft Outlook カレンダーの統合を設定します。

手順

ステップ 1 **Cisco Unified CM Administration** ユーザーインターフェイスにログインします。

ステップ 2 **[ユーザ管理（User Management）] > [エンド ユーザ（End User）]** の順に選択します。

ステップ 3 「検索」をクリックしてエンドユーザを選択します。

ステップ 4 **[Unified CM IM and Presenceに対してユーザーを有効にする]** チェックボックスをオンにします。

ステップ 5 **[プレゼンスにミーティング情報を含める]** チェックボックスをオンにします。

ステップ 6 **[保存（Save）]**をクリックします。

カレンダー連携を一括で有効化する

手順

ステップ 1 Cisco Unified Communications Manager ノードで、**Cisco Unified CM Administration** ユーザーインターフェイスにログインします。

ステップ 2 カレンダー連携を一括で有効化するには、以下のウィンドウから操作できます。

a) **[一括管理] > [ユーザー] > [ユーザーを挿入]**。
b) **[一括管理] > [ユーザー] > [ユーザーを更新] > [クエリ]**。
c) **[一括管理] > [ユーザー] > [ユーザーを更新] > [カスタムファイル]**。

（注）
各種更新オプションの詳細については、『*Cisco Unified Communications Manager* 向け一括管理ガイド』を参照してください。

ステップ 3 カレンダー連携を有効にするすべてのエンドユーザについて、以下のエンドユーザ設定オプションがチェックされていることを確認してください。

- **[Unified CM IM and Presence のユーザを有効にする（Enable User for Unified CM IM and Presence）]**

- **[プレゼンスに会議情報を含める(Include meeting information in Presence)]**

ステップ 4 csv ファイルから更新する場合は、該当する [ユーザー] 領域でファイル名を選択します。

（注）
[サンプルファイルを表示] をクリックして、正しいファイル形式を確認します。

ステップ 5 **[今すぐ実行]** または **[後で実行]** をクリックします。

ステップ 6 [送信（Submit）]をクリックします。

[オプション] Exchange Web Service 経由で送信される Exchange カレンダー通知送信頻度を構成する

（注） この手順は、Microsoft Exchange Server 2007、2010、または 2013 を Exchange Web Services（EWS）経由で統合する場合にのみ適用されます。

EWS Status Frequency パラメータは、Exchange Server が IM and Presence Service のサブスクリプションを更新する間隔を分単位で指定します。デフォルトでは、このパラメータは60分です。IM and Presence Service の Presence Engine が、デフォルト値である 60 分ごとよりも頻繁にサブスクリプションが失われたことを検出するようにしたい場合は、この間隔を短縮します。この間隔を短縮するとエラー検出の精度は向上しますが、Exchange Server と IM and Presence Service ノードの負荷が増加します。

手順

ステップ 1 **[Cisco Unified CM IM およびプレゼンス管理]** ユーザーインターフェイスにログインします。

ステップ 2 **[System（システム）]** > **[Service Parameters（サービス パラメータ）]** を選択します。

ステップ 3 [サーバー] ドロップダウンメニューで、[IM and Presence Service] ノードを選択します。

ステップ 4 「サービス」ドロップダウンリストから「Cisco Presence Engine (アクティブ)」を選択します。

ステップ 5 カレンダー設定（すべてのサーバに適用されるパラメーター）領域で、EWS ステータス頻度フィールドのパラメーター値を編集します。このパラメーターの制限値は1440分です。デフォルトでは、このパラメータは 60 分です。

ステップ 6 **[保存]** をクリックします。

次のタスク

EWS Status Frequency パラメータの変更は、ユーザー単位でカレンダー連携が実行されるにつれて段階的に更新されます。ただし、すべてのユーザに対してパラメータ変更を一度に反映さ

せるには、Cisco Presence Engine を再起動することをお勧めします。 **Cisco Unified IM and Presence Serviceability** のユーザーインターフェイスにログインします。 **[ツール（Tools）]** > **[サービス アクティベーション（Service Activation）]** を選択します。

[オプション] Microsoft Exchange 通知ポートの設定

このトピックは、Cisco Presence Engine が、ネットワーク構成に固有の別のポートで Exchange Server からの受信通知をリッスンするようにする場合にのみ適用されます。

EWS 統合の場合、HTTP 通知を受信するためにデフォルトで TCP ポートが使用されます。

始める前に

デフォルトポートから変更する場合は、割り当てる代替ポートが他で使用されていないことを確認します。

手順

ステップ 1 **[Cisco Unified CM IM およびプレゼンス管理]** ユーザーインターフェイスにログインします。

ステップ 2 **[System（システム）]** > **[Service Parameters（サービス パラメータ）]** を選択します。

ステップ 3 [サーバー] ドロップダウンメニューで、[IM and Presence Service] ノードを選択します。

ステップ 4 「サービス」ドロップダウンリストから「Cisco Presence Engine (アクティブ)」を選択します。

ステップ 5 カレンダー構成領域で、Microsoft Exchange 通知ポート フィールドのパラメーター値を編集し、[保存] をクリックします。

次のタスク

すべてのユーザに対してパラメータ変更を一度に反映させるには、Cisco Presence Engine を再起動することをお勧めします。 **Cisco Unified IM and Presence Serviceability** のユーザーインターフェイスにログインします。 **[ツール（Tools）]** > **[コントロール センター - 機能サービス（Control Center - Feature Services）]** の順に選択します。

ヒント

- デフォルトポートから変更した場合、Cisco Presence Engine は、ユーザーの Exchange サブスクリプションが更新されるまで、ユーザーごとの既存のカレンダー情報 (会議数、開始時刻、終了時刻など) を引き続き使用します。 Cisco Presence Engine がユーザのカレンダーの変更通知を受信するまでには、最大 1 時間かかる場合があります。
- すべてのユーザに一度に変更を適用するには、Cisco Presence Engine を再起動することをお勧めします。

[オプション] Microsoft Exchange カレンダー通知の期間範囲の設定

Cisco Presence Engine では、デフォルトで、分始めから 50 秒後に会議またはビジー通知を送信することができます。 ユーザ数が少ない場合は、この手順で指定されている計算式を使用して、この遅延時間を短縮することをお勧めします。 ただし、この項目はオプションであり、ネットワーク構成に特有の理由で期間範囲を変更したい場合にのみ適用されることに注意してください。

始める前に

このフィールド値 (秒単位) を構成するには「割り当てられたユーザーの最大数/100」の式を使用します。たとえば、ノートの最大ユーザー数が、1000 の場合、オフセット値は、10 秒です。

手順

ステップ 1 **[Cisco Unified CM IM およびプレゼンス管理]** ユーザーインターフェイスにログインします。

ステップ 2 **[System（システム）] > [Service Parameters（サービス パラメータ）]** を選択します。

ステップ 3 [サーバー] ドロップダウンメニューで、[IM and Presence Service] ノードを選択します。

ステップ 4 「サービス」ドロップダウンリストから「Cisco Presence Engine (アクティブ)」を選択します。

ステップ 5 [カレンダー設定] 領域で、[カレンダー配信] フィールドのパラメータ値を編集します。 このパラメータの制限値は 59 秒です。 会議の開始または終了が 1 分以上遅れると、会議の開始/終了カウンターや通知に支障をきたします。 デフォルトでは、このパラメータは 50 です。

ステップ 6 **[保存]** をクリックします。

次のタスク

Calendar Spread パラメータの変更は、ユーザーごとにカレンダー連携が発生すると更新されます。 ただし、すべてのユーザに対してパラメータ変更を一度に反映させるには、Cisco Presence Engine を再起動することをお勧めします。 **Cisco Unified IM and Presence Serviceability** にログインします。 **[ツール（Tools）] > [コントロール センター - 機能サービス（Control Center - Feature Services）]** の順に選択します。

ヒント 非常に多くのユーザが会議に参加または退出すると、一斉通知イベントが発生し、一部の通知が数分遅れる場合があります。

その他の Microsoft Exchange カレンダーパラメータ

Cisco Unified CM IM およびプレゼンス管理の **[サービスパラメータ]** ウィンドウで構成できる Exchange カレンダーパラメータは他に 3 つあります。

- Exchange タイムアウト（秒）— Exchange サーバへのリクエストがタイムアウトするまでの期間（秒単位）。
- Exchange キュー — リクエストキューの長さ。
- Exchange スレッド — Exchange リクエストを処理するために使用されるスレッドの数。

注意 これらのパラメーターのデフォルト設定を変更することはお勧めしません。変更すると、Exchange との連携に悪影響を及ぼす可能性があるためです。 サポートが必要な場合は、Cisco Technical Assistance Center (TAC) にお問い合わせください。

外出中プレゼンスステータス

IM and Presence Service は、ユーザーの空き状況のステータスとして、外出中 (OOO) をサポートしています。 その結果、Microsoft Outlook で外出中通知を特定の期間設定すると、Jabber プレゼンスステータスは、**[退席中]** または **[オフライン]** ではなく、**[外出中]** として表示されます。

さらに、ユーザーのステータス情報を収集する際のユーザーエクスペリエンスを向上させ、外出中であることを不在期間の開始日と終了日とともに他のユーザーに伝えやすくなります。 これにより、ユーザのプレゼンス状態をより明確かつ正確に提供することでインスタントメッセージングシステムを強化し、ユーザエクスペリエンスを向上させることができます。

さらに、カスタムプレゼンス設定を使用して不在時のプレゼンスステータスを上書きし、必要に応じてアクティブ状態と不在状態を切り替えることができます。 これにより、緊急の連絡や重要な会議をより効果的に処理できるようになります。 したがって、MS Exchange Server と Office 365 サーバーの両方をサポートしているため、オンプレミス型とクラウド型のカレンダリングサービスの間に生じるギャップを解消します。

例えば、顧客サポート担当リーダーのジョン・スミスは休暇を取るため、Office 365 で外出中通知を 20XX 年 12 月 10 日 8 時 から 20XX 年 12 月 20 日 23 時 までの期間に設定しました。この機能を実装すると、12 月 10 日に Jabber での彼のプレゼンスステータスは、状況に応じて、[アクティブ]/[退席中]/[オフライン] と表示され、「*2019* 年 *3* 月 *10* 日 *10:00 GMT* ～ *2019* 年 *3* 月 *12* 日 *18:00 GMT* まで外出中です」というメッセージが表示されます。 利用可能状況アイコンはオレンジ色に変わります（オフライン時を除く）。 12 月 14 日、ジョンは上司から電話を受け、緊急の技術的問題に対処するため、Jabber を使った業務上重要な会議に参加するよう依頼された。 この IM and Presence Service の新機能を使用すると、ジョンは、一時的に不在ステータスをオーバーライドでき、手動で空き状況のステータスを [アクティブ] に切り替え、お客様

とのミーティングに参加できるようになります。 会議が終了すると、彼は予定されている休暇期間が終了するまで、プレゼンスステータスを [OOO] に切り替えることができます。

Jabber と WebEx Teams における不在通知

MS Exchange や Office 365 などのカレンダリングサービスで外出中を構成すると、IM and Presence Service は定義されたポーリング間隔中に不在通知を取得し、プレゼンスステータスを [外出中] として表示します。 この期間中は、利用可能状況アイコンがオレンジ色で表示されます。 これは、現地のタイムゾーンでの不在時間を表示します。たとえば、メッセージには、「*2019* 年 *3* 月 *10* 日 *10:00 GMT* ～ *2019* 年 *3* 月 *12* 日 *18:00 GMT* まで外出中です」と表示されます。 また、メッセージのローカライズも処理します。

ただし、外出期間中にオフラインになっている場合は、ステータスは [オフライン] となり、不在通知メッセージも表示されます。

IM およびプレゼンス管理コンソールで不在通知を有効にする

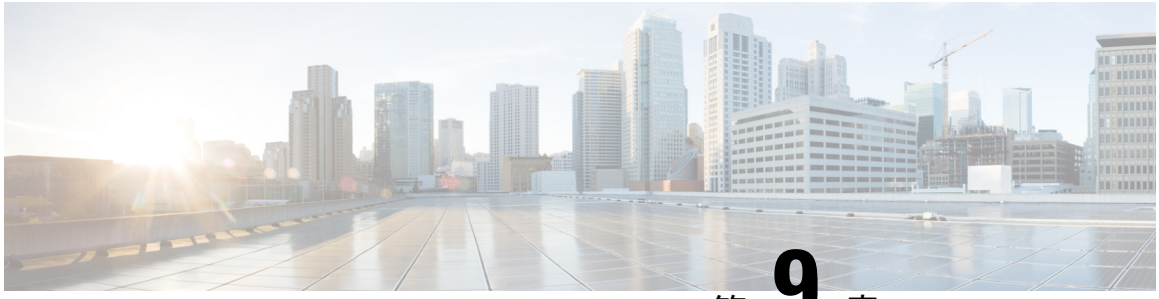
Cisco Presence Service の Calendar Out of Office Information パラメータを使用すると、IM クライアントアプリケーションで外出中の空き状況のステータスの表示を有効または無効にできます。 IM およびプレゼンスノードで不在通知を有効にするには、以下の手順を実行してください。

（注） マルチモードの IM and Presence 導入のあるノードで不在通知オプションを有効にすると、クラスターの他のノードにも適用されます。

1. Cisco Unified CM IM およびプレゼンス管理コンソールで、**[システム]** > **[サービスパラメータ]** の順に選択します。
2. [サービスパラメータ] 設定ページで、IM and Presence ノードがデプロイされている**サーバー**を選択します。
3. **[サービス]** フィールドで、**[Cisco Presence Engine]** を選択します。
4. **[カレンダリング構成(すべてのサーバー適用されるパラメータ)]** セクションで、**[カレンダーの外出中情報]** フィールドを **[外出中の空き状況を表示]** に設定します。 これはデフォルトで実行されます。
5. **[保存]** をクリックします。

外出中のの空き状況情報の表示を無効にするには、**[カレンダーの外出中情報]** フィールドで **[外出中の空き状況を表示しない]** を選択し、**[保存]** をクリックします。 これにより、クラスタ内のすべての IM およびプレゼンスノードでサービスが無効になります。

（注） この変更を行った後は、PE サービスを再起動する必要があります。



第 9 章

Exchange 予定表統合のトラブルシューティング

- Exchange Server の接続状態のトラブルシューティング （83 ページ）
- SSL 接続証明書の状態に関するトラブルシューティング （84 ページ）
- Microsoft Exchange との統合に影響を与えることが知られている問題 （87 ページ）

Exchange Server の接続状態のトラブルシューティング

Exchange Presence Gateway を Exchange Web Services (EWS) カレンダーリング統合用に設定すると、Exchange Server の接続状態が、**Cisco Unified CM IM およびプレゼンス管理**に表示されます (**[プレゼンス]**、 > **[ゲートウェイ]** の順に選択)。 **[Presence Gateway構成]** ウィンドウの [Exchangeサーバーステータス] 領域では、IM and Presence Service と Exchange Server 間の接続のステータスが表示されます。

（注） EWS サーバーは、上限なく 1 台または複数台を追加、更新、削除できます。 ただし、**[Presence Gateway構成]** ウィンドウの [Exchangeサーバーステータス] 領域は、構成した最初の 10 台の EWS サーバーのステータスのみを確認して報告するように設計されています。

.

テスト	ステータスの説明と推奨される処置
Exchange への到達可能性（ping 可能）	IM and Presence Service が、正常に Exchange Server に到達 (p

テスト	ステータスの説明と推奨される処置
Exchange への到達可能性（到達不能）	IM and Presence Service は、Exchange Server に到達できませんで か、またはお客様のネットワークに問題 (ケーブル接続など) が なっている可能性があります。 これを解決するには、ネットワークを介して Exchange Server に フィールドに適切な値 (FQDN または IP アドレス) が設定されて [プレゼンス ゲートウェイ（Presence Gateway）] フィールド値を ん。 Exchange Server との接続に問題がある場合は、**Cisco Unified CM** テム トラブルシューティング ツールを参照するか、推奨される 「システムトラブルシューター」を選択してください。 >

SSL 接続証明書の状態に関するトラブルシューティング

Exchange Web Services (EWS) カレンダリング統合 (**[プレゼンス]** > **[ゲートウェイ]** の順に選択) 向けに Exchange Presence Gateway を構成する際、**Cisco Unified CM IM およびプレゼンス管理** に SSL接続/証明書検証ステータスが表示されます。 「プレゼンス ゲートウェイ構成」ウィンドウの Exchange Server ステータス領域には、証明書のサブジェクト CN の不一致または SAN の不一致があるかどうかが表示されます。

（注） 1 つ以上の EWS サーバを追加、更新、または削除できます。上限はありません。 ただし、**[Presence Gateway]** ウィンドウのトラブルシューティングツールは、構成した最初の 10 の EWS サーバーのステータスのみを検証して報告します。

テスト	ステータスの説明と推奨される処置
SSL 接続/証明書の確認成功	IM およびプレゼンスサービスは、Exchange Server との SSL 接続 て、証明書の詳細を表示します。

テスト	ステータスの説明と推奨される処置

SSL 接続/証明書の確認に失敗：証明書がチェーンに見つからない
 	
（注）
この手順では、カスタマイズされた証明書のインポートツールのビューについて説明します。接続ステータスを確認するだけの場合は、ツールには確認済みのステータスが示されますが、**保存**するオプションはありません。
	Exchange Server へのセキュアな接続を確立するために IM and
	ありません。 証明書ビューアを使用すると、欠落している証
	
	欠落している証明書を表示するには、証明書ビューアを使用
	1. **[構成]** を選択して証明書ビューアーを開きます。
	2. **[証明書チェーンを受け入れる]** チェックボックスをオンに
	3. **[保存]** をクリックします。
	4. 証明書チェーンの詳細が表示されます。 ステータスが [見
	書き留めておきます。
	5. 証明書ビューアを閉じます。
	
	証明書チェーンを完成させるには、次の手順を実行します。
	1. Exchange Server から不足している証明書ファイルをダウン
	2. IM and Presence Service を管理する目的に使用しているコン
	または FTP 転送します。
	3. **[Cisco Unified IM and Presence OS Administration]** を使用し
	ます。
	
	トラブルシューティングのヒント
	• 証明書ビューアーに証明書が無い場合は、次のように、E
	ウンロードしてインストールし、これらの証明書を **Cisco**
	プロードする必要があります。
	  • **Cisco Unified IM and Presence OS Administration** にと
	  をアップロードして、証明書チェーンを完了します。
	  • **[Presence Gateway構成]** ウィンドウに戻り、**Cisco Un**
	  インターフェイスで、証明書ビューアーを再度開き、
	  [検証済み] になっているかを確認します。
	• Exchange の信頼証明書をアップロード後、Cisco Presence
	• Cisco Unified IM and Presence Serviceability のユーザインタ
	• **[ツール]**、 > **[サービスのアクティベーション]** の順に選択
	る可能性があることに注意してください。
	• **[構成]** または **[表示]** のいずれかを選択して、証明書チェ
	ら IM and Presence Service がダウンロードする証明書チェ
	れます。 例えば、上記で説明した証明書が見つからない
	インポートし、確認すると、SSL 接続/証明書確認ステー
	りに **[表示]** ボタンが表示されます。

テスト	ステータスの説明と推奨される処置
SSL 接続/証明書の確認失敗 - 件名 CN が一致しない	[プレゼンス ゲートウェイ（Presence Gateways）] フィールドの値 名 CN 値と一致している必要があります。 この問題は、[プレゼン ルドに正しい値を入力することで解決できます。 次の手順を実行して、[Presence Gateway] フィールドの入力値が正 **1.** 「プレゼンスゲートウェイ」フィールドに、正しいサブジェ Presence Service では、[プレゼンスゲートウェイ（Presence Ga に ping を送信します。 入力したホスト（FQDN または IP ア 完全に一致している必要があります。 **2.** **[保存]** をクリックします。 ヒント **[構成]** または **[表示]** のいずれかを選択して、証明書チェーンビュー Server からダウンロードした証明書チェーンに問題がある場合に 書が見つからないシナリオなどが挙げられます。 証明書チェーン 書確認ステータスが [検証済み] に更新され、**[構成]** ボタンの代わ
SSL 接続/証明書の確認失敗 - SAN が一致しない	「プレゼンスゲートウェイ」フィールドの値は、証明書チェーン内 値のいずれかと一致する必要があります。 この問題は、[プレゼン ルドに正しい値を入力することで解決できます。 次の手順を実行して、[Presence Gateway] フィールドの入力値が正 **1.** 「プレゼンスゲートウェイ」フィールドに正しい SAN 値を再 は、[プレゼンスゲートウェイ（Presence Gateway）] フィール す。 入力したホスト（FQDN または IP アドレス）は、証明書 と完全に一致する必要があります。 **2.** **[保存]** をクリックします。 ヒント **[構成]** または **[表示]** のいずれかを選択して、証明書チェーンビュー Server からダウンロードした証明書チェーンに問題がある場合に 書が見つからないシナリオなどが挙げられます。 証明書チェーン 書確認ステータスが [検証済み] に更新され、**[構成]** ボタンの代わ

テスト	ステータスの説明と推奨される処置
SSL 接続/証明書の検証エラー - 証明書に問題があります	証明書に不正な情報が含まれているため、その証明書が無効に 通常、この問題は、証明書が必要な件名 CN と一致しているも す。 これは、Exchange Server が証明書を再生成しても、 IM ま 保持している場合に発生する可能性があります。 これを解決するには、次の操作を実行します。 • ログを選択して、このエラーの原因を特定します。 • エラーの原因が不正な署名である場合は、古い証明書を C and Presence Service から削除し、Cisco Unified IM and Prese ドする必要があります。 • エラーの原因がサポートされていないアルゴリズムにあ Administration で、サポートされているアルゴリズムを含 す。
SSL 接続/証明書の検証に失敗しました - ネットワークエラー	応答なしによるタイムアウトなどのネットワーク上の問題が 続を確認できません。 Exchange Server へのネットワーク接続を確認し、Exchange Se 接続を受け入れていることを確認することをお勧めします。
SSL 接続/証明書の確認に失敗	不明確な原因または IM and Presence Service が到達可能性テス た。 デバッグ ログ ファイルを参照して詳細を確認することを推奨

Microsoft Exchange との統合に影響を与えることが知られている問題

このセクションでは、Microsoft Exchange Server 2007、2010、および 2013 に共通または固有の既知の問題について説明します。

カレンダー統合における規模の制限

Cisco Unified Communications Manager IM and Presence Service と Exchange カレンダリング連携は、カレンダーのプレゼンスをサブスクライブするユーザーが最大 X%、およびカレンダーの切り替え (ミーティングへの同時参加、退出など) を同時に行うユーザーが最大 Y% などの条件で検証されます。 Cisco Unified Presence の特定のリリースに関するパーセンテージ値については、以下の表を参照してください。

表 *12 : Cisco Unified Presence* の特定のリリースにおける規模の制限

ソフトウェアリリース	カレンダーのプレゼンスをサブスクライブしているユーザーの割合	同時にカレンダーを切り替えるユーザー合
8.5(1)	50	30
8.5(2) 以降	100	50

ユーザが Microsoft Exchange サーバ間を移動した場合、カレンダーの状態が更新されない。

問題

Exchange 管理者が Exchange 連携目的で、ユーザーをある Exchange Server から別の Exchange Server に移動した場合、カレンダリングステータスの変更は、そのユーザーには更新されません。

原因

この現象は、Exchange Server がユーザが 1 つのサーバから別のサーバに移動されたことを通知しないために発生します。

ソリューション

IM and Presence Service 管理者またはユーザーは、Exchange 管理者が、ある Exchange Server から別の Exchange Server にユーザーを移動した後に、カレンダー連携無効にし、再度有効化する必要があります。

LDAP ユーザの削除は、IM およびプレゼンスサービスに反映されるまでに少なくとも 24 時間かかります。

問題

LDAP からユーザーが削除された場合、CiscoUnified Communications Manager でユーザーのステータスが [非アクティブ] に変更され、その後クライアントアプリケーションでユーザーの認証に失敗します。 ただし、テスト中に CiscoUnified Communications Manager が LDAP からの変更を同期した場合、同期後 24 時間経過しても (管理者が強制的に同期した場合でも、特定の時間に同期をスケジュールした場合でも)、ユーザーが削除されないことが確認されました。

IM およびプレゼンス サービス上の Cisco Sync Agent は、ユーザが削除されるまで、ユーザの状態変更を同期しません。 それまでは、そのようなユーザーは、CiscoUnified Communications Manager とすべての IM and Presence Service 機能 (Exchange カレンダリング サブスクリプションを含む) に依然として存在し、そのユーザーのライセンスは 24 時間有効でした。 この遅延により、LDAP からユーザが削除される前に Cisco Jabber にログインしていたユーザは自動的

にログアウトされません。 ユーザーの以前の既存のカレンダーステータス (応答可能、ビジー) は、ユーザーがクライアントからログアウトするまで IM and Presence Service で保持されます。

原因

この状態は、Cisco Unified Communications Manager がセットアップされ、LDAP 認証が使用されている場合に発生します。 LDAP からユーザーが削除されると、そのユーザーのカレンダリング サブスクリプションは、少なくとも 24 時間は、IM and Presence Service で引き続き確立、更新されます。

ソリューション

LDAP からユーザーを削除する場合は、そのユーザーのライセンスを手動で削除することで、IM and Presence Service が、Exchange カレンダリング サブスクリプションを即座に終了し、クライアントアプリケーションからユーザーをログアウトさせることができます。 それ以外の場合は、24 時間程度の遅延が発生する可能性があることにご注意ください。

Microsoft Exchange Server URL にカレンダー向けにローカライズされた単語が含まれていることを確認する

カレンダー統合をローカライズする場合は、Exchange Server の URL にカレンダーを表すローカライズされた単語が含まれていることを確認してください。

手順

ステップ 1 IM and Presence Service と Cisco Unified Communications Manager の両方に同じ言語ロケールをインストールします (ロケールインストーラをロードします)。 IM and Presence Service へのロケールのインストールについては、「カレンダー連携に対するマルチリンガルサポートの構成」を参照してください。

ステップ 2 IM and Presence Service ノードを再起動し、Cisco Unified CM IM and Presence Administration ユーザインターフェイスにログインします。

ステップ 3 カレンダリング向けに別のロケールをサポートする既存の Exchange Presence Gateway を検索して削除します (**[プレゼンス]** > **[ゲートウェイ]**の順に選択)。

ステップ 4 新しい Exchange プレゼンス (Outlook) ゲートウェイを追加します。 [新規追加] をクリックします。

ステップ 5 データベース (pebackendgateway テーブル) で、localecalendarname 属性がインストールされている言語ロケールに対応していることを確認します。

ステップ 6 ロケールが両方の IM and Presence Service にインストールされた後、必要に応じて、Cisco Unified Communications Manager でユーザーロケールを切り替えて、ユーザーロケールが設定されていることを確認します。

Microsoft Exchange Server URL にカレンダー向けにローカライズされた単語が含まれていることを確認する

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。