IM and Presence Service on Cisco Unified Communications Manager, Release 9.1(1) 向け Microsoft Exchange

初版：2012 年 12 月 20 日

最終更新：2012 年 12 月 20 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/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。 このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。 このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。 添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。 シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

このマニュアルで使用している IP アドレスは、実際のアドレスを示すものではありません。 マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。 説明の中に実際のアドレスが使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2013 Cisco Systems, Inc. All rights reserved.

目 次

IM and Presence と Microsoft Exchange との統合 1

IM and Presence での Microsoft Exchange 予定表のステータス 1

プレゼンス ゲートウェイのオプション 2

Windows セキュリティ ポリシーの設定 2

Windows セキュリティ ポリシーの確認 3

証明書のサポート 3

WebDAV 経由での Microsoft Exchange 2003 および 2007 との統合 4

WebDAV インターフェイス経由での Exchange 統合の概要 4

Exchange 2003 および 2007 の管理役割と権限 4

この統合に伴う既知の問題 5

Exchange Web サービス（EWS）経由での Microsoft Exchange 2007/2010 との統合 5

EWS インターフェイス経由での Exchange 統合の概要 5

Exchange Server 2007 および 2010 の管理役割と権限 6

Microsoft Exchange Server 2007/2010 との統合向けのプレゼンス ゲートウェイの設定 7

この統合に伴う既知の問題 8

必要な設定タスク 8

追加情報 9

WebDAV 経由での Microsoft Exchange 2003/2007 Server と IM and Presence の統合 11

Microsoft Exchange 2003 設定チェックリスト（WebDAV） 11

Exchange 2003 アカウントの権限の確認 14

Microsoft Exchange 2007 設定チェックリスト（WebDAV） 14

Exchange 2007 アカウントの権限の確認 17

Exchange 2003/2007 仮想ディレクトリの認証の有効化 19

Exchange Web サービス（EWS）経由での Microsoft Exchange Server 2007/2010 と IM and Presence の統合 21

Microsoft Exchange 2007 設定チェックリスト（EWS） 21

Exchange 2007 アカウントの権限の確認 29
Microsoft Exchange 2010 設定チェックリスト（EWS） 30
Exchange 2010 アカウントの権限の確認 32
Exchange 2007/2010 仮想ディレクトリの認証 33
Windows Server 2003 がインストールされた Exchange 2007 での認証の有効化 34
Windows Server 2008 がインストールされた Exchange 2010 での認証の有効化 35
Microsoft Exchange Server との統合における IM and Presence の設定 37
Microsoft Exchange との統合向けのプレゼンス ゲートウェイの設定 37
WebDAV のプレゼンス ゲートウェイの設定 38
EWS のプレゼンス ゲートウェイの設定 40
予定表の統合の有効化 42
[オプション] EWS での Microsoft Exchange 予定表通知の頻度の設定 43
[オプション] 予定表と統合する場合の多言語サポートの設定 44
Cisco Unified Communications Manager へのロケール インストーラのインストール 44
IM and Presence へのロケール インストーラのインストール 45
多言語の予定表と統合する場合のユーザ ロケールの設定 47
[オプション] Microsoft Exchange 通知ポートの設定 49
[オプション] Microsoft Exchange 予定表通知の接続時間の設定 50
その他の Microsoft Exchange パラメータ 51
IM and Presence と Microsoft Exchange 間のセキュアな証明書交換 53
自己署名証明書およびサードパーティ証明書の交換の管理 53
認証局（CA）サービスのインストール 55
Windows Server 2003 への CA のインストール 56
Windows Server 2008 への CA のインストール 57
Exchange サーバの IIS での CSR の生成 59
CSR の生成（Windows Server 2003） 59
CSR の生成（Windows Server 2008） 60
CA サーバ/認証局への CSR の提出 61
署名付き証明書のダウンロード 63
署名付き証明書の Exchange IIS へのアップロード 64
署名付き証明書のアップロード（Windows 2003） 64

署名付き証明書のアップロード（Windows 2008） 65
ルート証明書のダウンロード 66
ルート証明書の IM and Presence サーバへのアップロード 67
Exchange 予定表の統合のトラブルシューティング 71
Exchange サーバの接続ステータスに関するトラブルシューティング 71
SSL 接続と証明書のステータスのトラブルシューティング 72
Microsoft Exchange の統合に影響することが確認されている問題 78
予定表の統合に関する規模の上限 79
ユーザが Exchange サーバ間で移動すると、予定表ステータスが更新されない 79
LDAP ユーザの削除が IM and Presence にレプリケートされるまで 24 時間以上かかる 80
WebDAV による予定表の統合に関するローカリゼーションの補足説明 81
Exchange サーバに「Calendar」の訳語が含まれているかどうかの確認 81
Microsoft のホットフィックス KB841561 の適用 82
Exchange 2007 から「HTTP 503 サービス利用不可（HTTP 503 Service Unavailable）」エラーを解決する 82
会議通知のサポート 84

第 1 章

IM and Presence と Microsoft Exchange との統合

- IM and Presence での Microsoft Exchange 予定表のステータス，1 ページ
- Windows セキュリティ ポリシーの設定，2 ページ
- 証明書のサポート，3 ページ
- WebDAV 経由での Microsoft Exchange 2003 および 2007 との統合，4 ページ
- Exchange Web サービス（EWS）経由での Microsoft Exchange 2007/2010 との統合，5 ページ
- 必要な設定タスク，8 ページ
- 追加情報，9 ページ

IM and Presence での Microsoft Exchange 予定表のステータス

Microsoft Exchange と IM and Presence Service の統合では、Microsoft Outlook の予定表/会議のステータスを IM and Presence のアベイラビリティ ステータスに組み込むことができます。 次の表は、到達可能性のマッピングと、IM and Presence において会議ステータス（Microsoft Outlook 予定表に表示される）と IM and Presence のユーザのアベイラビリティ ステータスがどのように対応付けられるかを示しています。

表 *1*：予定表ステータスに基づく集約されたアベイラビリティ ステータス

Microsoft Outlook のステータス	IM and Presence のステータス
空き時間/仮の予定	利用可能
ビジー	アイドル/ビジー

Microsoft Outlook のステータス	IM and Presence のステータス
不在[1] 退席中[2]	退席中

1 Microsoft Oulook 2003 および 2007
2 Microsoft Outlook 2010

プレゼンス ゲートウェイのオプション

予定表情報を交換するためには、Microsoft Exchange サーバ（Microsoft Outlook）をプレゼンス ゲートウェイとして設定する必要があります。 IM and Presence サーバは、Exchange ゲートウェイによってアベイラビリティ情報（予定表/会議ステータス）をユーザ単位でアベイラビリティ ステータスに反映できます。

プレゼンス ゲートウェイを設定すると、次のいずれかの値を使用して Microsoft Exchange サーバと接続できます。

- FQDN
- IP アドレス

Windows セキュリティ ポリシーの設定

Cisco Unified Presence は Exchange との統合で、Windows 統合認証（NTLM）を含む、さまざまな認証方式をサポートします。

（注） Cisco Unified Presence は、NTLMv1 Windows 統合認証のみをサポートし、現時点では、NTLMv2 をサポートしていません。

ある Windows ネットワーク セキュリティ ポリシーが NTLMv2 認証を許可している場合、Cisco Unified Presence と Exchange 間の統合が（WebDAV および EWS の両方で）機能しなくなります。 NTLMv2 認証が Exchange を稼働しているすべての Windows サーバで無効になっていることを必ず確認してください。 NTLMv2 認証が有効になっている場合、設定を無効にして、適切に新しいセキュリティ設定を適用するためにサーバを再起動します。

NTLM 認証の現在の設定値を確認し、必要な場合は、NTLMv2 認証を無効にするために、次の手順を実行してください。

Windows セキュリティ ポリシーの確認

手順

ステップ 1 Exchange が稼働している Windows サーバ上で、[スタート（Start）] > [管理ツール（Administrative Tools）] > [ローカル セキュリティ ポリシー（Local Security Policy）] をクリックします。

ステップ 2 [セキュリティ設定（Security Settings）] > [ローカル ポリシー（Local Policies）] > [セキュリティ オプション（Security Options）] に移動します。

ステップ 3 [ネットワーク セキュリティ：セキュア RPC を含むサーバー ベースの NTLM SSP 最小のセッション セキュリティ（Network Security: Minimum session security for NTLM SSP based (including secure RPC) servers）] をクリックします。

ステップ 4 [NTLMv2 セッション セキュリティが必要（Require NTLMv2 session security）] チェックボックスがオフになっていることを確認します。

ステップ 5 [NTLMv2 セッション セキュリティが必要（Require NTLMv2 session security）] チェックボックスがオンになっている場合は、次の手順を実行します。

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

b) [OK] を選択します。

ステップ 6 新しいセキュリティ設定を適用するには、Exchange が稼働している Windows サーバをリブートします。

証明書のサポート

IM and Presence では、Microsoft Exchange と予定表の統合においてセキュアな認証を行うために、X.509 証明書を使用します。 IM and Presence ではサブジェクトの別名（SAN）およびワイルドカード証明書に加え、標準的な証明書もサポートします。

SAN 証明書を使用すると、複数のホスト名と IP アドレスを単一の証明書で保護できるようになります。これを行うには、ホスト名や IP アドレスの一覧を [X509v3 サブジェクトの別名（X509v3 Subject Alternative Name）] フィールドで指定します。

（注） SAN 証明書については、保護されたホストが [サブジェクトの別名（Subject Alternative Name）] フィールドのホスト名/IP アドレスのフィールド一覧に含まれている必要があります。

ワイルドカード証明書を使用すると、ドメインと無制限のサブドメインを保護できるようになります。これを行うには、ドメイン名にアスタリスクを指定します。 名前にはワイルドカード文字 * を含めることができます。ワイルドカードは単一のドメイン名コンポーネントに対応します。たとえば、`*.a.com` は `foo.a.com` と一致しますが、`bar.foo.a.com` とは一致しません。

（注） ワイルドカードは、標準証明書の共通名（CN）と、SAN 証明書のサブジェクトの別名に使用することができます。

WebDAV 経由での Microsoft Exchange 2003 および 2007 との統合

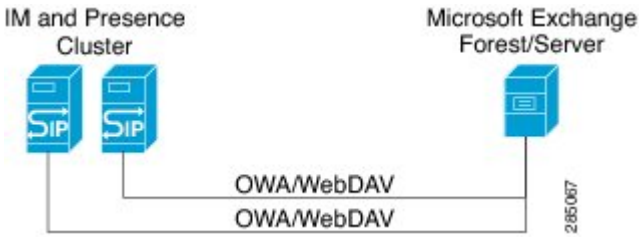
- WebDAV インターフェイス経由での Exchange 統合の概要, （4 ページ）
- Exchange 2003 および 2007 の管理役割と権限, （4 ページ）
- 次の作業, （5 ページ）

WebDAV インターフェイス経由での Exchange 統合の概要

Microsoft Exchange サーバ（バージョン 2003 および 2007）は、WebDav による予定表の統合をサポートしています。図 1：Microsoft Exchange と IM and Presence アーキテクチャとの統合, （4 ページ） に、Microsoft Exchange サーバ（2003 および 2007 バージョン）と IM and Presence を Exchange サーバの WebDAV インターフェイス上で Outlook Web Access（OWA）プロトコルを使用して統合する方法について説明します。

IM and Presence は、1 つの WebDav フロントエンド Exchange サーバとのみ通信できます。 Exchange フロントエンド サーバは、ユーザが Webdav のセットアップ時に設定する複数の Exchange バックエンド サーバと通信します。 Microsoft Exchange は、IM and Presence 上の Exchange サーバ向けに設定されたプレゼンス ゲートウェイを通じて IM and Presence と通信します。

図 1：*Microsoft Exchange* と *IM and Presence* アーキテクチャとの統合



Exchange 2003 および 2007 の管理役割と権限

Microsoft Exchange 2003 および 2007 のデフォルト状態では、管理者は Exchange サーバのユーザ メールボックスにサインインする権限は拒否されます。 IM and Presence が Exchange サーバ上のメールボックス ストアに接続し、エンドユーザの予定表データを照会するためには、「Receive As」アカウントと呼ばれる、特別な権限を持つ Exchange アカウントが必要です。

次の作業

WebDAV 経由での Microsoft Exchange 2003/2007 Server と IM and Presence の統合, （11 ページ）

この統合に伴う既知の問題

WebDAV による統合に影響することが明らかになっている問題については、このガイドの「トラブルシューティング」のセクションを参照してください。Microsoft Exchange の統合に影響することが確認されている問題, （78 ページ）を参照してください。

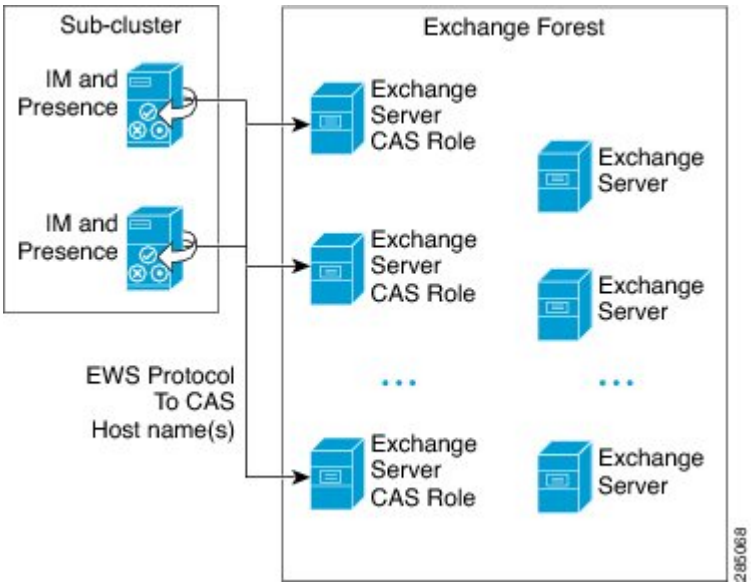
Exchange Web サービス（EWS）経由での Microsoft Exchange 2007/2010 との統合

- EWS インターフェイス経由での Exchange 統合の概要, （5 ページ）
- Exchange Server 2007 および 2010 の管理役割と権限, （6 ページ）
- Microsoft Exchange Server 2007/2010 との統合向けのプレゼンス ゲートウェイの設定, （7 ページ）
- この統合に伴う既知の問題, （8 ページ）

EWS インターフェイス経由での Exchange 統合の概要

Microsoft Exchange 2007 では、WedDAV による統合以外にも Exchange Web サービス（EWS）による予定表の統合を利用できます。ここでは Exchange サーバに対して SOAP に似たインターフェイスが使用されます。 Microsoft Exchange 2010 では、WebDAV のサポートは廃止されているため、予定表の統合を行うには EWS しか使用できません。

（注） 会議通知機能は、Exchange と Microsoft Exchange 2003 または 2007 との統合が WebDAV 経由で行われる場合にのみ使用できます。



Exchange Server 2007 および 2010 の管理役割と権限

すべてのユーザ アカウントにアクセスするために WebDAV アクセスに特別なアカウントが必要であるのと同じように、EWS でも同様の機能が必要となります。 EWS は、指定アカウントに対して「役割」を割り当てることで、この機能を管理します。 この役割は偽装権限を持っています。

Microsoft Exchange Server 2007

呼び出し元が Exchange 2007 サーバ上の別のユーザの電子メール アカウントにアクセスするには、EWS の統合には偽装権限を持つアカウントが必要となります。 呼び出し元は、呼び出し元のアカウントと関連付けられた権限ではなく、偽装したアカウントに関連付けられた権限を使用し、指定したユーザ アカウントを偽装します。

偽装したアカウントには、Exchange 2007 を実行するクライアント アクセス サーバ（CAS）の **ms-Exch-EPI-Impersonation** 権限を付与する必要があります。 これで、CAS サーバを使用してユーザの電子メール アカウントを偽装する権限が呼び出し元に与えられます。 さらに、呼び出し元は、メールボックスデータベースとディレクトリ内の個々のユーザオブジェクトのいずれかに対する **ms-Exch-EPI-MayImpersonat**e 権限も取得する必要があります。

個々のユーザのアクセス コントロール リスト（ACL）がメールボックス データベース設定に優先するため、呼び出し元に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、必要に応じて同じ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できます。

Microsoft Exchange Server 2010

Microsoft Exchange Server 2010 は、ロールベース アクセス コントロール（RBAC）を使用して偽装アカウントに権限を付与し、ユーザに組織での職務に関連するタスクの実行を許可します。 RBAC 権限を適用するには主に 2 つの方法があり、ユーザが管理者またはスーパー ユーザであるかエンドユーザであるかによって使い分けます。

- 管理役割グループ：Exchange のセットアップ プロセス中に 11 のデフォルト管理役割グループが提示されます。各グループには、その役割に固有の権限が関連付けられています。組み込まれている役割グループの例として、「受信者の管理」と「ヘルプデスク」があります。一般に、特定のタスクを実行する必要があるスーパーユーザには適切な管理役割グループが割り当てられ、それに関連付けられた権限を継承します。たとえば、Exchange 組織内の任意のユーザの連絡先情報を修正する必要のある製品サポート担当者は、「ヘルプデスク」管理役割グループのメンバーとして割り当てられます。
- 管理役割割り当てポリシー：管理者またはスーパーユーザではない一般ユーザの場合、管理役割割り当てポリシーは、ユーザが修正できるメールボックスの種類を制御します。**New-ManagementRoleAssignment** コマンドレットを使用してユーザに **ApplicationImpersonation** 役割を割り当てると、アカウントが組織内のユーザを偽装し、そのユーザの代わりにタスクを実行できます。役割の割り当て範囲は、**New-ManagementScope** コマンドレットを使用して個別に管理され、特定の受信者やサーバを対象として絞り込むことができます。

（注） RBAC では、Exchange Server 2007 で求められるように ACL を修正および管理する必要はありません。

Microsoft Exchange Server 2007/2010 との統合向けのプレゼンス ゲートウェイの設定

多数のユーザをサポートするには（EWS での予定表の統合が有効になった状態で）、IM and Presence Service は複数の CAS サーバ間で EWS トラフィックの負荷を分散する必要があります。IM and Presence は EWS 経由でいくつかの CAS サーバと通信し、ラウンド ロビン戦略を使用してトラフィック負荷に対処します。

- 最初にユーザの予定表購読を有効にしたときには、そのユーザには管理者によって設定された対象 CAS ホストのプールから CAS が割り当てられます。
- ユーザへの割り当ては、そのユーザの予定表購読が失敗するまで保持されます。
- ユーザの予定表購読が失敗した場合は、対象 CAS ホストのプールから CAS サーバが再度割り当てられます。
- IM and Presence が中間証明書チェーンを信頼できるよう、各 CAS には独自の中間証明書が必要です。

（注） IM and Presence の本リリースでは、Microsoft Exchange の自動検出サービスに対応していません。自動検出サービスでは、負荷分散機能がすでに CAS サーバに配置されていることが前提となっています。

IM and Presence の管理での Exchange の統合向けに EWS プレゼンス ゲートウェイを設定する場合は、次の点を念頭に置いておいてください。

- WebDAV サーバと EWS サーバの混在環境を展開することはできません。 1 つの WebDAV サーバと 1 つ以上の EWS サーバ ゲートウェイのいずれかを設定する必要があり、両方を設定することはできません。
- 1 台以上の 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（Presence Gateway）] ウィンドウの [トラブルシューター（Troubleshooter）] は、設定した最初の 10 台までの EWS サーバのステータスのみを検証し、レポートするよう作られています。
- EWS サーバ ゲートウェイは、最初の EWS サーバ ゲートウェイに対して設定したクレデンシャル（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 ゲートウェイのクレデンシャルを変更すると、設定されたすべての EWS ゲートウェイのクレデンシャルもそれに準じて変更されます。
- 1 つ以上の EWS サーバを追加、更新、または削除した後に設定の変更を反映するには、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した場合は、すべての変更を同時に反映するよう Cisco Presence Engine を一度だけ再起動することができます。

次の作業

Exchange Web サービス（EWS）経由での Microsoft Exchange Server 2007/2010 と IM and Presence の統合, （21 ページ）

この統合に伴う既知の問題

EWS による統合に影響することが明らかになっ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」を参照してください。

Microsoft Exchange の統合に影響することが確認されている問題, （78 ページ）を参照してください。

必要な設定タスク

Microsoft Exchange の IM and Presence への統合を設定する前に、次の互換性マトリクスを参照し、統合に必要なコンポーネントのインストールおよび設定が完了していることを確認してください。

表 *2*：互換性マトリクス

コンポーネント	互換性のあるバージョン
Windows Server	• Windows Server 2003 の最新のサービス パック（SP2） • Windows Server 2008 の最新のサービス パック（SP2）

コンポーネント	互換性のあるバージョン
Cisco Unified Communications Manager	リリース 9.0(1) 以上
IM and Presence	リリース 9.0(1) 以上
Microsoft Exchange Server 2003	Microsoft Exchange 2003 の最新のサービス パック（SP2）
Microsoft Exchange Server 2007	Microsoft Exchange 2007 の最新のサービス パック（SP1）
Microsoft Exchange Server 2010	Microsoft Exchange 2010 の最新のサービス パック（SP1）
Active Directory	• Active Directory 2003 と Windows Server 2003（SP2） -- または -- • Active Directory 2008 と Windows Server 2008（SP2） （注） Active Directory 内のユーザ名は、Cisco Unified Communications Manager に定義されたユーザ名と一致している必要があります。
サードパーティの証明書または証明書サーバ	証明書を作成するためには、これらのいずれかが必要。

クライアント アプリケーションに予定表ステータスを設定するには、[Cisco Unified CM IM and Presence のユーザ オプション（Cisco Unified CM IM and Presence User Options）] ページを使用します。

追加情報

Cisco Unified Communications Manager および IM and Presence のマニュアル

http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

Microsoft Exchange 2003 のマニュアル

http://technet.microsoft.com/en-us/library/bb123872.aspx

Microsoft Exchange 2007 のマニュアル

http://technet.microsoft.com/en-us/library/bb124558(EXCHG.80).aspx

- Exchange 2007 で Outlook Web アクセスに対して FBA を設定する方法については、次のサイトを参照してください。

  http://technet.microsoft.com/en-us/library/aa998867(EXCHG.80).aspx

Microsoft Exchange 2010 のマニュアル

http://technet.microsoft.com/en-us/library/bb124558.aspx

Microsoft Active Directory のマニュアル

http://www.microsoft.com/windowsserver2008/en/us/ad-main.aspx

第 2 章

WebDAV 経由での Microsoft Exchange 2003/2007 Server と IM and Presence の統合

（注） このモジュールでは、IM and Presence Service と、**WebDAV 経由**での Microsoft Exchange Server 2003 および 2007 との統合について説明します。 Exchange Web サービス（EWS）経由で Exchange サーバ 2007 または 2010 と統合する場合は、Exchange Web サービス（EWS）経由での Microsoft Exchange Server 2007/2010 と IM and Presence の統合, （21 ページ） を参照してください。各種の Exchange の統合の概要については、IM and Presence と Microsoft Exchange との統合, （1 ページ） を参照してください。

- Microsoft Exchange 2003 設定チェックリスト（WebDAV）, 11 ページ
- Exchange 2003 アカウントの権限の確認, 14 ページ
- Microsoft Exchange 2007 設定チェックリスト（WebDAV）, 14 ページ
- Exchange 2007 アカウントの権限の確認, 17 ページ
- Exchange 2003/2007 仮想ディレクトリの認証の有効化, 19 ページ

Microsoft Exchange 2003 設定チェックリスト（WebDAV）

表 3：Microsoft Exchange 2003 コンポーネントの設定作業, （12 ページ） は、Microsoft Exchange 2003 サーバ上のメールボックスへのアクセスを設定するときに従う必要のあるチェックリストです。 詳細については、Microsoft Server 2003 のマニュアル（http://technet.microsoft.com/en-us/library/bb123872(EXCHG.65).aspx）を参照してください。

表 *3*：*Microsoft Exchange 2003* コンポーネントの設定作業

作業	手順	特記事項
Windows のセキュリティ ポリシーの設定が正しいことを確認します。	「Windows セキュリティ ポリシーの確認」を参照してください。	Cisco Unified Presence は、NTLMv1 Windows 統合認証のみをサポートし、現時点では、NTLMv2 をサポートしていません。
サービス アカウントを作成し、「Exchange 表示専用管理者」セキュリティ グループのメンバとして追加する。	**1** Exchange サーバの **Active Directory ユーザとコンピュータ**（ADUC）で新しいサービス アカウントを作成します。 **2** Exchange サーバの **Active Directory ユーザとコンピュータ**（ADUC）で新しいセキュリティ グループを作成します。そのセキュリティ グループに「Exchange 表示専用管理者」という名前を付けます。 **3** 作成した Exchange 表示専用管理者グループを右クリックし、[プロパティ（Properties）]を選択します。[メンバー（Members）] タブで、このグループに作成したサービス アカウントを追加します。 **4** Exchange サーバで [システム マネージャー（System Manager）] を開き、[管理グループ（Administrative Groups）] で「Exchange 表示専用管理者」グループに移動します。 **5** このグループを右クリックし、[制御の委任（Delegate Control）] を選択して、Exchange 管理委任ウィザードを開始します。 **6** [追加（Add）] を選択し、作成したグループまで移動して選択します。 **7** そのグループに Exchange 表示専用管理者の役割を割り当てます。	Exchange サーバに管理者アカウントがすでに設定されている場合があります。ただし、Exchange 統合には別個の管理者アカウントを作成することをお勧めします。デフォルトの管理者設定では、Exchange サーバの他のユーザアカウントにサインインできない可能性があるためです。

作業	手順	特記事項
ユーザ アカウントを作成し、「Exchange 表示専用管理者」の制御をユーザ アカウントに委任する。	**1** Exchange サーバに新しいユーザ アカウントを作成します。 **2** Exchange サーバの [システム マネージャー（System Manager）] を開き、[Administrative Groups（管理グループ）] で作成したアカウントを追加する管理グループに移動します。 **3** このグループを右クリックし、[制御の委任（Delegate Control）] を選択して、Exchange 管理委任ウィザードを開始します。 **4** [追加（Add）] を選択し、作成したユーザ アカウントまで移動して選択します。 **5** そのアカウントに Exchange 表示専用管理者の役割を割り当てます。	Exchange 2003 環境では、管理者（Exchange 表示専用の権限を持つ）だけが Exchange サーバ上のユーザ アカウントにサインインして Exchange 設定を表示できるように、このユーザ アカウントに「Exchange 表示専用管理者」権限を委任する必要があります。 ユーザ アカウントは、一般の Exchange ユーザが使用する標準の Windows アカウントです。
ユーザ メールボックスに対する Receive As 権限を付与する。	**1** Exchange サーバで [システム マネージャ（System Manager）] を開き、[管理グループ（Administrative Group）] で [最初の管理グループ（First Administrative Group）] > [サーバ（Servers）] > [最初のサーバ（First Server）] > [メールボックス ストア（Mailbox Store）] に移動します。 **2** メールボックス ストアを右クリックし、[プロパティ（Properties）] を選択します。[セキュリティ（Security）] タブで、予定表の情報にアクセスする必要のあるアカウントの名前を入力します。 **3** アカウントとすべての関連メールボックス ストアに Receive As 権限を割り当てます。	IM and Presence では、Exchange サーバ上のユーザの予定表を確認するために、Receive As アカウント権限が追加で必要となります。この権限を上位レベル（メール ストレージ グループなど）で割り当て、メール ストレージ グループ内のすべてのメールボックスに対する読み取り専用アクセスを有効にすることを推奨します。

トラブルシューティングのヒント

- IM and Presence は、Exchange サーバへの接続時にアカウントへのサイン インを可能にするためにのみ、そのアカウントに Receive As 権限を必要とします。 このアカウントは、通常、メールを受信しないため、領域の割り当てについて考慮する必要はありません。

- Exchange サーバがダウンしていることを示すエラー メッセージが表示され、証明書が正しく設定されている場合は、Receive As アカウントが適切に設定されていません。 上記の手順に従ってアカウントを再作成してください。

次の作業

Exchange 2003 アカウントの権限の確認, （14 ページ）

Exchange 2003 アカウントの権限の確認

この手順は、Microsoft Exchange Server 2003 SP1 以降のリリースに適用されます。

手順

ステップ 1 Internet Explorer で次の URL に接続します。

```
https://server/exchange/user@domain
```

ここで、server = サーバ名、user = ユーザ名（Receive-As アカウント以外のユーザ）、domain = exchange ドメイン名です。

ステップ 2 Receive As クレデンシャルを使用してサイン インします。 このクレデンシャルによって OWA アカウントにアクセスできる場合は、権限が Exchange サーバまで正しく伝播されたことを意味します。

次の作業

Microsoft Exchange との統合向けのプレゼンス ゲートウェイの設定, （37 ページ）

Microsoft Exchange 2007 設定チェックリスト（WebDAV）

次の表は、Microsoft Exchange 2007 サーバ上のメールボックスへのアクセスを設定するときに従う必要のあるチェックリストです。 詳細については、Microsoft Server 2007 のマニュアル（http://technet.microsoft.com/en-us/library/bb124558(EXCHG.80).aspx）を参照してください。

表 4 : *Microsoft Exchange 2007* コンポーネントの設定作業

作業	手順	特記事項
Windows のセキュリティポリシーの設定が正しいことを確認します。	「Windows セキュリティ ポリシーの確認」を参照してください。	Cisco Unified Presence は、NTLMv1 Windows 統合認証のみをサポートし、現時点では、NTLMv2 をサポートしていません。

作業	手順	特記事項
Exchange 表示専用管理者アカウントにメールボックスを追加する。	**1** Exchange 表示専用管理者の役割を委任されているアカウントを使用して Exchange 2007 サーバにサイン インします。 **2** Exchange 2007 サーバで Exchange 管理コンソール（EMC）を開きます。 **3** コンソール ツリーで [受信者の構成（Recipient Configuration）] をクリックします。 **4** [メールボックスの新規作成（New Mailbox）] を選択し、メールボックスの新規作成ウィザードを実行します。 • [ユーザ ログオン名（ユーザ プリンシパル名）（User Logon Name (User Principal Name)）] には、ユーザ アカウントが常駐する Microsoft のドメイン名に続き、ユーザがメールボックスにサインインするときに使用する名前を入力します。 例：**msoft-domain-name\username**	指定のストレージにメールボックスを持たないアカウントは機能せず、いずれかの段階でメールボックスを削除された場合、そのアカウントは機能を停止します。

作業	手順	特記事項

Exchange 表示専用管理者の権限をアカウントに委任する。	**Exchange 管理コンソール（EMC）を使用する場合**
	1 Exchange 2007 サーバで EMC を開きます。
	2 コンソール ツリーで [組織構成（Organization Configuration）] を右クリックします。
	3 [Exchange 管理者の追加（Add Exchange Administrator）] を選択し、作成したユーザ アカウントまで移動して選択します。
	4 そのアカウントに Exchange 表示専用管理者の役割を割り当てます。
	
	Exchange 管理シェル（EMS）を使用する場合
	1 コマンド ライン入力を行うために EMS を開きます。
	2 Run 行または EMS のコマンドプロンプトから、関連する引数を伴う Add-Exchange コマンドを実行します。
	
	次に、構文とコマンド例を示します。
	構文
	`Add-ExchangeAdministrator -Role "role" -Identity "identity"`
	例
	`Add-ExchangeAdministrator -Role ViewOnlyAdmin -Identity CUPSAdmin`
		• Exchange 2007 環境では、管理者（Exchange 表示専用の権限を持つ）だけが Exchange サーバ上のユーザ アカウントにサイン インして Exchange 設定を表示できるように、このユーザ アカウントに「Exchange 表示専用管理者」権限を委任する必要があります。
		• ユーザ アカウントは、一般の Exchange ユーザが使用する標準の Windows アカウントです。

ユーザ メールボックスに対する Receive As 権限を付与する。	**Exchange 管理シェル（EMS）を使用する場合**
	1 コマンド ライン入力を行うために EMS を開きます。
	2 EMS で次のように Add-ADPermission コマンドを実行します。
	
	構文
	`Add-ADPermission -Identity "Mailbox Store" -User "Trusted User" -ExtendedRights Receive-As`
	例
	`Add-ADPermission -Identity "First Storage Group" -User CUPSAdmin -ExtendedRights Receive-A`
		この手順を実行するために、Exchange 管理コンソール（EMC）を使用することはできません。

トラブルシューティングのヒント

- IM and Presence は、Exchange サーバへの接続時にアカウントへのサイン インを可能にするためにのみ、そのアカウントに Receive As 権限を必要とします。 このアカウントは、通常、メールを受信しないため、領域の割り当てについて考慮する必要はありません。
- Exchange サーバがダウンしていることを示すエラー メッセージが表示され、証明書が正しく設定されている場合は、Receive As アカウントが適切に設定されていません。 上記の手順に従ってアカウントを再作成してください。

次の作業

Exchange 2007 アカウントの権限の確認, （17 ページ）

Exchange 2007 アカウントの権限の確認

Exchange 2007 アカウントにアクセス許可を割り当てた後は、そのアクセス許可がメールボックス レベルに伝播されており、エンドユーザのメールボックスにアクセスできることを確認する必要があります。 Exchange 2007 では、権限がメールボックスに伝播されるまでに時間を要します。

はじめる前に

- Exchange アカウントに適切な役割と Receive-As 権限を委任してください。 「Microsoft Exchange 2007 設定チェックリスト」を参照してください。
- 次の手順の例では、Exchange アカウントが「cupsadmin」であり、メール ストレージ グループの名前が「First Storage Group」であることを前提とします。

手順

ステップ 1 コマンド ライン入力を行うために Exchange 管理シェル（EMS）を開きます。

ステップ 2 次のように Exchange アカウントが「Exchange 表示専用管理者」グループのメンバであることを確認します。

a) EMS で次のコマンドを実行します。

```
([ADSI]"LDAP://CN=CUPS Admin,CN=Users,DC=r7,DC=com").memberof
```

（注） 「CN=CUPS Admin,CN=Users,DC=r7,DC=com」は、Exchange アカウントの識別名（DN）です。 DN を決定するには、**adsiedit.msc** を使用します。 また、必要に応じて Active Directory 管理者に DN を確認することもできます。

b) 次のように、Exchange アカウントが「Exchange 表示専用管理者」グループのメンバであることがコマンド出力に示されていることを確認します。
例：コマンド出力

CN=Exchange View-Only Administrators,	OU=Microsoft Exchange Security Groups,	DC=r7,	DC=com

ステップ 3 次のように、Exchange アカウントにメール ストレージ グループに対する「Receive-As」権限があることを確認します。

a) EMS で次のコマンドを実行します。

```
Get-ADPermission "First Storage Group" -user cupsadmin | Format-Table
-AutoSize
```

（注） 「First Storage Group」は、メール ストレージ グループの名前です。「cupsadmin」は、Exchange アカウントです。

b) 次のように、Exchange アカウントがメール ストレージ グループに対する「Receive-As」権限を持っていることがコマンド出力に示されていることを確認します。

例：コマンド出力

Identity- - - - - -	**User - - - -**	**Deny- - -**	**Inherited- - - - - -**	**Rights- - - - -**
HTLUO-MAIL\First Storage Group	R7\cupsadmin	False	False	Receive-As

ステップ 4 Exchange アカウントがエンドユーザのメールボックスに対するアクセス許可を持っていることを確認するには、次の操作を行います。

a) EMS で次のコマンドを実行します。

```
Get-MailboxPermission jdoe -user cupsadmin | Format-Table -autosize
```

（注） 「jdoe」は、エンドユーザのメールボックスです。「cupsadmin」は、Exchange アカウントです。

b) 次のように、Exchange アカウントが jdoe のメールボックスに対する FullAccess 権限を持っていることがコマンド出力に示されていることを確認します。

例：コマンド出力

Identity- - - - - -	User - - - -	AccessRights- - - - - - - -	IsInherited- - - - - - - -	Deny- - -
r7.com/Dallas/John Doe	R7\cupsadmin	{FullAccess}	True	False

トラブルシューティングのヒント

ユーザ メールボックスに対するフル アクセス権限は、最上位の権限（この例では「First Storage Group」）から継承されます。 コマンド（ステップ 4, （18 ページ） で実行したコマンド以外）が出力を返さない場合は、権限がメールボックスまで伝播されていないことを意味します。 Exchange アカウントがエンド ユーザのメールボックスに対して FullAccess 権限を持つまで、先に進まないでください。

次の作業

Microsoft Exchange との統合向けのプレゼンス ゲートウェイの設定, （37 ページ）

Exchange 2003/2007 仮想ディレクトリの認証の有効化

Microsoft Office Outlook Web アクセスが正しく動作するためには、Exchange 仮想ディレクトリ（/exchange および /exchweb）の基本認証を有効にする必要があります。 /exchange ディレクトリは、OWA と WebDAV のメールボックス アクセス リクエストを処理します。 /exchweb ディレクトリには、OWA および WebDAV が使用するリソース ファイルが含まれています。 また、Exchange 仮想ディレクトリで Windows 統合認証を有効にすることもできます（オプション）。 さらに、フォーム ベース認証もオプションで有効にできます。

次に、Windows Server 2003 を搭載した Exchange 2003 および Exchange 2007 での WebDAV 統合の手順を示します。

手順

ステップ 1 [管理ツール（Administrative Tools）] から [インターネット インフォメーション サービス（Internet Information Services）] を開き、サーバを選択します。

ステップ 2 [Web サイト（Web Sites）] を選択し、[既定の Web サイト（Default Web Site）] を選択します。

ステップ 3 /exchange または/exchwebディレクトリ フォルダを右クリックし、[プロパティ（Properties）] を選択します。

ステップ 4 [ディレクトリ セキュリティ（Directory Security）] タブを選択します。

ステップ 5 [認証とアクセス制御（Authentication and Access Control）] で、[編集（Edit）] を選択します。

ステップ 6 [認証（Authentication）] では [基本認証（Basic Authentication）] と [統合 Windows（Integrated Windows）] チェックボックスが選択されていることを確認します。

ステップ 7 [オプション] フォーム ベース認証を有効にするには、次の手順を実行します。

a) Exchange 管理コンソール（EMC）を開きます。

b) 左側のペインで [サーバの構成（Server Configuration）] > [クライアント アクセス（Client Access）] を選択します。

c) [クライアント アクセス（Client Access）] ペインで適切なサーバを選択し、[Outook Web アクセス（Outlook Web Access）] タブを選択します。

d) OWA（デフォルトの Web サイト） を右マウス ボタンで選択し、[プロパティ（Properties）] を選択します。

e) [認証（Authentication）] タブを選択します。

f) [フォームベースの認証を使用する（Use forms-based authentication）] を選択し、[ログオン形式（Logon Format）] で [ドメイン\ユーザ名（Domain\user name）] を選択します。

（注） [Form Based Authentication（フォーム ベースの認証）] が選択されている場合は、基本認証はデフォルトで OWA になります。

関連トピック

http://technet.microsoft.com/en-us/library/aa998849(EXCHG.80).aspx

Exchange 2007 から「HTTP 503 サービス利用不可（HTTP 503 Service Unavailable）」エラーを解決する，（82 ページ）

第 3 章

Exchange Web サービス（EWS）経由での Microsoft Exchange Server 2007/2010 と IM and Presence の統合

（注） このモジュールでは、IM and Presence Service と、**Exchange Web サービス（EWS）経由**での Microsoft Exchange Server 2007 および 2010 との統合について説明します。 WebDAV 経由で Exchange サーバ 2003 または 2007 と統合する場合は、WebDAV 経由での Microsoft Exchange 2003/2007 Server と IM and Presence の統合，（11 ページ） を参照してください。 各種の Exchange 統合の概要については、IM and Presence と Microsoft Exchange との統合，（1 ページ） を参照されることをお勧めします。

- Microsoft Exchange 2007 設定チェックリスト（EWS），21 ページ
- Exchange 2007 アカウントの権限の確認，29 ページ
- Microsoft Exchange 2010 設定チェックリスト（EWS），30 ページ
- Exchange 2010 アカウントの権限の確認，32 ページ
- Exchange 2007/2010 仮想ディレクトリの認証，33 ページ

Microsoft Exchange 2007 設定チェックリスト（EWS）

はじめる前に

Exchange 2007 サーバの設定手順は、Windows Server 2003 と Windows Server 2008 のどちらを使用するかによって異なります。

次の表に、Windows Server 2003 および Windows Server 2008 の Microsoft Exchange 2007 サーバ上のメールボックスへのアクセスを設定するときに従う必要のあるチェックリストを示します。 詳細

については、Microsoft Server 2007 のマニュアル（http://technet.microsoft.com/en-us/library/bb124558(EXCHG.80).aspx）を参照してください。

表 *5*：*Microsoft Exchange 2007* コンポーネントの設定作業

作業	手順	特記事項
Windows のセキュリティ ポリシーの設定が正しいことを確認します。	「Windows セキュリティ ポリシーの確認」を参照してください。	Cisco Unified Presence は、NTLMv1 Windows 統合認証のみをサポートし、現時点では、NTLMv2 をサポートしていません。

作業	手順	特記事項
サービス アカウントにローカルでサインインする権限をユーザに与える。		• Exchange の偽装を正常に機能させるには、すべての Exchange サーバを Windows Authorization Access Group のメンバにする必要があります。 • サービス アカウントは、Exchange 管理グループのメンバであってはなりません。Microsoft Exchange は、これらのグループのすべてのアカウントの偽装を明示的に拒否します。

作業	手順	特記事項
	Windows Server 2003 での Exchange 2007 の設定 1 Exchange 表示専用管理者の役割を委任されているサービス アカウントを使用して Exchange 2007 サーバにサイン インします。 2 Exchange サーバで [ドメイン コントローラ セキュリティの設定（Domain Controller Security Settings）] ウィンドウを開きます。 3 左側のフレームの [セキュリティの設定（Security Settings）] から [ローカル ポリシー（Local Policies）] > [ユーザ権利の割り当て（User Rights Assignments）] の順に選択します。 4 コンソールの右側のフレームで [ローカル ログインを許可する（Allow Log On Locally）] をダブルクリックします。 5 [ユーザまたはグループの追加（Add User or Group）] を選択し、作成済みのサービス アカウントに移動して選択します。 6 [名前の確認（Check Names）] を選択し、指定されたユーザが正しいことを確認します。 [OK] をクリックします。 **Windows Server 2008 での Exchange 2007 の設定** 1 Exchange 表示専用管理者の役割を委任されているサービス アカウントを使用して Exchange 2007 サーバにサイン インします。 2 [スタート（Start）] を選択します。 3 **gpmc.msc** と入力します。 4 Enter を押します。 5 Exchange サーバで [ドメイン コントローラ セキュリティの設定（Domain Controller Security Settings）] ウィンドウを開きます。	

作業	手順	特記事項
	6 左側のフレームの [セキュリティの設定（Security Settings）] から [ローカル ポリシー（Local Policies）] > [ユーザ権利の割り当て（User Rights Assignments）] の順に選択します。 **7** コンソールの右側のフレームで [ローカルログインを許可する（Allow Log On Locally）] をダブルクリックします。 **8** [これらのポリシーの設定を定義する（Define these policy settings）] チェックボックスが選択されていることを確認します。 **9** [ユーザまたはグループの追加（Add User or Group）] を選択し、作成済みのサービス アカウントに移動して選択します。 [OK] をクリックします。 **10** [名前の確認（Check Names）] を選択し、指定されたユーザが正しいことを確認します。 [OK] をクリックします。 **11** [ローカルログオンを許可する（Allow Log On Locally）] プロパティのダイアログボックスで [適用（Apply）] と [OK] をクリックします。 **12** ユーザ SMTP アドレスが alias @ FQDN であることを確認します。 そうでない場合は、ユーザ プリンシパル名（UPN）を使用して偽装する必要があります。 これは alias@FQDN と定義されます。	

作業	手順	特記事項

偽装権限をサーバ レベルで設定する。	**Exchange 管理シェル（EMS）を使用する場合**
	1 コマンドライン入力を行うためにEMSを開きます。
	2 この Add-ADPermission コマンドを実行し、サーバに偽装権限を追加します。
	`Add-ADPermission -Identity (get-exchangeserver).DistinguishedName -User (Get-User -Identity User | select-object).identity -AccessRights GenericAll -InheritanceType Descendents`
	次に例を示します。
	`Add-ADPermission -Identity (get-exchangeserver).DistinguishedName -User (Get-User -Identity Ex2007 | select-object).identity -ExtendedRight ms-Exch-EPI-Impersonation`
		• これらのコマンドレットは、サーバ レベルで偽装権限を付与します。 また、データベース、ユーザ、および連絡先レベルでも権限を付与することもできます。
		• 複数のサーバがある場合は、各サーバ（またはデータベース）への偽装権限を付与する必要があります。Exchange 2007 には、システム全体を対象とする偽装権限の機能はありません。
		• 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）を使用してユーザ アカウントを偽装する必要があります。

作業	手順	特記事項

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。	**Exchange 管理シェル（EMS）を使用する場合**
	1 EMS で次の Add-ADPermission コマンドを実行して、指定したサービス アカウント（Exch2007 など）のサーバに対する偽装権限を追加します。
	`Add-ADPermission -Identity (get-exchangeserver).DistinguishedName -User (Get-User -Identity User | select-object).identity -ExtendedRight ms-Exch-EPI-Impersonation`
	次に例を示します。
	`Add-ADPermission -Identity (get-exchangeserver).DistinguishedName -User (Get-User -Identity Ex2007 | select-object).identity -ExtendedRight ms-Exch-EPI-Impersonation`
	2 EMS で次の Add-ADPermission コマンドを実行して、サービス アカウントに偽装する各メールボックスへの偽装権限を追加します。
	`Add-ADPermission -Identity (get-exchangeserver).DistinguishedName -User (Get-User -Identity User | select-object).identity -ExtendedRight ms-Exch-EPI-May-Impersonate`
	次に例を示します。
	`Add-ADPermission -Identity (get-exchangeserver).DistinguishedName -User (Get-User -Identity Ex2007 | select-object).identity -ExtendedRight ms-Exch-EPI-May-Impersonate`
		• これらの権限は、偽装を実行するサービス アカウントに対して設定する必要があります（クライアント アクセス サーバ（CAS）上）。
		• CAS がロードバランサの背後に配置されている場合は、ロードバランサの背後にあるすべての CAS サーバの Ex2007 アカウントに対して **ms-Exch-EPI-Impersonation** 権限を付与します。
		• お使いのメールボックス サーバが CAS サーバとは異なるマシン上にある場合は、すべてのメールボックス サーバの Ex2007 アカウントに対して **ms-Exch-EPI-Impersonation** 権限を付与します。
		• この権限は、[Active Directory サイトとサービス（Active Directory Sites and Services）] または [Active Directory ユーザとコンピュータ（Active Directory Users and Computers）] ユーザ インターフェイスを使用して設定することもできます。

作業	手順	特記事項

サービス アカウントおよびユーザ メールボックスに Send As 権限を付与する。	**Exchange 管理シェル（EMS）を使用する場合**
	EMS で次の Add-ADPermission コマンドを実行して、サービスアカウントおよび関連するすべてのユーザメールボックス ストアに Send As 権限を付与します。
	`Add-ADPermission -Identity (get-exchangeserver).DistinguishedName -User (Get-User -Identity User | select-object).identity -ExtendedRights Send-As`
	次に例を示します。
	`Add-ADPermission -Identity (get-exchangeserver).DistinguishedName -User (Get-User -Identity Ex2007 ¦ select-object).identity -ExtendedRights Send-As`
		この手順を実行するために、Exchange 管理コンソール（EMC）を使用することはできません。

サービス アカウントおよびユーザ メールボックスに Receive As 権限を付与する。	**Exchange 管理シェル（EMS）を使用する場合**
	EMS で次の Add-ADPermission コマンドを実行して、サービスアカウントおよび関連するすべてのユーザ メールボックス ストアに Receive As 権限を付与します。
	`Add-ADPermission -Identity (get-exchangeserver).DistinguishedName -User (Get-User -Identity User | select-object).identity -ExtendedRights Receive-As`
	次に例を示します。
	`Add-ADPermission -Identity (get-exchangeserver).DistinguishedName -User (Get-User -Identity Ex2007 ¦ select-object).identity -ExtendedRights Receive-As`
		この手順を実行するために、Exchange 管理コンソール（EMC）を使用することはできません。

トラブルシューティングのヒント

IM and Presence は、Exchange サーバへの接続時にアカウントへのサイン インを可能にするためにのみ、そのアカウントに Receive As 権限を必要とします。 このアカウントは、通常、メールを受信しないため、領域の割り当てについて考慮する必要はありません。

次の作業

Exchange 2007 アカウントの権限の確認, （29 ページ）

Exchange 2007 アカウントの権限の確認

Exchange 2007 アカウントに権限を割り当てた後で、その権限がメールボックスのレベルまで伝播し、選択されたユーザがメールボックスにアクセスしたり別のユーザのアカウントを偽装したりできることを確認する必要があります。 Exchange 2007 では、権限がメールボックスに伝播されるまでに時間を要します。

はじめる前に

Exchange アカウントに適切な権限を委任してください。 「Microsoft Exchange 2007 設定チェックリスト（EWS）」を参照してください。

手順

ステップ 1 Exchange 2007 サーバの EMC で、コンソール ツリーの [Active Directory サイトとサービス（Active Directory Sites and Services）] を右クリックします。

ステップ 2 [表示（View）] をポイントし、[サービス ノードの表示（Show Services Node）] を選択します。

ステップ 3 サービス ノード（Services/MS Exchange/First Organization/Admin Group/Exchange Admin Group/Servers など）を展開します。

ステップ 4 選択したサービス ノードに CAS が含まれていることを確認します。

ステップ 5 各 CAS サーバの「プロパティ（Properties）」を表示し、[セキュリティ（Security）] タブで以下を確認します。

a) サービス アカウントがリストされている。

b) サービスアカウントに付与されている権限が（チェックされているボックスにより）アカウントに Exchange Web サービスの偽装権限が付与されていることを示している。

ステップ 6 サービス アカウント（Ex2007 など）にストレージ グループおよびメールボックス ストアに対する Allow impersonationpermission が付与され、個人情報の交換や別のユーザ アカウントでの送受信が可能であることを確認します。

トラブルシューティングのヒント

- アカウントまたは偽装権限が ステップ 5, （29 ページ） のとおりに表示されない場合は、サービス アカウントを再度作成し、必要な偽装権限をアカウントに付与する必要があります。
- 変更を有効にするために、Exchange サーバの再起動が必要となる場合があります。 これはテストによって確認されています。

次の作業

Exchange 2007/2010 仮想ディレクトリの認証, （33 ページ）

Microsoft Exchange 2010 設定チェックリスト（EWS）

次に、Microsoft Exchange 2010 サーバ上のメールボックスへのアクセスを設定するときに従う必要のある手順を示します。 詳細の手順については、Microsoft Server 2010 のマニュアルを参照してください。

はじめる前に

Microsoft Exchange 2010 サーバと IM and Presence を EWS 経由で統合する前に、Exchange サーバ上で次のスロットル ポリシー パラメータ値を設定してください。 これらの値は、EWS の予定表と IM and Presence との統合を正常に機能させるために必要な値です。

表 *6*：*Microsoft Exchange* のスロットル ポリシー パラメータの推奨値

パラメータ	推奨設定値
EWSMaxConcurrency	シスコがテストを行った結果、デフォルトのスロットル ポリシー値があれば、50% の予定表対応ユーザに十分に対応できることがわかっています。 ただし、CAS への EWS リクエストの負荷が高い場合は、パラメータを 100 に増やすことを推奨します。
EWSPercentTimeInAD	50
EWSPercentTimeInCAS	90
EWSPercentTimeInMailboxRPC	60
EWSMaxSubscriptions	Null
EWSFastSearchTimeoutInSeconds	60
EWSFindCountLimit	1000

手順

Microsoft Exchange 2010 の特定のユーザまたはユーザのグループに対し、Exchange の偽装権限を設定するには、次の手順を実行します。

1 コマンド ライン入力を行うために EMS を開きます。

2 EMS で New-ManagementRoleAssignment コマンドを実行し、他のユーザ アカウントを偽装する権限を指定サービス アカウント（Ex2010 など）に付与します。

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

例：

```
new-ManagementRoleAssignment -Name:_suImpersonateRoleAsg -Role:ApplicationImpersonation
-User:Ex2010@domain
```

3 この New-ManagementRoleAssignment コマンドを実行し、偽装権限が適用される範囲を定義します。 この例では、指定された Exchange サーバのすべてのアカウントを偽装する権限が、Exch2010 アカウントに対して与えられます。

```
new-ManagementScope -Name:_suImpersonateScope -ServerList:<server name>
```

例：

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

4 New-ThrottlingPolicy コマンドを実行し、上の表で定義された推奨値を使用して新しいスロットリング ポリシーを作成します。

```
New-ThrottlingPolicy -Name:"<Policy Name>" -EWSMaxConcurrency:100 -EWSPercentTimeInAD:50
-EWSPercentTimeInCAS:90 -EWSPercentTimeInMailboxRPC:60
-EWSMaxSubscriptions:5000-EWSFastSearchTimeoutInSeconds:60-EWSFindCountLimit:1000
```

例：

```
New-ThrottlingPolicy -Name:"IM and Presence ThrottlingPolicy" -EWSMaxConcurrency:100
-EWSPercentTimeInAD:50 -EWSPercentTimeInCAS:90 -EWSPercentTimeInMailboxRPC:60
-EWSMaxSubscriptions:5000 -EWSFastSearchTimeoutInSeconds:60 -EWSFindCountLimit:1000
```

5 Set-ThrottlingPolicyAssociation コマンドを実行し、新しいスロットリング ポリシーと前述の手順 2 で使用されたサービス アカウントを関連付けます。

```
Set-ThrottlingPolicyAssociation -Identity "<Username>" -ThrottlingPolicy “<Policy Name>"
```

例：

```
Set-ThrottlingPolicyAssociation -Identity "Ex2010" -ThrottlingPolicy “IM and Presence
ThrottlingPolicy"
```

次の作業

Exchange 2010 アカウントの権限の確認

関連トピック

Windows セキュリティ ポリシーの確認, （3 ページ）
Exchange 2010 アカウントの権限の確認, （32 ページ）
Microsoft Exchange Server 2010 のマニュアル
Microsoft Exchange サーバのパラメータ

Exchange 2010 アカウントの権限の確認

Exchange 2010 アカウントに権限を割り当てた後で、その権限がメールボックスのレベルまで伝播し、選択されたユーザがメールボックスにアクセスしたり別のユーザのアカウントを偽装したりできることを確認する必要があります。 Exchange 2010 では、権限がメールボックスに伝播されるまでに時間を要します。

はじめる前に

- Exchange アカウントに適切な権限を委任してください。 「Microsoft Exchange 2010 設定チェックリスト（EWS）」を参照してください。

手順

ステップ 1 コマンド ライン入力を行うために Exchange 管理シェル（EMS）を開きます。

ステップ 2 サービス アカウントに必要な偽装権限が付与されていることを確認します。

a) EMS で次のコマンドを実行します。

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

b) コマンド出力に、指定アカウントに対する「ApplicationImpersonation」の役割割り当てが示されることを確認します。
例：コマンド出力

Name- - - - - -	Role - - - -	RoleAssigneeName- - - - - - - - - - - -	RoleAssigneeType- - - - - -	AssignmentMethod- - - - -	EffectiveUserName- - - - - - - - -
_suImpersonateRoleAsg	ApplicationImpersonation	ex 2010	User	Direct	ex 2010

ステップ 3 サービス アカウントに適用される管理の範囲が正しいことを確認します。

a) EMS で次のコマンドを実行します。

```
Get-ManagementScope _suImpersonateScope
```

b) 次のように、コマンド出力に偽装アカウント名が含まれていることを確認します。
例：コマンド出力

Name	ScopeRestrictionType	Exclusive	RecipientRoot	RecipientFilter	ServerFilter
_suImpersonateScope	ServerScope	False			DistinguishedName

ステップ 4 ThrottlingPolicy パラメータが、表 6：Microsoft Exchange のスロットル ポリシー パラメータの推奨値, （30 ページ） に定義されているものと一致することを確認します。

a) EMS で次のコマンドを実行します。

```
Get-ThrottlingPolicy -Identity "<Policy Name>" | findstr ^EWS
```

b) コマンド出力が 表 6：Microsoft Exchange のスロットル ポリシー パラメータの推奨値, （30 ページ） に定義されているものと同じ値を持つことを確認します。

次の作業

Exchange 2007/2010 仮想ディレクトリの認証, （33 ページ）

Exchange 2007/2010 仮想ディレクトリの認証

Microsoft Office Outlook Web アクセスが正しく動作するためには、Exchange 仮想ディレクトリ（/exchange および /exchweb）の基本認証を有効にする必要があります。 /exchange ディレクトリは、OWA と WebDAV のメールボックス アクセス リクエストを処理します。 /exchweb ディレクトリには、OWA および WebDAV が使用するリソースファイルが含まれています。 また、Exchange 仮想ディレクトリで Windows 統合認証を有効にすることもできます（オプション）。 さらに、フォーム ベース認証もオプションで有効にできます。

- Windows Server 2003 がインストールされた Exchange 2007 での認証の有効化, （34 ページ）
- Windows Server 2008 がインストールされた Exchange 2010 での認証の有効化, （35 ページ）

Windows Server 2003 がインストールされた Exchange 2007 での認証の有効化

手順

ステップ 1 [管理ツール（Administrative Tools）] から [インターネット インフォメーション サービス（Internet Information Services）] を開き、サーバを選択します。

ステップ 2 [Web サイト（Web Sites）] を選択し、[既定の Web サイト（Default Web Site）] を選択します。

ステップ 3 /exchange または/exchwebディレクトリ フォルダを右クリックし、[プロパティ（Properties）] を選択します。

ステップ 4 [ディレクトリ セキュリティ（Directory Security）] タブを選択します。

ステップ 5 [認証とアクセス制御（Authentication and Access Control）] で、[編集（Edit）] を選択します。

ステップ 6 [認証（Authentication）] で、次の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。

- Basic Authentication (password is sent in clear text)
- Integrated Windows Authentication

ステップ 7 [オプション] フォーム ベース認証を有効にするには、次の手順を実行します。

a) Exchange 管理コンソール（EMC）を開きます。

b) 左側のペインで [サーバの構成（Server Configuration）] > [クライアント アクセス（Client Access）] を選択します。

c) [クライアント アクセス（Client Access）] ペインで適切なサーバを選択し、[Outook Web アクセス（Outlook Web Access）] タブを選択します。

d) OWA（デフォルトの Web サイト） を右マウス ボタンで選択し、[プロパティ（Properties）] を選択します。

e) [認証（Authentication）] タブを選択します。

f) [フォームベースの認証を使用する（Use forms-based authentication）] を選択し、[ログオン形式（Logon Format）] で [ドメイン\ユーザ名（Domain\user name）] を選択します。

（注） [Form Based Authentication（フォーム ベースの認証）] が選択されている場合は、基本認証はデフォルトで OWA になります。

次の作業

Microsoft Exchange との統合向けのプレゼンス ゲートウェイの設定, （37 ページ）

Windows Server 2008 がインストールされた Exchange 2010 での認証の有効化

手順

ステップ 1 Exchange 管理コンソールを開き、サーバを選択します。

ステップ 2 [サーバ構成（Server Configuration）] を選択します。

ステップ 3 [クライアント アクセス（Client Access）] を選択します。

ステップ 4 Outlook Web App 仮想ディレクトリをホストしているサーバを選択します。

ステップ 5 [Outlook Web App] タブを選択します。

ステップ 6 作業ペインで、認証を設定する仮想ディレクトリを選択して右クリックします。

ステップ 7 [プロパティ（Properties）] を選択し、[認証（Authentication）] タブを選択します。

ステップ 8 [認証（Authentication）] で次のチェックボックスが選択されていることを確認し、[OK] を選択します。

- Basic Authentication (password is sent in clear text)
- Integrated Windows Authentication

ステップ 9 [Exchange コントロール パネル（Exchange Control Panel）] ディレクトリを選択します。

ステップ 10 作業ペインで、認証を設定する仮想ディレクトリを選択して右クリックします。

ステップ 11 [認証（Authentication）] で次のチェックボックスが選択されていることを確認し、[OK] を選択します。

- Basic Authentication (password is sent in clear text)
- Integrated Windows Authentication

ステップ 12 変更内容を有効にするには、CLI に次のコマンドを入力して IIS を再起動します。

```
iisreset /noforce
```

ステップ 13 コントロール パネルで IIS Admin Service および World Wide Publishing Service が起動済みの状態になっていることを確認します。

ステップ 14 [オプション] フォーム ベース認証を有効にするには、次の手順を実行します。

a) Exchange 管理コンソール（EMC）を開きます。

b) 左側のペインで [サーバの構成（Server Configuration）] > [クライアント アクセス（Client Access）] を選択します。

c) [クライアント アクセス（Client Access）] ペインで適切なサーバを選択し、[Outook Web アクセス（Outlook Web Access）] タブを選択します。

d) OWA（デフォルトの Web サイト） を右マウス ボタンで選択し、[プロパティ（Properties）] を選択します。

e) [認証（Authentication）] タブを選択します。

f) [フォームベースの認証を使用する（Use forms-based authentication）] を選択し、[ログオン形式（Logon Format）] で [ドメイン\ユーザ名（Domain\user name）] を選択します。

（注） [Form Based Authentication（フォーム ベースの認証）] が選択されている場合は、基本認証はデフォルトで OWA になります。

次の作業

Microsoft Exchange との統合向けのプレゼンス ゲートウェイの設定, （37 ページ）

関連トピック

http://technet.microsoft.com/en-us/library/aa998849.aspx
http://technet.microsoft.com/en-us/library/ee633481.aspx

第 4 章

Microsoft Exchange Server との統合における IM and Presence の設定

- Microsoft Exchange との統合向けのプレゼンス ゲートウェイの設定，37 ページ
- 予定表の統合の有効化，42 ページ
- [オプション] EWS での Microsoft Exchange 予定表通知の頻度の設定，43 ページ
- [オプション] 予定表と統合する場合の多言語サポートの設定，44 ページ
- [オプション] Microsoft Exchange 通知ポートの設定，49 ページ
- [オプション] Microsoft Exchange 予定表通知の接続時間の設定，50 ページ
- その他の Microsoft Exchange パラメータ，51 ページ

MicrosoftExchangeとの統合向けのプレゼンスゲートウェイの設定

予定表情報を交換するためには、Microsoft Exchange サーバ（Microsoft Outlook）をプレゼンス ゲートウェイとして設定する必要があります。 IM and Presence サーバは、Exchange ゲートウェイによってアベイラビリティ情報（予定表/会議ステータス）をユーザ単位でアベイラビリティ ステータスに反映できます。

この手順の設定オプションは、ネットワーク環境と次のうちどの統合を行うかによって異なります。

- WebDAV 経由での Exchange 2003 と IM and Presence の統合
- WebDAV または Exchange Web サービス（EWS）経由での Exchange 2007 と IM and Presence の統合
- EWS 経由での Exchange 2010 と IM and Presence の統合

1 つの WebDav サーバまたは複数の EWS サーバを設定できます。 展開環境に WebDAV サーバと EWS サーバを混在させることはできません。 各種の Exchange 統合の概要については、IM and Presence と Microsoft Exchange との統合, （1 ページ） を参照されることをお勧めします。

EWS または WebDAV サーバを追加、更新、または削除した場合、設定の変更を有効にするためには、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した場合は、すべての変更を同時に反映するよう Cisco Presence Engine を一度だけ再起動することができます。 IM and Presence は、サービスを再起動するタイミングを通知し（自動通知）、IM and Presence のサービスアビリティに Cisco Presence Engine を再起動するよう指示します（[Cisco Unified IM and Presence のサービスアビリティ（Cisco Unified IM and Presence Serviceability）] > [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）。

Cisco Unified Presence リリース 8.6 以前では、Exchange ゲートウェイを追加、変更、または削除すると、クラスタ内の全ユーザの予定表がオフになります。 Cisco Unified Presence リリース 8.6 以降では、ユーザ予定表の一括無効化は、WebDAV ゲートウェイまたは最後の EWS ゲートウェイを削除した場合にのみ行われます。

（注） Cisco Unified Presence リリース 8.6 以前のバージョンでは、サーバをアップグレードまたはダウングレードする場合には現在のサーバを削除し、ターゲット サーバを手動で追加する必要があります。 これにより、クラスタ内のすべてのユーザの予定表のプレゼンスが無効になります。 Cisco Unified Presence リリース 8.6 以降では、この問題に対処済みです。 エンド ユーザに何の影響も及ぼすことなく、サーバをアップグレードまたはダウングレードし、IM and Presence のゲートウェイ タイプを変更できるようになりました。 ただし、アップグレードまたはダウングレードを行った後は、Presence Engine（PE）を再起動する必要があります。これによってユーザに影響が及ぶことがあります。

DNS の設定に対する、以下の影響を考慮に入れておいてください。

- IM and Presence で DNS を設定した場合は、リーフ証明書の件名 CN 値は FQDN または IP アドレスのいずれかになると考えられます。 [プレゼンス ゲートウェイ（Presence Gateway）] フィールドの値は、リーフ証明書の件名 CN 値と一致している必要があります。
- IM and Presence で DNS を設定していない場合は、リーフ証明書の件名 CN 値は IP アドレスになります。 件名 CN 値が IP アドレスでない場合は、件名 CN 値が Exchange サーバの IP アドレスになるようにこの Exchange 証明書を生成し直す必要があります。 [プレゼンス ゲートウェイ（Presence Gateway）] フィールドの値は、リーフ証明書の件名 CN 値と一致している必要があります。

WebDAV のプレゼンス ゲートウェイの設定

はじめる前に

プレゼンス ゲートウェイを設定する前に、IM and Presence 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。

手順

ステップ 1 [Cisco Unified CM IM and Presence 管理（Cisco Unified CM IM and Presence Administration）] にサイン インします。

ステップ 2 [プレゼンス（Presence）] > [ゲートウェイ（Gateways）] を選択します。

ステップ 3 [新規追加（Add New）] を選択します。

ステップ 4 [Exchange -- WebDAV] を選択します。

ステップ 5 1 種類以上のゲートウェイを設定した場合にプレゼンス ゲートウェイのインスタンスを区別できるよう、[説明（Description）] フィールドに意味のある説明を入力します。

ステップ 6 [プレゼンス ゲートウェイ（Presence Gateway）] フィールドにプレゼンス ゲートウェイのサーバの場所を入力し、それが Exchange サーバの IIS 証明書のサブジェクトの共通名（CN）と一致することを確認します。 Microsoft Exchange サーバに接続するには、次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

プレゼンス ゲートウェイをワイルドカード証明書で使用するよう設定するには、指定したサーバの場所の値は、ワイルドカード証明書で保護された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 `*.cup.cisco.com`, を保護する場合は、[プレゼンス ゲートウェイ（Presence Gateway）] フィールドに `<server name>.cup.cisco.com` というサーバの場所の値を入力します。

（注） FQDN を入力する場合は、Exchange サーバの証明書の件名と一致する必要があります。これは、証明書チェーンのリーフ証明書のサブジェクトの共通名（CN）値です。 FQDN は、要求を処理し、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。

ステップ 7 [アカウント名（Account Name）] フィールドには、IM and Presence が Microsoft Exchange サーバに接続するときに使用する Receive-As アカウントの名前を <domain>\<username> の形式で入力します。このとき、次の点に留意してください。

- Exchange サーバがデフォルトのドメインを指定するよう設定されている場合は、ユーザ名の一部としてドメインを含める必要がないことがあります。
- それ以外の場合は、証明書エラー（401 および 404 認証応答）の発生を防ぐために、アカウント名の前にドメインを指定してください。

ステップ 8 IM and Presence が Microsoft Exchange サーバに接続するために必要となる Microsoft Exchange アカウント パスワードを入力し、確認します。 確認のためもう一度パスワードを入力します。 この

値は、Microsoft Exchange サーバで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 Microsoft Exchange サーバとの接続に使用するポートを入力します。 IM and Presence と Microsoft Exchange との統合は、セキュアな HTTP 接続を介して行う必要があります。 ポート 443（デフォルト ポート）を使用し、それ以外のポートに変更しないことを推奨します。

ステップ 10 [保存（Save）] を選択します。

ステップ 11 IM and Presence と Exchange サーバ間の接続が成功したことを確認します。 [プレゼンス ゲートウェイの設定（Presence Gateway Configuration）] ウィンドウの [トラブルシューティング（Troubleshooter）] に接続ステータスが表示されます。 解決のための処置を行う必要がある場合は、Exchange サーバの接続ステータスのトラブルシューティングに関するトピックを参照してください。

ステップ 12 Exchange SSL 証明書チェーンのステータスを確認します（[確認が成功しました（Verified）]。 証明書の件名 CN に不一致がある場合は、プレゼンス ゲートウェイの設定ウィンドウの [トラブルシューティング（Troubleshooter）] に表示されます。 解決のための処置を行う必要がある場合は、SSL 接続のトラブルシューティングに関するトピックを参照してください。

ステップ 13 [オプション] 予定表の統合をローカライズする場合は、Exchange サーバの URL に「Calendar」の訳語が含まれていることを確認してください。 解決のための処置を行う必要がある場合は、Microsoft Exchange との統合に関する既知の問題についてのトピックを参照してください。

関連トピック

Exchange サーバの接続ステータスに関するトラブルシューティング, （71 ページ）
SSL 接続と証明書のステータスのトラブルシューティング, （72 ページ）
Microsoft Exchange の統合に影響することが確認されている問題, （78 ページ）

EWS のプレゼンス ゲートウェイの設定

はじめる前に

プレゼンス ゲートウェイを設定する前に、IM and Presence 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。

手順

ステップ 1 [Cisco Unified CM IM and Presence 管理（Cisco Unified CM IM and Presence Administration）] にサイン インします。

ステップ 2 [プレゼンス（Presence）] > [ゲートウェイ（Gateways）] を選択します。

ステップ 3 [新規追加（Add New）] を選択します。

ステップ 4 [Exchange - EWS サーバ（Exchange -- EWS Server）] を選択します。

ステップ 5 1 種類以上のゲートウェイを設定した場合にプレゼンス ゲートウェイのインスタンスを区別できるよう、[説明（Description）] フィールドに意味のある説明を入力します。

ステップ 6 [プレゼンス ゲートウェイ（Presence Gateway）] フィールドにプレゼンス ゲートウェイのサーバの場所を入力し、それが Exchange サーバの IIS 証明書のサブジェクトの共通名（CN）と一致することを確認します。 Microsoft Exchange サーバに接続するには、次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

プレゼンス ゲートウェイをワイルドカード証明書で使用するよう設定するには、指定したサーバの場所の値は、ワイルドカード証明書で保護された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 `*.cup.cisco.com`, を保護する場合は、[プレゼンス ゲートウェイ（Presence Gateway）] フィールドに `<server name>.cup.cisco.com` というサーバの場所の値を入力します。

（注） FQDN を入力する場合は、Exchange サーバの証明書の件名と一致する必要があります。これは、証明書チェーンのリーフ証明書のサブジェクトの共通名（CN）値です。 FQDN は、要求を処理し、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。

ステップ 7 IM and Presence が Microsoft Exchange サーバに接続するときに使用する偽装アカウントの名前を入力します。この形式は、ユーザ プリンシパル名（user@domain など）か、ダウンレベルのログオン名（domain\user など）のどちらかです。

ステップ 8 IM and Presence が Microsoft Exchange サーバに接続するために必要となる Microsoft Exchange アカウント パスワードを入力し、確認します。 確認のためもう一度パスワードを入力します。 この値は、Microsoft Exchange サーバで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。

（注）
- EWS サーバを追加した後に別のサーバを追加した場合は、[アカウント名（Account Name）] および [パスワード（Password）] フィールドのデフォルト値は、最初のサーバに対して入力したクレデンシャルになります。
- EWS サーバのアカウント名およびパスワードのクレデンシャルを変更した場合は、設定されたすべての EWS サーバに対して新しいクレデンシャルが複製されます。

ステップ 9 Microsoft Exchange サーバとの接続に使用するポートを入力します。 IM and Presence と Microsoft Exchange との統合は、セキュアな HTTP 接続を介して行う必要があります。 ポート 443（デフォルト ポート）を使用し、それ以外のポートに変更しないことを推奨します。

ステップ 10 [保存（Save）] を選択します。

ステップ 11 IM and Presence と Exchange サーバ間の接続が成功したことを確認します。 [プレゼンス ゲートウェイの設定（Presence Gateway Configuration）] ウィンドウの [トラブルシューティング（Troubleshooter）] に接続ステータスが表示されます。 解決のための処置を行う必要がある場合は、Exchange サーバの接続ステータスのトラブルシューティングに関するトピックを参照してください。

ステップ 12 Exchange SSL 証明書チェーンのステータスを確認します（[確認が成功しました（Verified）]。 証明書の件名 CN に不一致がある場合は、プレゼンス ゲートウェイの設定ウィンドウの [トラブルシューティング（Troubleshooter）] に表示されます。 解決のための処置を行う必要がある場合は、SSL 接続のトラブルシューティングに関するトピックを参照してください。

ステップ 13 [オプション] 予定表の統合をローカライズする場合は、Exchange サーバの URL に「Calendar」の訳語が含まれていることを確認してください。 解決のための処置を行う必要がある場合は、Microsoft Exchange との統合に関する既知の問題についてのトピックを参照してください。

関連トピック

Exchange サーバの接続ステータスに関するトラブルシューティング, （71 ページ）
SSL 接続と証明書のステータスのトラブルシューティング, （72 ページ）
Microsoft Exchange の統合に影響することが確認されている問題, （78 ページ）

予定表の統合の有効化

デフォルトでは、各ユーザのアベイラビリティ ステータスは Cisco Jabber によって自動的に判断されます。 ユーザがアプリケーションにサインインするか、電話中になると、それが検出されます。 システム管理者は、Microsoft Outlook 予定表と一体化してユーザが会議中であることを示すこともできます。 オプションを設定して、電話機のステータスと会議のステータスを表示するかどうかを選択できます。

電話機と会議のステータスを表示するオプションを設定するには、次の手順を実行します。

（注） 予定表の統合は個別にのみ有効にできますが、最後の予定表プレゼンス ゲートウェイを設定から削除すると、すべてのユーザに対して無効にすることができます。

はじめる前に

プレゼンス ゲートウェイが IM and Presence で設定されていることを確認します。 詳細については、Microsoft Exchange との統合向けのプレゼンス ゲートウェイの設定, （37 ページ）を参照してください。

手順

ステップ 1 [Cisco Unified CM IM and Presence のユーザ オプション（Cisco Unified CM IM and Presence User Options）] ページにサイン インします。

ステップ 2 [ユーザ オプション（User Options）] > [設定（Preferences）] を選択します。

ステップ 3 [予定表の設定（Calendar Settings）] で [自分のプレゼンス ステータスに予定表情報を含める（Include Calendar Information in my Presence Status）] を [オン（On）] に設定します。

ステップ 4 [保存（Save）] を選択します。

[オプション] EWS での Microsoft Exchange 予定表通知の頻度の設定

この手順は、Microsoft Exchange サーバ 2007 または 2010 を EWS 経由で統合する場合にのみ必要となります。 予定表を WebDAV 経由で統合する場合、この手順を実行する必要はありません。

[EWS ステータスの頻度（EWS Status Frequency）] パラメータは、Exchange サーバが IM and Presence 上のサブスクリプションを更新する間隔（分数）を指定します。 このパラメータのデフォルト値は 60 分です。 IM and Presence 上のプレゼンス エンジンがサブスクリプションを失ったことを 60 分（デフォルト）よりも短い間隔で検出する必要がある場合は、この間隔をデフォルト値より小さい値に変更してください。 この間隔を短くすると、エラーの検出能力は向上しますが、それに伴って Exchange サーバおよび IM and Presence サーバへの負荷も増加します。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [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（Server）] メニューから IM and Presence サーバを選択します。

ステップ 3 [サービス（Service）] メニューから [Cisco UP プレゼンス エンジン（アクティブ）（Cisco UP Presence Engine (Active)）] を選択します。

ステップ 4 [EWS ステータスの頻度（EWS Status Frequency）] フィールドのパラメータ値を編集します。 このパラメータのデフォルト値は 60 分です。

ステップ 5 [保存（Save）] を選択します。

次の作業

予定表の統合はユーザ単位で行われるため、[EWS ステータスの頻度（EWS Status Frequency）] パラメータの変更はその都度に更新されます。 ただし、すべてのユーザについてパラメータの変更を有効にするために、Cisco Presence Engine を再起動することを推奨します。 [Cisco Unified IM and

Presence のサービスアビリティ（Cisco Unified IM and Presence Serviceability）] > [ツール（Tools）] > [サービスの開始（Service Activation）] を選択します。

トラブルシューティングのヒント

このパラメータの最大値は 1440 分です。

[オプション] 予定表と統合する場合の多言語サポートの設定

この手順は、Microsoft Exchange サーバ 2003 または 2007 を WebDAV 経由で統合する場合にのみ必要となります。 予定表を EWS 経由で統合する場合、この手順を実行する必要はありません。

ユーザ ロケールは国特有のものです。ユーザ ロケール ファイルは、指定のロケールのユーザ アプリケーションおよびユーザ Web ページ向けに翻訳されたテキストを提供します。 Microsoft Exchange の導入を拡張し、多言語をサポートできるようにするには、予定表の統合に必要なユーザ ロケールをサポートするよう Cisco Unified Communications Manager と IM and Presence を設定する必要があります。 サポートされる言語の数には上限はありません。

- Cisco Unified Communications Manager へのロケール インストーラのインストール, （44 ページ）
- IM and Presence へのロケール インストーラのインストール, （45 ページ）
- 多言語の予定表と統合する場合のユーザ ロケールの設定, （47 ページ）

Cisco Unified Communications Manager へのロケール インストーラのインストール

この手順を実行する前に、次の補足情報を考慮に入れてください。

- Cisco Unified Communications Manager ロケール インストーラをインストールする前に、クラスタ内の各サーバに Cisco Unified Communications Manager（Release 6.x 以降）をインストールする必要があります。
- インストールされるロケールのデフォルト設定は、「英語（米国）（English United States）」です。 Cisco Unified Communications Manager に適切な言語/ロケールをインストールし、ユーザが最初にサイン インするときに Exchange サーバで適切な言語/ロケールを選択することを強く推奨します。 WebDAV での統合に対してのみ適用される、次の事項も考慮に入れてください。
  - Cisco Unified Communications Manager に別の言語/ロケールがインストールされているときにエンド ユーザの Exchange メールボックスにデフォルト言語（英語）を設定した場合、それ以降にそのユーザのロケールを変更することはできません。 この問題の詳細については、WebDAV による予定表の統合に関するローカリゼーションの補足説明, （81 ページ）を参照してください。

- 英語以外のロケールを使用する場合は、Cisco Unified Communications Manager と IM and Presence の両方に適切な言語インストーラをインストールする必要があります。 クラスタ内のすべてのサーバにロケールインストーラをインストールしてください（パブリッシャ サーバにインストールしてからサブスクライバ サーバにインストールします）。

- 適切なすべてのロケールインストーラが両方のシステムにロードされるまで、ユーザ ロケールを設定しないでください。 ロケール インストーラが Cisco Unified Communications Manager にロードされた後であっても、IM and Presence にロードされる前にユーザがユーザ ロケールを設定してしまうと、予定表が正しく動作しないことがあります。 問題が報告された場合は、各ユーザに対し、Cisco Unified Communications Manager の [ユーザ オプション（User Options）] ページにサイン インし、ロケールを現在の設定から [英語（English）] に変更してから適切な現在に戻すように指示することを推奨します。 BAT ツールを使用してユーザ ロケールを適切な現在に同期させることもできます。
- 変更を有効にするためには、サーバを再起動する必要があります。 ロケールのインストール手順がすべて完了したら、クラスタ内の各サーバを再起動してください。 クラスタ内のすべてのサーバを再起動するまで、システム内で更新は行われません。サーバの再起動後にサービスが再開されます。
- クラスタ内のすべてのサーバに同じコンポーネントをインストールしてください。

この手順を Cisco Unified Communications Manager で実行する方法については、次の URL にある『Cisco Unified Communications Operating System Administration Guide』を参照してください。

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/cucos/8_0_1/cucos/iptpch7.html#wp1054072

次の作業

Cisco Unified Communications Manager へのロケール インストーラのインストール, （44 ページ）

IM and Presence へのロケール インストーラのインストール

はじめる前に

- Cisco Unified Communications Manager にロケール インストーラをインストールします。 英語以外のロケールを使用する場合は、Cisco Unified Communications Manager と IM and Presence に適切な言語インストーラをインストールする必要があります。
- IM and Presence クラスタに複数のノードがある場合は、クラスタ内のすべてのサーバにロケール インストーラをインストールしてください（パブリッシャ サーバにインストールしてからサブスクライバ サーバにインストールします）。
- 適切なすべてのロケールインストーラが両方のシステムにロードされるまで、ユーザ ロケールを設定しないでください。 ロケール インストーラが Cisco Unified Communications Manager にロードされた後であっても、IM and Presence にロードされる前にユーザがユーザ ロケールを設定してしまうと、予定表が正しく動作しないことがあります。 問題が報告された場合は、各ユーザに対し、Cisco Unified Communications Manager の [ユーザ オプション（User Options）] ページにサイン インし、ロケールを現在の設定から [英語（English）] に変更して

から適切な現在に戻すように指示することを推奨します。 BAT ツールを使用してユーザ ロケールを適切な現在に同期させることもできます。

- 変更を有効にするためには、サーバを再起動する必要があります。 ロケールのインストール手順がすべて完了したら、クラスタ内の各サーバを再起動してください。 クラスタ内のすべてのサーバを再起動するまで、システム内で更新は行われません。サーバの再起動後にサービスが再開されます。

手順

ステップ 1 IM and Presence ロケール インストーラを入手するには、Cisco.com のこのページにアクセスします。

ステップ 2 作業環境に適した IM and Presence ロケール インストーラ バージョンを選択します。

ステップ 3 ファイルをダウンロードしたら、ハード ドライブに保存し、ファイルの保存場所をメモします。

ステップ 4 SFTP をサポートするサーバにこのファイルをコピーします。

ステップ 5 管理者アカウントとパスワードを使用し、[Cisco Unified IM and Presence OS の管理（Cisco Unified IM and Presence Operating System Administration）] にサイン インします。

ステップ 6 [ソフトウェア アップグレード（Software Upgrades）] > [インストール/アップグレード（Install/Upgrade）] を選択します。

ステップ 7 ソフトウェアの入手先として [リモート ファイル システム（Remote File System）] を選択します。

ステップ 8 [ディレクトリ（Directory）] フィールドにファイルの保存場所（/tmp など）を入力します。

ステップ 9 ロケール インストーラ ファイルが保存されているサーバ（ステップ 4, （46 ページ） で指定したサーバ）の名前を入力します。 これにより、ロケール インストーラ ファイルが IM and Presence サーバにコピーされ、インストールできるようになります。

ステップ 10 [ユーザ名（User Name）] フィールドと [ユーザ パスワード（User Password）] フィールドに自分のユーザ名とパスワードを入力します。

ステップ 11 [転送プロトコル（Transfer Protocol）] で [SFTP] を選択します。

ステップ 12 [次へ（Next）] を選択します。

ステップ 13 検索結果のリストから IM and Presence ロケール インストーラを選択します。

ステップ 14 [次へ（Next）] を選択してインストーラ ファイルをロードし、検証します。

ステップ 15 ロケールのインストールが完了したら、クラスタ内の各サーバを再起動します。

ステップ 16 インストールされるロケールのデフォルト設定は、「英語（米国）（English United States）」です。 IM and Presence の再起動中に、必要に応じて、ダウンロードしたインストーラのロケールに合わせてブラウザの言語を変更してください。

使用するブラウザ	設定手順
Internet Explorer バージョン 6.x	**1** [ツール（Tools）]>[インターネット オプション（Internet Options）] を選択します。 **2** [全般（General）] タブを選択します。 **3** [言語（Languages）] を選択します。 **4** [上へ（Move Up）] ボタンを使用して、優先する言語をリストの先頭に移動します。 **5** [OK] を選択します。
Mozilla Firefox バージョン 3.x	**1** [ツール（Tools）] > [オプション（Options）] を選択します。 **2** [コンテンツ（Content）] タブを選択します。 **3** [言語（Languages）] セクションの [言語設定（Choose）] を選択します。 **4** [上へ（Move Up）] ボタンを使用して、優先する言語をリストの先頭に移動します。 **5** [OK] を選択します。

ステップ 17 ユーザがサポートされている製品のロケールを選択できることを確認します。

トラブルシューティングのヒント

クラスタ内のすべてのサーバに同じコンポーネントをインストールしてください。

次の作業

多言語の予定表と統合する場合のユーザ ロケールの設定, （47 ページ）

多言語の予定表と統合する場合のユーザ ロケールの設定

はじめる前に

- 使用可能なすべての言語が含まれている、Cisco Unified Communications Manager および IM and Prsence のロケール インストーラをインストールします。 適切なすべてのロケール インストーラが両方のシステムにロードされるまで、ユーザ ロケールを設定しないでください。
- インストールされるロケールのデフォルト設定は、「英語（米国）（English United States）」です。 Cisco Unified Communications Manager に適切な言語/ロケールをインストールし、ユーザが最初にサイン インするときに Exchange サーバで適切な言語/ロケールを選択することを

強く推奨します。 Cisco Unified Communications Manager に別の言語/ロケールがインストールされているときにエンド ユーザの Exchange メールボックスにデフォルト言語（英語）を設定した場合、それ以降にそのユーザのロケールを変更することはできません。 この問題に関する詳細については、WebDAV での予定表統合に関するローカライズの補足情報についてのトピックを参照してください。

- ロケール インストーラが Cisco Unified Communications Manager にロードされた後であっても、IM and Presence にロードされる前にユーザ ロケールを設定してしまうと、予定表が正しく動作しないことがあります。 システムが適切な言語を使用するようにするには、Cisco Unified Communications Manager のユーザ ページにサイン インし、ユーザ ロケールを現在の設定から英語に変更することを推奨します。 その後、ロケールを必要な言語に戻します。

手順

次の表のうち自分のロール（管理者またはユーザ）に対応する手順を実行します。

a) 管理者の場合は、次の操作を実行します。

1. 管理者のアカウントとパスワードを使用して Cisco Unified Communications Manager の管理画面にログインします。
2. [ユーザ管理（User Management）] > [エンド ユーザ（End User）] を選択します。
3. 検索と一覧表示機能を使用して、必要なユーザを検索します。
4. 必要なユーザの [ユーザ ID（User ID）] ハイパーリンクを選択します。
5. [ユーザ ロケール（User Locale）] ドロップダウン リストからユーザの適切な言語を選択します。

b) ユーザの場合は、次の操作を実行します。

1. ユーザのアカウントおよびパスワードを使用して [Cisco Unified Communications Manager のユーザ オプション（Cisco Unified Communications Manager User Options）] にサイン インします。
2. [ユーザ オプション（User Options）] > [ユーザ設定（User Settings）] を選択します。
3. [ユーザ ロケール（User Locale）] ドロップダウン リストからユーザの適切な言語を選択します。
4. [保存（Save）] を選択します。

関連トピック

Cisco Unified Communications Manager へのロケール インストーラのインストール, （44 ページ）
IM and Presence へのロケール インストーラのインストール, （45 ページ）
WebDAV による予定表の統合に関するローカリゼーションの補足説明, （81 ページ）

[オプション] Microsoft Exchange 通知ポートの設定

このトピックは、プレゼンスエンジンにおいてExchangeサーバからの通知をネットワーク設定に固有の別のポートで受信する場合にのみ当てはまります。 この手順は、WebDAV と EWS の両方の Exchange 設定を対象とします。

WebDAV 統合では、HTTPU 通知の受信にデフォルトで UDP ポート 50020 が使用されます。 EWS 統合では、HTTP 通知の受信にデフォルトで TCP ポートが使用されます。

はじめる前に

デフォルト ポート以外のポートを使用する場合は、必ず未使用のポートを割り当ててください。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [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（Server）] メニューから IM and Presence サーバを選択します。

ステップ 3 [サービス（Service）] メニューから [Cisco Presence Engine（アクティブ）（Cisco Presence Engine (Active)）] を選択します。

ステップ 4 [プレゼンス エンジン構成（Presence Engine Configuration）] セクションの [Microsoft Exchange 通知ポート（Microsoft Exchange Notification Port）] フィールドのパラメータ値を編集します。 WebDAV 設定の場合、このパラメータのデフォルト値は 50020 です。

ステップ 5 [保存（Save）] を選択します。

次の作業

一度にすべてのユーザのパラメータ変更を有効にするために、Cisco Presence Engine を再起動することを推奨します。 [Cisco Unified IM and Presence のサービスアビリティ（Cisco Unified IM and Presence Serviceability）] > [ツール（Tools）] > [サービスの開始（Service Activation）] を選択します。

トラブルシューティングのヒント

- ポートをデフォルト以外に変更した場合、そのユーザのExchangeサブスクリプションが更新されるまで、プレゼンスエンジンはユーザの既存の予定表情報（会議数、開始時刻、終了時刻など）を使用し続けます。 プレゼンス エンジンがユーザの予定表の変更通知を受け取るまでに最大で 1 時間かかることがあります。
- 一度にすべてのユーザの変更を有効にするために、Cisco Presence Engine を再起動することを推奨します。

[オプション] Microsoft Exchange 予定表通知の接続時間の設定

デフォルトでは、プレゼンス エンジンは会議/取り込み中通知を発生から 50 秒で送信できます。ユーザ数が少ない場合は、この手順に示す方法に従って、この遅延を短くすることを推奨します。ただし、この手順は任意です。ネットワーク設定に特有の理由から接続時間を変更する必要がある場合にのみ実行してください。

はじめる前に

この手順では、フィールド値（秒数）を「割り当てられたユーザの最大数/100」に設定します。たとえば、ユーザの最大数が 1000 である場合、オフセット範囲は 10 秒となります。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [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（Server）] メニューから IM and Presence サーバを選択します。

ステップ 3 [サービス（Service）] メニューから [Cisco Presence Engine（アクティブ）（Cisco Presence Engine (Active)）] を選択します。

ステップ 4 [予定表スプレッド（Calendar Spread）] フィールドのパラメータ値を編集します。 このパラメータのデフォルト値は 50 です。

ステップ 5 [保存（Save）] を選択します。

次の作業

[予定表スプレッド（Calendar Spread）] パラメータの変更は、ユーザ単位で予定表の統合が発生するたびに付加的に更新されます。 ただし、すべてのユーザについてパラメータの変更を有効にするために、Cisco Presence Engine を再起動することを推奨します。 [Cisco Unified IM and Presence のサービスアビリティ（Cisco Unified IM and Presence Serviceability）] > [ツール（Tools）] > [サービスの開始（Service Activation）] を選択します。

トラブルシューティングのヒント

- このパラメータの最大値は 59 秒です。 会議の開始または終了が 1 分を超えて遅れた場合、会議の開始/終了カウンタおよび通知に影響します。
- 多数のユーザが会議に出入りすると、大量の通知イベントが発生し、一部の通知に最大で数分の遅れが生じることがあります。

その他の Microsoft Exchange パラメータ

[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] の [サービスパラメータ（Service Parameters）] ウィンドウで設定できる Microsoft Exchange の予定表パラメータには、他にも 3 つあります。

- [Exchange タイムアウト（秒）（Exchange Timeout (seconds)）]：Exchange サーバに対するリクエストがタイムアウトするまでの秒単位の時間。
- [Exchange キュー（Exchange Queue）]：リクエスト キューの長さ。
- [Exchange スレッド（Exchange Threads）]：Exchange リクエストにサービスを提供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のデフォルト設定を変更しないことをお勧めします。パラメータを変更すると、Microsoft Exchange との統合に悪影響が及ぶ可能性があります。 サポートについては、Cisco Technical Assistance Center（TAC）にお問い合わせください。

第 5 章

IM and Presence と Microsoft Exchange 間のセキュアな証明書交換

- 自己署名証明書およびサードパーティ証明書の交換の管理，53 ページ
- 認証局（CA）サービスのインストール，55 ページ
- Exchange サーバの IIS での CSR の生成，59 ページ
- CA サーバ/認証局への CSR の提出，61 ページ
- 署名付き証明書のダウンロード，63 ページ
- 署名付き証明書の Exchange IIS へのアップロード，64 ページ
- ルート証明書のダウンロード，66 ページ
- ルート証明書の IM and Presence サーバへのアップロード，67 ページ

自己署名証明書およびサードパーティ証明書の交換の管理

自己署名証明書およびサードパーティ証明書のセキュアな交換を設定する手順の概要を次の表に示します。

表 7：自己署名証明書およびサードパーティ証明書チェックリスト

設定手順		設定方法
ステップ 1：	[Cisco Unity Connection の管理（Cisco Unity Connection Administration）] から [システム設定（System Settings）]>[エンタープライズ パラメータ（Enterprise Parameters）] を選択し、トレース可能な最大デバイス数を設定する。[デバイス レベル トレースの最大数（Max Number of Device Level Trace）] フィールドに値を入力します。デフォルトは 12 です。	『Cisco Unity Connection System Administration Guide』
ステップ 2：	証明書 CA サービスをインストールする。	**自己署名証明書** 認証局（CA）サービスのインストール，（55 ページ）
ステップ 3：	Exchange サーバの IIS で CSR を作成する。	**自己署名証明書** Exchange サーバの IIS での CSR の生成，（59 ページ） **サードパーティ証明書** Exchange サーバの IIS での CSR の生成，（59 ページ）
ステップ 4：	CA サーバ/認証局に CSR を提出する。	**自己署名証明書** CA サーバ/認証局への CSR の提出，（61 ページ） **サードパーティ証明書** 認証局に CSR を要求します。
ステップ 5：	署名済みの証明書をダウンロードする。	**自己署名証明書** 署名付き証明書のダウンロード，（63 ページ） **サードパーティ証明書** 認証局から署名付き証明書が提供されます。

設定手順		設定方法
ステップ 6：	署名付き証明書を Exchange IIS にアップロードする。	**自己署名証明書** 署名付き証明書の Exchange IIS へのアップロード，（64 ページ） **サードパーティ証明書** 署名付き証明書の Exchange IIS へのアップロード，（64 ページ）
ステップ 7	ルート証明書をダウンロードする。	**自己署名証明書** ルート証明書のダウンロード，（66ページ） **サードパーティ証明書** 認証局にルート証明書を要求する。
ステップ 8：	ルート証明書を IM and Presence サーバにアップロードする。	**自己署名証明書** ルート証明書の IM and Presence サーバへのアップロード，（67 ページ） **サードパーティ証明書** サードパーティの CA 署名付きの Exchange サーバ証明書がある場合は、証明書チェーン内のすべての CA 証明書を IM and Presence の信頼証明書（cup-trust）として IM and Presence にアップロードする必要があります。

認証局（CA）サービスのインストール

CA は Exchange サーバ上で実行することもできますが、サードパーティの証明書交換のセキュリティを強化するために、別の Windows サーバを認証局（別名 CA）として使用することをお勧めします。

- Windows Server 2003 への CA のインストール，（56 ページ）
- Windows Server 2008 への CA のインストール，（57 ページ）

Windows Server 2003 への CA のインストール

はじめる前に

- 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 コンピュータにデフォルトでインストールされません。
- Windows Server ディスク 1 および SP1 ディスクがあることを確認します。

手順

ステップ 1 [スタート（Start）] > [コントロール パネル（Control Panel）] > [プログラムの追加と削除（Add or Remove Programs）] の順に選択します。

ステップ 2 [プログラムの追加と削除（Add or Remove Programs）] ウィンドウで [Windows コンポーネントの追加と削除（Add/Remove Windows Components）] を選択します。

ステップ 3 [Windows コンポーネント（Windows Components）] ウィザードの 1 ページ目の [Components（コンポーネント）] で [証明書サービス（Certificate Services）] を選択し、ドメインのメンバーシップとコンピュータの名前変更の制約に関する警告が表示されたら [はい（Yes）] を選択します。

ステップ 4 [Windows コンポーネント（Windows Components）] ウィザードの 2 ページ目で [スタンドアロンのルート CA（Stand-alone Root CA）] を選択し、[次へ（Next）] を選択します。

ステップ 5 [Windows コンポーネント（Windows Components）] ウィザードの 3 ページ目で、CA サーバの [共通名（Common Name）] フィールドにサーバ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ください。 [次へ（Next）] を選択します。

ステップ 6 [Windows コンポーネント（Windows Components）] ウィザードの 4 ページ目でデフォルトの設定を受け入れ、[次へ（Next）] を選択します。

ステップ 7 Internet Information Services を停止するよう指示されたら [はい（Yes）] を選択します。

ステップ 8 Active Server Pages（ASP）を有効にするよう指示されたら [はい（Yes）] を選択します。

ステップ 9 インストール手順が完了したら [終了（Finish）] を選択します。

トラブルシューティングのヒント

CA はサードパーティの権限であることを覚えておいてください。 CA の共通名と、CSR の生成に使用された共通名を同じにすることはできません。

次の作業

CSR の生成（Windows Server 2008）, （60 ページ）

Windows Server 2008 への CA のインストール

手順

ステップ 1 [スタート（Start）]>[管理ツール（Administrative Tools）]>[サーバマネージャー（Server Manager）] を選択します。

ステップ 2 コンソール ツリーで [役割（Roles）] を選択します。

ステップ 3 [操作（Action）] > [役割の追加（Add Roles）] を選択します。

ステップ 4 [役割の追加（Add Roles）] ウィザードを完了します。

ウィンドウ	設定手順
[開始する前に（Before You Begin）] ウィンドウ 1/13 ページ	ウィンドウに表示されている前提条件をすべて満たしていることを確認し、[次へ（Next）] を選択します。
[サーバの役割の選択（Select Server Roles）] ウィンドウ 2/13 ページ	[Active Directory 証明書サービス（Active Directory Certificate Services）] にチェックを入れ、[次へ（Next）] を選択します。
[開始（Introduction）] ウィンドウ 3/13 ページ	[次へ（Next）] を選択します。
[役割サービスの選択（Select Role Services）] ウィンドウ 4/13 ページ	次のボックスを選択し、[次へ（Next）] を選択します。 • Certificate Authority • Certificate Authority Web Enrollment • Online Responder
[セットアップ タイプの指定（Specify Setup Type）] ウィンドウ 5/13 ページ	[スタンドアロン（Standalone）] を選択します。
[CA タイプの指定（Specify CA Type）] ウィンドウ 6/13 ページ	[ルート CA（Root CA）] を選択します。

ウィンドウ	設定手順
[秘密キーの設定（Set Up Private Key）] ウィンドウ 7/13 ページ	[新しい秘密キーを作成する（Create a new private key）] を選択します。
[CA の暗号化を設定（Configure Cryptography for CA）] ウィンドウ 8/13 ページ	デフォルトの暗号化サービス プロバイダーを選択します。
[CA 名の設定（Configure CA Name）] ウィンドウ 9/13 ページ	CA を識別する共通名を入力します。
[有効期限の設定（Set Validity Period）] ウィンドウ 10/13 ページ	CA に対して生成された証明書の有効期間を設定します。 （注） CA が発行する証明書は、ここで指定した期日まで有効です。
[証明書データベースを構成（Configure Certificate Database）] ウィンドウ 11/13 ページ	証明書データベースの場所をデフォルトのままにします。
[インストール内容の確認（Confirm Installation Selections）] ウィンドウ 12/13 ページ	[インストール（Install）] を選択します。
[インストールの結果（Installation Results）] ウィンドウ 13/13 ページ	すべてのコンポーネントについて、[インストールが正常に完了しました（Installation Succeeded）] というメッセージが表示されていることを確認し、[閉じる（Close）] を選択します。 （注） サーバ マネージャに役割の 1 つとして [Active Directory 証明書サービス（Active Directory Certificate Services）] が表示されます。

次の作業

Exchange サーバの IIS での CSR の生成, （59 ページ）

Exchange サーバの IIS での CSR の生成

- CSR の生成（Windows Server 2003），（59 ページ）
- CSR の生成（Windows Server 2008），（60 ページ）

CSR の生成（Windows Server 2003）

Exchange の IIS で証明書の署名要求（CSR）を作成する必要があります。作成した CSR は CA サーバによって署名されます。 証明書の [サブジェクトの別名（Subject Alternative Name (SAN)）] フィールドに値が入力されている場合、その値は証明書の共通名（CN）と一致している必要があります。

はじめる前に

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ます。

手順

ステップ 1 [管理ツール（Administrative Tools）] から [インターネット インフォメーション サービス（Internet Information Services）] を開きます。

ステップ 2 [既定の Web サイト（Default Web Site）] を右クリックし、[プロパティ（Properties）] を選択します。

ステップ 3 [ディレクトリ セキュリティ（Directory Security）] タブを選択します。

ステップ 4 [サーバ証明書（Server Certificate）] を選択し、[次へ（Next）] を選択します。

ステップ 5 [新しい証明書の作成（Create a new certificate）] を [サーバ証明書（Server Certificate）] ウィンドウから選択し、[次へ（Next）] を選択します。

ステップ 6 [証明書の要求の送信方法（Delayed or Immediate Request）] ウィンドウで [証明書の要求を作成して後で送信する（Prepare the request now, but send it later）] を選択し、[次へ（Next）] を選択します。

ステップ 7 デフォルトの Web サイト証明書名を受け入れ、[名前およびセキュリティの設定（Name and Security Settings）] でビット長として [2048] を選択し、[次へ（Next）] を選択します。

ステップ 8 [組織情報（Organization Information）] ウィンドウの [組織（Organization）] フィールドに会社名、[組織単位（Organizational Unit）] フィールドに部署名をそれぞれ入力し、[次へ（Next）] を選択します。

ステップ 9 Exchange サーバのホスト名と IP アドレスを [サイトの一般名（Your Site's Common Name）] ウィンドウの [共通名（Common Name）] フィールドに入力し、[次へ（Next）] を選択します。

（注） ここで入力する IIS 証明書の一般名は、IM and Presence でプレゼンス ゲートウェイを設定するときに使用されるため、接続先のホスト（URI または IP アドレス）と一致している必要があります。

ステップ 10 [地理情報（Geographical Information）] ウィンドウに地理情報を入力し、[次へ（Next）] を選択します。

ステップ 11 [証明書要求ファイル名（Certificate Request File Name）] ウィンドウに、証明書要求の適切な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（Next）] を選択します。

（注） CSR は拡張子（.txt）なしで保存してください。この CSR ファイルを後で探す必要があるため、保存場所を覚えておいてください。 このファイルを開くには、必ずメモ帳を使用します。

ステップ 12 [要求ファイルの概要（Request File Summary）] ウィンドウに表示されている情報に誤りがないことを確認し、[次へ（Next）] を選択します。

ステップ 13 [完了（Finish）] を選択します。

次の作業

CA サーバ/認証局への CSR の提出, （61 ページ）

CSR の生成（Windows Server 2008）

Exchange の IIS で証明書の署名要求（CSR）を作成する必要があります。作成した CSR は CA サーバによって署名されます。

手順

ステップ 1 [管理ツール（Administrative Tools）] から [インターネット インフォメーション サービス（IIS）マネージャ（Internet Information Services (IIS) Manager）] を開きます。

ステップ 2 IIS マネージャの左側のフレームにある [接続（Connections）] ウィンドウで [Exchange Server] を選択します。

ステップ 3 [サーバ証明書（Server Certificates）] をダブルクリックします。

ステップ 4 IIS マネージャの右側のフレームにある [操作（Actions）] ウィンドウで [証明書の要求の作成（Create Certificate Request）] を選択します。

ステップ 5 [識別名プロパティ（Distinguished Name Properties）] ウィンドウに関連情報を入力し、[次へ（Next）] を選択します。

a) [共通名（Common Name）] フィールドに Exchange Server ホスト名または IP アドレスを入力します。

（注） ここで入力する IIS 証明書の一般名は、IM and Presence でプレゼンス ゲートウェイを設定するときに使用されるため、接続先のホスト（URI または IP アドレス）と一致している必要があります。

b) [組織（Organization）] フィールドに会社名を入力します。

c) [組織単位（Organizational Unit）] フィールドに部署名を入力します。

d) 地理情報を入力します。

ステップ 6 デフォルトの暗号化サービスプロバイダーを受け入れ、[暗号化サービスプロバイダのプロパティ（Cryptographic Service Provider Properties）] ウィンドウでビット長を [2048] に設定し、[次へ（Next）] を選択します。

ステップ 7 [証明書要求ファイル名（Certificate Request File Name）] ウィンドウで証明書要求の適切なファイル名を入力し、[次へ（Next）] を選択します。

（注） CSR は拡張子（.txt）なしで保存してください。この CSR ファイルを後で探す必要があるため、保存場所を覚えておいてください。 このファイルを開くには、必ずメモ帳を使用します。

ステップ 8 [要求ファイルの概要（Request File Summary）] ウィンドウに表示されている情報に誤りがないことを確認し、[次へ（Next）] を選択します。

ステップ 9 [完了（Finish）] を選択します。

次の作業

CA サーバ/認証局への CSR の提出, （61 ページ）

CA サーバ/認証局への CSR の提出

IIS で Exchange 用に作成されるデフォルトの SSL 証明書には、Exchange サーバの完全修飾ドメイン名（FQDN）を使用し、IM and Presence が信頼している認証局の署名を付けることを推奨します。 この手順により、CA が Exchange IIS からの CSR に署名できます。 次の手順を CA サーバで実行し、次の場所にある Exchange サーバの FQDN を設定してください。

- Exchange 証明書
- [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] の Exchange プレゼンス ゲートウェイの [プレゼンス ゲートウェイ（Presence Gateway）] フィールド。

はじめる前に

Exchange サーバの IIS で CSR を作成します。

手順

ステップ 1 証明書要求ファイルを CA サーバにコピーします。

ステップ 2 次のいずれかの URL にアクセスします。

- Windows 2003 または Windows 2008：http://local-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 [証明書の要求（Request a certificate）] を選択します。

ステップ 4 [詳細証明書要求（advanced certificate request）] を選択します。

ステップ 5 [ベース 64 エンコード 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か、ベース 64 エンコード PKCS #7 ファイルを使用して更新要求を送信する（Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file）] を選択します。

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

ステップ 7 次の行から、
-----BEGIN CERTIFICATE REQUEST

次の行までの情報をすべてコピーします。

END CERTIFICATE REQUEST-----

ステップ 8 CSR の内容を [証明書要求（Certificate Request）] テキストボックスに貼り付けます。

ステップ 9 （任意）[証明書テンプレート（Certificate Template）] ドロップダウン リストのデフォルト値は [管理者（Administrator）]テンプレートです。このテンプレートでは、サーバの認証に適した有効な署名付き証明書が作成されることもあれば、作成されないこともあります。 エンタープライズのルート CA がある場合は、[証明書テンプレート（Certificate Template）] ドロップダウン リストから [Web サーバ（Web Server）] 証明書テンプレートを選択してください。 [Web サーバ（Web Server）] 証明書テンプレートは表示されないことがあるため、CA 設定をすでに変更している場合、この手順は不要となることがあります。

ステップ 10 [送信（Submit）] を選択します。

ステップ 11 [管理ツール（Administrative Tools）] で [スタート（Start）] > [管理ツール（Administrative Tools）] > [証明（Certification）] > [機関（Authority）] > [CA 名（CA name）] > [保留中の要求（Pending Request）] を選択し、認証局を開きます。 [認証局（Certificate Authority）] ウィンドウの [保留中の要求（Pending Requests）] の下に、送信したばかりの要求が表示されます。

ステップ 12 要求を右クリックし、次の操作を実行します。

- [すべてのタスク（All Tasks）] を選択します。
- [発行（Issue）] を選択します。

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

次の作業

署名付き証明書のダウンロード, （63 ページ）

署名付き証明書のダウンロード

はじめる前に

自己署名証明書：CA サーバに CSR を提出します。

サードパーティ証明書：認証局に CSR を要求します。

手順

ステップ 1 [管理ツール（Administrative Tools）] から [認証局（Certification Authority）] を開きます。 先ほど発行した証明書の要求が [発行済み要求（Issued Requests）] に表示されます。

ステップ 2 その要求を右クリックし、[開く（Open）] を選択します。

ステップ 3 [詳細（Details）] タブを選択します。

ステップ 4 [ファイルのコピー（Copy to File）] を選択します。

ステップ 5 [証明書のエクスポート ウィザード（Certificate Export Wizard）] が表示されたら、[次へ（Next）] を選択します。

ステップ 6 証明書のエクスポート ウィザードを完了します。

ウィンドウ	設定手順
[エクスポート ファイル形式（Export File Format）] ウィンドウ 1/3 ページ	[Base-64 encoded X.509] を選択し、[次へ（Next）] を選択します。
[エクスポートするファイル（File to Export）] ウィンドウ 2/3 ページ	証明書の保存場所を入力します。証明書の名前には **cert.cer** を使用します（c:\cert.cer など）。 [次へ（Next）] を選択します。
[証明書エクスポートウィザードの完了（Certificate Export Wizard Completion）] ウィンドウ 3/3 ページ	表示されている概要情報に目を通し、エクスポートが成功したことを確認して [完了（Finish）] を選択します。

ステップ 7 IM and Presence の管理に使用するコンピュータに、cert.cer をコピーするか、FTP で送信します。

次の作業

署名付き証明書の Exchange IIS へのアップロード, （64 ページ）

署名付き証明書の Exchange IIS へのアップロード

- 署名付き証明書のアップロード（Windows 2003）, （64 ページ）
- 署名付き証明書のアップロード（Windows 2008）, （65 ページ）

署名付き証明書のアップロード（Windows 2003）

ここでは、署名付き CSR を IIS にアップロードする手順を説明します。 署名付き証明書をアップロードするには、IM and Presence の管理に使用するコンピュータで次の手順を実行します。

はじめる前に

自己署名証明書：署名付き証明書をダウンロードします。

サードパーティ証明書：認証局から署名付き証明書が提供されます。

手順

ステップ 1 [管理ツール（Administrative Tools）] から [インターネット インフォメーション サービス（Internet Information Services）] を開きます。

ステップ 2 [インターネット インフォメーション サービス（Internet Information Services）] ウィンドウで次の手順を実行します。

a) [既定の Web サイト（Default Web Site）] を右クリックします。

b) [プロパティ（Properties）] を選択します。

ステップ 3 [既定の Web サイト（Default Web Site）] ウィンドウで次の手順を実行します。

a) [ディレクトリ セキュリティ（Directory Security）] タブを選択します。

b) [サーバ証明書（Server Certificate）] を選択します。

ステップ 4 [Web サーバ証明書ウィザード（Web Server Certificate Wizard）] ウィンドウが表示されたら、[次へ（Next）] を選択します。

ステップ 5 Web Server Certificate Wizard を完了します。

ウィンドウ	設定手順
[保留中の証明書要求（Pending Certificate Request）] ウィンドウ 1/4 ページ	[保留中の要求を処理し、証明書をインストールする（Process the Pending Request and Install the Certificate）] を選択し、[次へ（Next）] を選択します。

ウィンドウ	設定手順
[保留中の要求の処理（Process a Pending Request）] ウィンドウ 2/4 ページ	[参照（Browse）] を選択して証明書を探し、正しいパスとファイル名を選択して [次へ（Next）] を選択します。
[SSL ポート（SSL Port）] ウィンドウ 3/4 ページ	SSL ポートには **443** と入力し、[次へ（Next）] を選択します。
[サーバ証明書の完了（Server Certificate Completion）] ウィンドウ 4/4 ページ	[完了（Finish）] を選択します。

トラブルシューティングのヒント

証明書が信頼できる証明書ストアにない場合、署名付き CSR は信頼できません。 信頼を確立するには、次の操作を実行します。

- [ディレクトリ セキュリティ（Directory Security）] タブで [証明書の表示（View Certificate）] を選択します。
- [詳細（Details）] > [ルート証明書の強調表示（Highlight root certificate）] を選択し、[表示（View）] を選択します。
- ルート証明書の [詳細（Details）] タブを選択し、証明書をインストールします。

次の作業

ルート証明書のダウンロード, （66 ページ）

署名付き証明書のアップロード（Windows 2008）

ここでは、署名付き CSR を IIS にアップロードする手順を説明します。 署名付き証明書をアップロードするには、IM and Presence の管理に使用するコンピュータで次の手順を実行します。

はじめる前に

自己署名証明書：署名付き証明書をダウンロードします。

サードパーティ証明書：認証局から署名付き証明書が提供されます。

手順

ステップ 1 [管理ツール（Administrative Tools）] から [インターネット インフォメーション サービス（IIS）マネージャ（Internet Information Services (IIS) Manager）] を開きます。

ステップ 2 IIS マネージャの左側のフレームにある [接続（Connections）] ウィンドウで [Exchange Server] を選択します。

ステップ 3 [サーバ証明書（Server Certificates）] をダブルクリックします。

ステップ 4 IIS マネージャの右側のフレームにある [操作（Actions）] ウィンドウで [証明書要求の完了（Complete Certificate Request）] を選択します。

ステップ 5 [認証局の応答の指定（Specify Certificate Authority Response）] ウィンドウで次の操作を実行します。

a) 省略記号 [...] を選択して証明書を指定します。
b) 正しいパスおよびファイル名に移動します。
c) 証明書のわかりやすい名前を入力します。
d) [OK] を選択します。要求が完了した証明書が証明書のリストに表示されます。

ステップ 6 [インターネット インフォメーション サービス（Internet Information Services）] ウィンドウで次の手順を実行し、証明書をバインドします。

a) [既定の Web サイト（Default Web Site）] を選択します。
b) IIS マネージャの右側のフレームにある [操作（Actions）] ウィンドウで [バインディング（Bindings）] を選択します。

ステップ 7 [サイト バインディング（Site Bindings）] 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) [編集（Edit）] をクリックします。

ステップ 8 [サイト バインディングの編集（Edit Site Binding）] ウィンドウで次の手順を実行します。

a) SSL 証明書のリスト ボックスから、作成した証明書を選択します。 証明書に付けた「わかりやすい名前」が表示されます。
b) [OK] を選択します。

次の作業

ルート証明書のダウンロード, （66 ページ）

ルート証明書のダウンロード

はじめる前に

署名付き証明書を Exchange IIS にアップロードします。

手順

ステップ 1 CA サーバにサイン インし、Web ブラウザを開きます。

ステップ 2 使用している Windows プラットフォームの種類に応じ、次のいずれかの URL にアクセスします。

a) Windows server 2003：http://127.0.0.1/certserv

b) 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 のダウンロード（Download a CA certificate, certificate chain, or CRL）] を選択します。

ステップ 4 [エンコード方法（Encoding Method）] で、[Base 64] を選択します。

ステップ 5 [CA 証明書のダウンロード（Download CA Certificate）] を選択します。

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。

トラブルシューティングのヒント

ルート証明書のサブジェクトの共通名（CN）がわからない場合は、外部の証明書管理ツールを使用して調べることができます。 Windows オペレーティング システムで、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。

次の作業

ルート証明書の IM and Presence サーバへのアップロード, （67 ページ）

ルート証明書の IM and Presence サーバへのアップロード

はじめる前に

- 自己署名証明書：ルート証明書をダウンロードします。
- サードパーティ証明書：認証局にルート証明書を要求します。 CA 署名付きのサードパーティ Exchange サーバ証明書がある場合は、証明書チェーン内のすべての CA 証明書を Cisco Unified Presence の信頼証明書（cup-trust）として IM and Presence 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 and Presence の管理（Cisco Unified CM IM and Presence Administration）] の [証明書インポート ツール（Certificate Import Tool）] を使用して、次の操作を行います。

証明書のアップロード方法	アクション
[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] の [証明書インポート ツール（Certificate Import Tool）] [証明書インポート ツール（Certificate Import Tool）] は、信頼証明書を IM and Presence にインストールするプロセスを簡略化するもので、証明書交換の主要な方法です。 このツールでは、Exchange サーバのホストとポートを指定すると、サーバから証明書チェーンがダウンロードされます。 承認すると、欠落している証明書が自動的にインストールされます。 （注） この手順では、[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] の [証明書インポート ツール（Certificate Import Tool）] にアクセスし、設定する方法を 1 つ紹介します。 いずれかの形式での予定表統合のために Exchange プレゼンス ゲートウェイを設定した場合（[プレゼンス（Presence）]>[ゲートウェイ（Gateways）] の順に選択）、カスタマイズされた証明書インポートツールを表示することもできます。	**1** [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] の [システム（System）] > [セキュリティ（Security）] > [証明書インポート ツール（Certificate Import Tool）] を選択します。 **2** 証明書をインストールする証明書信頼ストアとして [CUP の信頼性（CUP Trust）] を選択します。 この証明書信頼ストアには、Exchange の統合に必要なプレゼンス エンジン信頼証明書が保存されます。 **3** Exchange サーバに接続するために、次のいずれかの値を入力します。 • IP アドレス • ホスト名 • FQDN この [ピア サーバ（Peer Server）] フィールドに入力する値は、Exchange サーバの IP アドレス、ホスト名、または FQDN と完全に一致している必要があります。 **4** Exchange サーバとの通信に使用するポートを入力します。 この値は、Exchange サーバの使用可能なポートと一致している必要があります。 **5** [送信（Submit）] を選択します。 ツールが完了すると、テストごとに次の状態が報告されます。 • ピア サーバの到達可能性ステータス：IM and Presence が Exchange サーバに到達（ping）できるかどうかを示します。 Exchange サーバの接続ステータスに関するトラブルシューティング, （71 ページ）を参照してください。 • SSL 接続/証明書の確認ステータス：証明書のインポート ツールが指定されたピア サーバから証明書をダウンロードすることに成功したかどうかと、IM and Presence とリモート サーバの間にセキュアな接続が確立されたかどうかを示します。 SSL 接続と証明書のステータスのトラブルシューティング, （72 ページ）を参照してください。

ステップ 2 証明書のインポート ツールによって、証明書が欠落していることがわかった場合は（通常、Microsoft サーバでは CA 証明書が欠落します）、Cisco Unified OS の管理画面の [証明書の管理（Certificate Management）] ウィンドウを使用して、手動で CA 証明書をアップロードしてください。

証明書のアップロード方法	アクション
Cisco Unified Operating System Administration Exchange サーバが SSL/TLS ハンドシェイク中に証明書を送信しない場合、それらの証明書は証明書のインポート ツールではインポートできません。 その場合は、Cisco Unified オペレーティング システムの管理画面にある証明書の管理ツール（[セキュリティ（Security）] > [証明書の管理（Certificate Management）] の順に選択）を使用して、欠落している証明書を手動でインポートする必要があります。	**1** IM and Presence サーバの管理に使用するコンピュータに、certnew.cer 証明書ファイルをコピーするか、FTP で送信します。 **2** [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] のログイン ウィンドウの [ナビゲーション（Navigation）] メニューから [Cisco Unified IM and Presence OS の管理（Cisco Unified IM and Presence OS Administration）] を選択し、[移動（Go）] を選択します。 **3** Cisco Unified IM and Presence オペレーティング システムの管理画面用のユーザ名とパスワードを入力して、[ログイン（Login）] を選択します。 **4** [セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択します。 **5** [証明書の一覧（Certificate List）] ウィンドウで [証明書のアップロード（Upload Certificate）] を選択します。 **6** [証明書のアップロード（Upload Certificate）] ポップアップ ウィンドウが表示されたら、次の操作を実行します。 • [証明書の名前（Certificate Name）] リスト ボックスから [cup-trust] を選択します。 • 拡張子を付けずにルート証明書の名前を入力します。 **7** [参照（Browse）] を選択し、[certnew.cer] を選択します。 **8** [ファイルのアップロード（Upload File）] を選択します。

ステップ 3 証明書のインポート ツール（ステップ 1, （67 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ます。

ステップ 4 すべての Exchange 信頼証明書をアップロードしたら、Cisco Presence Engine と SIP プロキシ サービスを再起動します。 [Cisco Unified IM and Presence のサービスアビリティ（Cisco Unified IM and Presence Serviceability）] > [ツール（Tools）] > [サービスの開始（Service Activation）] を選択します。

トラブルシューティングのヒント

- IM and Presence では、Exchange サーバの信頼証明書をサブジェクトの共通名（CN）あり/なしのどちらでもアップロードできます。
- 会議通知機能を使用する場合は、すべての種類の証明書についてプレゼンス エンジンと SIP プロキシを再起動する必要があります。 証明書をアップロードしたら、[Cisco Unified IM and Presence のサービスアビリティ（Cisco Unified IM and Presence Serviceability）] へ移動し、まずプレゼンスエンジン、次に SIP プロキシを再起動します。 これによって予定表の接続が影響を受ける可能性があることに注意してください。

第 6 章

Exchange 予定表の統合のトラブルシューティング

- Exchange サーバの接続ステータスに関するトラブルシューティング，71 ページ
- SSL 接続と証明書のステータスのトラブルシューティング，72 ページ
- Microsoft Exchange の統合に影響することが確認されている問題，78 ページ

Exchange サーバの接続ステータスに関するトラブルシューティング

Exchange サーバの接続ステータスは、WebDAV または EWS 経由での予定表の統合を Exchange プレゼンス ゲートウェイで設定後、[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] に表示されます（[プレゼンス（Presence）] > [ゲートウェイ（Gateways）] を選択）。[プレゼンス ゲートウェイの設定（Presence Gateway Configuration）] ウィンドウの [トラブルシューティング（Troubleshooter）] には、IM and Presence と Exchange サーバとの接続のステータスが表示されます。

（注） 1 台以上の 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（Presence Gateway）] ウィンドウの [トラブルシューティング（Troubleshooter）] は、設定した最初の 10 台までの EWS サーバのステータスのみを検証し、レポートするよう作られています。

.

テスト	ステータスの説明と推奨される処置
Exchange の到達可能性（ping 可能）	IM and Presence は Exchange サーバに正常に到達（ping）できました。

テスト	ステータスの説明と推奨される処置
Exchange の到達可能性（到達不可能）	IM and Presence は Exchange サーバに ping を送信できませんでした。 フィールド値が誤っているか、またはお客様のネットワークに何らかの問題（ケーブリングなど）があるため、サーバが到達不可になっていると考えられます。 これを解決するには、ネットワークを介して Exchange サーバに到達できるように [プレゼンス ゲートウェイ（Presence Gateway）] フィールドに適切な値（FQDN または IP アドレス）が設定されていることを確認します。 UI では、[プレゼンス ゲートウェイ（Presence Gateway）] フィールド値を件名 CN 値にする必要はありません。 Exchange サーバとの接続に問題がある場合は、[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] の [システム トラブルシュータ（System Troubleshooter）] も参照のうえ、推奨される解決策を実行してください。 [診断（Diagnostics）] > [システム トラブルシュータ（System Troubleshooter）] を選択します。

SSL 接続と証明書のステータスのトラブルシューティング

WebDAV または EWS による予定表の統合を行うために Exchange プレゼンス ゲートウェイを設定すると、SSL 接続/証明書の確認ステータスが Cisco Unified CM IM and Presence の管理 に表示されます（[プレゼンス（Presence）] > [ゲートウェイ（Gateways）] を選択）。 件名 CN の不一致か SAN の不一致があれば、[プレゼンス ゲートウェイ（Presence Gateway）] 設定ウィンドウの [Troubleshooter（トラブルシュータ）] に表示されます。

（注） 1 台以上の 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（Presence Gateway）] ウィンドウの [トラブルシュータ（Troubleshooter）] は、設定した最初の 10 台までの EWS サーバのステータスのみを検証し、レポートするよう作られています。

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	Exchange サーバとの SSL 接続が IM and Presence によって確認されました。 証明書の詳細を表示するには、[表示（View）] をクリックします。

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。 接続の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、その場合は[保存（Save）]することはできません。	

テスト	ステータスの説明と推奨される処置
	Exchange サーバとのセキュアな接続を確立するために IM and Presence で必要な 1 つ以上の証明書がない 証明書ビューアを使用すると、欠落している証明書の詳細を表示できます。 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して次の手順を実行します。 **1** [設定（Configure）] を選択して証明書ビューアを開きます。 **2** [証明書チェーンを許可（Accept Certificate Chain）] をオンにします。 **3** [保存（Save）] を選択します。 証明書チェーンの詳細が表示されます。 ステータスが [見つかりません（Missing）] になっている証明書を書き留めておきます。 **4** 証明書ビューアを閉じます。 **5** 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。 • 欠落している証明書ファイルを Exchange サーバからダウンロードします。 • IM and Presence を管理する目的に使用しているコンピュータに欠落している証明書ファイルをコピーまたは FTP 転送します。 • Cisco Unified IM and Presence OS の管理画面を使用して、欠落している必要な証明書をアップロードします。 **トラブルシューティングのヒント** • 証明書ビューアに証明書が表示されない場合は、欠落している証明書を Exchange サーバから手動でダウンロードしてインストールし、Cisco Unified OS IM and Presence の管理画面で次のようにアップロードする必要があります。 ◦ 必要であれば、Cisco Unified IM and Presence OS 管理ページに移動し、証明書をアップロードして証明書チェーンを完成させます。 ◦ Cisco Unified CM IM and Presence の管理の [プレゼンス ゲートウェイの設定（Presence Gateway Configuration）] ウィンドウに戻り、証明書ビューアをもう一度開いて、証明書チェーン内のすべての証明書のステータスが [Verified（確認が成功しました）] であることを確認します。

テスト	ステータスの説明と推奨される処置
	• Exchange の信頼証明書をアップロード後、Cisco Presence Engine を再起動する必要があります。 [Cisco Unified IM and Presence のサービスアビリティ（Cisco Unified IM and Presence Serviceability）] > [ツール（Tools）] > [サービスの開始（Service Activation）] を選択します。 これによって予定表の接続が影響を受ける可能性があることに注意してください。 • [設定（Configure）] または [表示（View）] を選択して証明書チェーン ビューアを開き、証明書チェーンの詳細を確認してください。 IM and Presence が Exchange サーバからダウンロードした証明書チェーンに問題（前述したように証明書が欠落しているなど）がある場合は、[設定（Configure）] ボタンが表示されます。 証明書チェーンをインポートし、確認すると、SSL 接続/証明書の確認ステータスが [確認が成功しました（Verified）] に更新され、[設定（Configure）] ボタンの代わりに [表示（View）] 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）] フィールドの値は、必ず証明書チェーン内のリーフ証明書の件名 CN 値と一致している必要があります。 これは、[プレゼンス ゲートウェイ（Presence Gateways）] フィールドに正しい値を入力することで解決できます。 [プレゼンス ゲートウェイ（Presence Gateways）] フィールドの値が正しいことを次の手順で確認してください。 **1** [プレゼンス ゲートウェイ（Presence Gateway）] フィールドに正しい件名 CN 値を再入力します。 IM and Presence では、[プレゼンス ゲートウェイ（Presence Gateway）] フィールドの値を使用して、サーバに ping を送信します。 入力したホスト（FQDN または IP アドレス）は、IIS 証明書のサブジェクトの CN と完全に一致している必要があります。 **2** [保存（Save）] を選択します。 **トラブルシューティングのヒント** [設定（Configure）] または [表示（View）] を選択して証明書チェーン ビューアを開き、証明書チェーンの詳細を確認してください。 Exchange サーバからダウンロードされた証明書チェーンに問題（前述したように証明書が欠落しているなど）がある場合は、[設定（Configure）] ボタンが表示されます。 証明書チェーンをインポートし、確認すると、SSL 接続/証明書の確認ステータスが [確認が成功しました（Verified）] に更新され、[設定（Configure）] ボタンの代わりに [表示（View）] 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 - SAN が一致しない	[プレゼンス ゲートウェイ（Presence Gateway）] フィールド値は、証明書チェーンのリーフ証明書のサブジェクトの別名（SAN）値のいずれかと一致する必要があります。 これは、[プレゼンス ゲートウェイ（Presence Gateways）] フィールドに正しい値を入力することで解決できます。 [プレゼンス ゲートウェイ（Presence Gateways）] フィールドの値が正しいことを次の手順で確認してください。 **1** [プレゼンス ゲートウェイ（Presence Gateway）] フィールドに正しい SAN 値を再入力します。 IM and Presence では、[プレゼンス ゲートウェイ（Presence Gateway）] フィールドの値を使用して、サーバに ping を送信します。 入力したホスト（FQDN または IP アドレス）は、証明書のサブジェクトの別名のいずれかのエントリと完全に一致する必要があります。 **2** [保存（Save）] を選択します。 **トラブルシューティングのヒント** [設定（Configure）] または [表示（View）] を選択して証明書チェーン ビューアを開き、証明書チェーンの詳細を確認してください。 Exchange サーバからダウンロードされた証明書チェーンに問題（前述したように証明書が欠落しているなど）がある場合は、[設定（Configure）] ボタンが表示されます。 証明書チェーンをインポートし、確認すると、SSL 接続/証明書の確認ステータスが [確認が成功しました（Verified）] に更新され、[設定（Configure）] ボタンの代わりに [表示（View）] 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/証明書の確認に失敗 - 不正な証明書	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なっています。 通常、この問題は、証明書が必要な件名 CN と一致しているものの公開キーとは一致していない場合に発生します。 これは、Exchange サーバが証明書を再生成したが、IM and Presence サーバに古い証明書が保持されたままの場合に見られる現象です。 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 Cisco Unified IM and Presence OS の管理の IM and Presence から削除し、新しい証明書を Cisco Unified IM and Presence OS の管理にアップロードします。 • このエラーの原因がサポートされていないアルゴリズムの場合は、サポートされているアルゴリズムを含む新しい証明書を Cisco Unified IM and Presence OS の管理にアップロードする必要があります。
SSL 接続/証明書の確認に失敗：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発生したために、IM and Presence が SSL 接続を確認できません。 Exchange サーバへのネットワーク接続を検証し、適切な IP アドレスとポート番号で Exchange サーバに接続できることを確認するようお勧めします。
SSL 接続/証明書の確認に失敗	不明確な原因または IM and Presence が到達可能性テストを実行できないことにより、確認が失敗しました。 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します。

MicrosoftExchangeの統合に影響することが確認されている問題

ここでは、Microsoft Exchange Server のバージョン（2003、2007、2010）に共通または特有の既知の問題について説明します。

• 予定表の統合に関する規模の上限, （79 ページ）
• ユーザが Exchange サーバ間で移動すると、予定表ステータスが更新されない, （79 ページ）

- LDAP ユーザの削除が IM and Presence にレプリケートされるまで 24 時間以上かかる，（80 ページ）
- WebDAV による予定表の統合に関するローカリゼーションの補足説明，（81 ページ）
- Exchange サーバに「Calendar」の訳語が含まれているかどうかの確認，（81 ページ）
- Microsoft のホットフィックス KB841561 の適用，（82 ページ）
- Exchange 2007 から「HTTP 503 サービス利用不可（HTTP 503 Service Unavailable）」エラーを解決する，（82 ページ）
- 会議通知のサポート，（84 ページ）

予定表の統合に関する規模の上限

IM and Presence と Exchange の予定表の統合は、予定表プレゼンスを購読するユーザの最大 X% と予定表の同時移行（会議への同時出席または同時退席など）を行うユーザの最大 Y% について検証されています。 特定の IM and Presence のリリースに関するパーセンテージ値については、表 8：特定の IM and Presence リリースの規模の上限，（79 ページ） を参照してください。

表 *8*：特定の *IM and Presence* リリースの規模の上限

ソフトウェア リリース	予定表プレゼンスを購読するユーザの %	予定表の同時移行を行うユーザの %
8.5(1)	50	30
8.5(2) 以降	100	50

（注） MCS-7825 プラットフォームの予定表の値は、リリース 8.5(1) に対して設定された値を超えてはなりません。

ユーザが Exchange サーバ間で移動すると、予定表ステータスが更新されない

問題

Exchange 管理者が、Exchange 統合内の Exchange サーバ間でユーザを移動すると、そのユーザの予定表ステータスの変更が更新されません。

原因

これは、ユーザがサーバ間を移動したときに Exchange サーバが通知しないために起こる現象です。

ソリューション

IM and Presence の管理者またはユーザは、Exchange 管理者がユーザを Exchange サーバ間で移動した後に、そのユーザの予定表統合を無効にしてから、もう一度有効にする必要があります。

LDAP ユーザの削除が IM and Presence にレプリケートされるまで 24 時間以上かかる

問題

LDAP からユーザを削除すると、そのユーザのステータス変更が Cisco Unified Communications Manager で非アクティブとなり、それ以降、クライアント アプリケーションでのユーザ認証は失敗します。 ただし、Cisco Unified Communications Manager が LDAP との間で変更を同期すると、管理者による強制的な同期またはスケジュールされた同期が実行された後24時間、ユーザは削除されないことがテストによって確認されています。

IM and Presence の Cisco Sync Agent は、ユーザが削除されるまでユーザのステータス変更を同期しません。 その間、ユーザは Cisco Unified Communications Manager 上に存在し続け、すべての IM and Presence 機能（Exchange 予定表購読を含む）のライセンスは 24 時間そのユーザに与えられたままになります。 このような遅延が生じるということは、LDAP から削除される前に Cisco Jabber にサイン インしていたユーザは、自動的にサイン アウトされないことを意味します。 ユーザの既存の予定表ステータス（[Available（応対可能）]、[Busy（話中）]）は、ユーザがクライアントからサイン アウトするまで IM and Presence に残されます。

原因

これは、Cisco Unified Communications Manager が設定され、LDAP 認証が使用される場合に見られる現象です。 ユーザが LDAP から削除されると、そのユーザの予定表購読は少なくとも 24 時間は IM and Presence 上に設定されたままの状態で更新されます。

ソリューション

ユーザが LDAP から削除されると、IM and Presence が Exchange の予定表購読をただちに終了し、ユーザをクライアントアプリケーションからサインアウトできるよう、そのユーザのライセンスを手動で削除することができます。 手動で削除しなければ、24時間の遅延が生じることがあります。

WebDAV による予定表の統合に関するローカリゼーションの補足説明

問題

Cisco Unified Communications Manager に別の言語/ロケールがインストールされているが、ユーザの Exchange メールボックスに対してデフォルトの言語（英語）を設定した場合、Exchange サーバはデフォルトの予定表名を保持し（英語）、そのユーザの言語/ロケールを変更することができません。 予定表の購読について 404 エラーが返されます。

原因

これは、ローカライズされた Exchange 2003/2007 を WebDAV 経由で統合する場合にのみ見られる現象です。 この問題は EWS 統合には影響しません。

ソリューション

- この問題の発生を防ぐには、Exchange の設定時に言語を正しく設定することを推奨します。 Cisco Unified Communications Manager に適切な言語/ロケールをインストールし、ユーザが最初にサイン インするときに Exchange サーバで適切な言語/ロケールを選択してください。
- ユーザの Exchange メールボックスの言語を英語に設定し、Cisco Unified Communications Manager に別の言語/ロケールがインストールされている場合は、そのユーザについて Cisco Unified Communications Manager の言語/ロケールを英語に戻す必要があります。 これを行うには、多言語の予定表と統合する場合のユーザ ロケールの設定, （47 ページ）を参照してください。

Exchange サーバに「Calendar」の訳語が含まれているかどうかの確認

予定表の統合をローカライズする場合は、Exchange サーバの URL に「Calendar」の訳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 と Cisco Unified Communications Manager に同じ言語ロケールをインストールします（ロケール インストーラを読み込む）。 IM and Presence にロケールをインストールする方法に

ついては、[オプション] 予定表と統合する場合の多言語サポートの設定, （44 ページ） を参照してください。

ステップ 2 IM and Presence サーバを再起動し、[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] にサイン インします。

ステップ 3 予定表について別のロケールをサポートしている既存の Exchange プレゼンス ゲートウェイを検索し、削除します（[プレゼンス（Presence）] > [ゲートウェイ（Gateways）] を選択）。

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（Add New）] を選択します。

ステップ 5 データベース（pebackendgateway テーブル）で、インストールした言語ロケールに 'localecalendarname' 属性が含まれていることを確認します。

ステップ 6 IM and Presence と Cisco Unified Communications Manager の両方にロケールをインストール後、ユーザ ロケールを設定します。必要であれば、Cisco Unified Communications Manager のユーザ ロケールを切り替えます。

Microsoft のホットフィックス KB841561 の適用

この問題は Microsoft Exchange 2003 でのみ発生します。 Exchange 2003 サーバで問題が発生し、「500 内部サーバ エラー（500 Internal Server Error）」が表示された場合は、Microsoft HotFix KB841561 を適用してください。

手順

ステップ 1 Windows Server 2003 および Microsoft Exchange 2003 の SP2 をアンインストールします。

ステップ 2 Windows Server 2003 および Exchange 2003 の SP1 をインストールします。

ステップ 3 次の URL から KB841561 をダウンロードし、インストールします。http://www.microsoft.com/downloads/details.aspx?familyid=050be883-11fc-4045-b988-c737e79c65d0&displaylang=enhttp://www.microsoft.com/downloads/details.aspx?familyid=050be883-11fc-4045-b988-c737e79c65d0&displaylang=en

ステップ 4 Windows Server 2003 および Microsoft Exchange 2003 の SP2 をインストールします。

Exchange 2007 から「HTTP 503 サービス利用不可（HTTP 503 Service Unavailable）」エラーを解決する

この問題は Microsoft Exchange 2007 でのみ発生します。

問題

Exchange 2007 以降においては、Outlook Web アクセスの URL が **/exchange** から **/owa** に変更されています。これは、OWA が Exchange 2007 メールボックス サーバ上のメールボックスにアクセスするときに使用する仮想ディレクトリです。 ところが、WebDAV 経由での Exchange 2007 との統

合では以前の URL が使用されているため、IM and Presence は SUSCRIBE 要求を常に /exchange 仮想ディレクトリに送信します。 Exchange Server 2007（SP1）でのテストでは、http://<server>/exchange を http://<server>/owa にリダイレクトすると、Exchange 2007 のインターネット インフォメーション サービス（IIS）マネージャ コンソールにエラー（HTTP 503 サービス利用不可（HTTP 503 Service Unavailable））が表示されることが確認されています。

原因

この問題は、Exchange 2007 SP1 を使用していて、Exchange 仮想ディレクトリのターゲット アドレスを Web メール用のデフォルト OWA ディレクトリにリダイレクトした場合に発生します。

ソリューション

「503 サービス利用不可（503 Service Unavailable）」エラー メッセージが表示された場合は、次の手順を実行してください。

手順

ステップ 1 [管理ツール（Administrative Tools）] から [インターネット インフォメーション サービス（Internet Information Services）] を開きます。

ステップ 2 IIS の Microsoft Exchange 仮想ディレクトリを削除します。

ステップ 3 表示される警告を確認し、推奨されているコマンドレットを Exchange 管理シェル（EMS）で実行します。

ステップ 4 このコマンドレットを EMS で実行することにより、Exchange 仮想ディレクトリが正しく設定されていることを確認し、ディレクトリを再度 IIS に追加します。

```
SyntaxNew-OwaVirtualDirectory -name exchange -OWAVersion Exchange2003or2000
 -VirtualDirectoryType mailboxes
```

ステップ 5 Exchange サーバによって仮想ディレクトリが IIS に設定されるのを待ちます。

ステップ 6 IIS を再起動します。

ステップ 7 完全なターゲット アドレス（http://mail.contoso.com/exchange/user@contoso.com/calendar など）を使用して、http://<server>/exchange/<user email address>/calendar をテストします。

ステップ 8 ユーザ名とパスワードの入力を求めるメッセージが表示されることを確認します。 これは、WebDAV が有効であり、仮想ディレクトリに正しく設定されていることを示します。 Active Directory のクレデンシャルを入力します。

ステップ 9 IM and Presence に対して表示される IIS ログを確認します。

ステップ 10 ログに 401 認証の問題が報告されている場合は、アクセスを認証するドメインを追加します。

ステップ 11 IIS を再起動します。

ステップ 12 [Cisco Unified IM and Presence Serviceability（Cisco Unified IM and Presence のサービスアビリティ）] > [ツール（Tools）] > [サービスの開始（Service Activation）] を選択し、Cisco Presence Engine を再起動します。

ステップ 13 再度 IIS ログを調べ、予定表に関して正しい SUBSCRIBE メッセージが含まれていることを確認します。
トラブルシューティングのヒント

この手順は、Microsoft Entourage 2008 を使用して電子メールを表示するために WebDAV を必要とする Apple MAC ユーザも対象となります。

会議通知のサポート

会議通知機能は、WebDAV 経由でネットワーク統合を行う場合にのみ使用できます。 そのため、この問題は Microsoft Exchange 2003 または 2007 でのみ発生します。 これらの機能は EWS 統合ではサポートされません。