予定表統合のための IM and Presence Service 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

予定表情報を交換するには、Exchange Server（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。Exchange ゲートウェイにより、IM and Presence Service のノードがユーザー単位でユーザーの在席情報を反映できるようになります。

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 Exchange Server と接続できます。

- FQDN（DNS で解決可能）
- IP アドレス

Exchange 統合のために Exchange Web サービス（EWS）のプレゼンスゲートウェイを **Cisco Unified CM IM and Presence Administration** ユーザーインターフェイスを使用して設定する場合は、次の点に注意してください。

- *1* 台または複数の EWS サーバーを追加、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の設定（Presence Gateway Configuration）] ウィンドウの [トラブルシューティングツール（Troubleshooter）] は、設定した最初の 10 台の EWS サーバーのステータスのみを検証し、レポートするように設計されています。
- EWS サーバーゲートウェイは、最初の EWS サーバーゲートウェイに対して設定した偽装アカウントログイン情報（アカウント名とパスワード）を共有します。1 つの EWS サーバーゲートウェイのログイン情報を変更すると、設定されたすべての EWS ゲートウェイのログイン情報もそれに準じて変更されます。
- 1 つまたは複数の EWS サーバーを追加、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 サーバーを連続して追加した場合は、Cisco Presence Engine を一度だけ再起動してすべての変更を同時に反映できます。

（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。
- プレゼンスゲートウェイの設定時に、[プレゼンスゲートウェイ（Presence Gateway）] フィールドは [サブジェクトの別名（Subject Alternative Name）] フィールドに表示されている保護されたホストと完全に一致している必要があります。

Exchange Web サービスを介したプレゼンスゲートウェイとしての Exchange 2007、2010、または 2013 の設定

始める前に

プレゼンスゲートウェイを設定する前に、IM and Presence 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 Exchange Server への接続を IPv6 経由で行う場合は、導入時に各 IM and Presence Service ノード上でエンタープライズ パラメータが IPv6 に対し設定され、その Eth0 が IPv6 に対し設定されていることを確認します。IM and Presence Service での IPv6 の設定の詳細については、『*Cisco Unified Communications Manager* での *IM and Presence Service* 設定および管理』を参照してください。

手順

ステップ 1 **Cisco Unified CM IM and Presence Administration** の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（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）] をクリックします。

ステップ 4 [プレゼンスゲートウェイのタイプ（Presence Gateway Type）] に [Exchange - EWS サーバー（Exchange -- EWS Server）] を選択します。

設定の変更を反映するには、1 つまたは複数の EWS サーバーを追加、更新、または削除した後に Cisco Presence Engine を再起動する必要があります。複数の EWS サーバーを連続して追加した場合は、Cisco Presence Engine を一度だけ再起動してすべての変更を同時に反映できます。

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ーの場所を入力し、そ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 [サブジェクトの別名（Subject Alternative Name）] フィールドにあることを確認します。Microsoft Exchange Server 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、指定するサーバーの場所の値は、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 `*.imp.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`*`.imp.cisco.com` という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、それがサブジェクト共通名（CN）に一致するか、または証明書チェーンの Exchange Server リーフ証明書での [サブジェクトの別名（Subject Alternative Name）] フィールドの保護されたホストのいずれかに一致する必要があります。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。

IPv6 の場合は、入力する IPv6 アドレスが Exchange Server 証明書の [SAN] フィールドに入力された値と一致する必要があります。

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。この名前は、ユーザープリンシパル名（user@domain など）か、ダウンレベルのログオン名（domain\user など）のどちらかの形式です。

ステップ 8 IM and Presence Service が Exchange Server に接続するのに必要な Exchange アカウントパスワードを入力します。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 との接続に使用するポートを入力します。Exchange との IM and Presence Service の統合は、セキュアな HTTP 接続を介して行われます。ポート 443（デフォルト ポート）を使用し、それ以外のポートは変更しないことを推奨します。

ステップ 10 [保存（Save）] をクリックします。

ステップ 11 [Exchange Server] ステータスが次を示すグリーンになっていることを確認します。

- **Exchange の到達可能性（ping 可能）**

- **Exchange SSL の接続/認定の検証**

次のタスク

Exchange プレゼンスゲートウェイを設定後、次の点を確認します。

- IM and Presence Service と Exchange Server の接続が成功したかどうかを確認します。[プレゼンスゲートウェイの設定（Presence Gateway Configuration）] ウィンドウの [Exchange Serverのステータス（Exchange Server Status）] には、 と Exchange Server との接続のステータスが表示されます。修正が必要な場合は、「Exchange Server の接続ステータスに関するトラブルシューティング」を参照してください。
- Exchange SSL 証明書チェーンのステータスが正しい（[確認が成功しました（Verified）]）かどうかを確認します。[プレゼンスゲートウェイ設定（Presence Gateway Configuration）] ウィンドウの [Exchange Serverステータス（Exchange Server Status）] 領域には、証明書のサブジェクト CN の不一致があるかどうかが示されます。修正が必要な場合は、「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」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 では、Microsoft Exchange との予定表統合をセキュリティ保護するために、X.509 証明書を使用します。IM and Presence Service では、標準の証明書とともに、SAN および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、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。

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により、ドメインと無制限のサブドメインを表すことができます。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） 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。プレゼンスゲートウェイの設定時に、[プレゼンスゲートウェイ（Presence Gateway）] フィールドは [サブジェクトの別名（Subject Alternative Name）] フィールドに表示されている保護されたホスト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、[標準証明書の共通名（CN）（Common Name (CN)）]と、SAN 証明書の [サブジェクトの別名（Subject Alternative Name）] に使用することができます。

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

認証局サービスのインストール方法

認証局（CA）は Exchange Server 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 Server を CA として使用することをお勧めします。

Windows Server 2003 での CA のインストール

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 Component）] ウィザードを完了します。

a) [Windows コンポーネント（Windows Components）] ウィンドウで、[証明書サービス（Certificate Services）] の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の名前変更の制約に関する警告が表示された場合 [はい（Yes）] を選択します。

b) [CAの種類（CA Type）] ウィンドウで、[スタンドアロンルートCA（Stand-alone Root CA）] を選択し、[次へ（Next）] をクリックします。

c) [CA 識別情報（CA Identifying Information）] ウィンドウで、CA サーバーの [共通名（Common Name）] 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、[次へ（Next）] を選択します。

（注） 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、証明書署名要求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。

d) [証明書データベースの設定（Certificate Database Settings）] ウィンドウで、デフォルト設定を受け入れて [次へ（Next）] を選択します。

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（Yes）] を選択します。

ステップ 5 Active Server Pages（ASP）を有効にするように求められたら [はい（Yes）] をクリックします。

ステップ 6 インストールが完了したら、[完了（Finish）] をクリックします。

次のタスク

証明書署名要求の生成：Windows Server 2003 を実行している場合

Windows Server 2008 での 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）] > [サーバーマネージャ（Server Manager）]** の順に選択します。

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。

a) [開始する前に（Before You Begin）] ウィンドウで、リストされている前提条件がすべて完了していることを確認し、[次へ（Next）] をクリックします。

b) [サーバーの役割の選択（Select Server Roles）] ウィンドウで、[Active Directory証明書サービス（Active Directory Certificate Services）] のチェックボックスをオンにして、[次へ（Next）] をクリックします。

c) [概要（Introduction）] ウィンドウで、[次へ（Next）] をクリックします。

d) [役割サービスの選択（Select Role Services）] ウィンドウで、次のチェックボックスをオンにし、[次へ（Next）] をクリックします。

- 証明機関（Certificate Authority）
- 証明機関 Web 登録（Certificate Authority）
- オンライン レスポンダー（Online Responder）

e) [セットアップの種類の指定（Specify Setup Type）] ウィンドウで、[スタンドアロン（Standalone）] をクリックします。

f) [CAの種類の指定（Specify CA Type）] ウィンドウで、[ルートCA（Root CA）] をクリックします。

g) [秘密キーの設定（Set Up Private Key）] ウィンドウで、[新しい秘密キーを作成する（Create a new private key）] をクリックします。

h) [CAの暗号化を構成（Configure Cryptography for CA）] ウィンドウで、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。

i) [CA名を構成（Configure CA Name）] ウィンドウで、CA を識別する共通名を入力します。

j) [有効期間の設定（Set Validity Period）] 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） CA が発行する証明書は、ここで指定した期日まで有効になります。

k) [証明書データベースを構成（Configure Certificate Database）] ウィンドウで、デフォルトの証明書データベースの場所を選択します。

l) [インストールオプションの確認（Confirm Installation Selections）] ウィンドウで、[インストール（Install）] をクリックします。

m) [インストールの結果（Installation Results）] ウインドウで、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）] をクリックします。

（注） サーバー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。

次のタスク

証明書署名要求の生成：Windows Server 2008 を実行している場合

Microsoft Exchange Server の IIS での証明書署名要求の生成

証明書署名要求の生成：Windows Server 2003 を実行している場合

Exchange の IIS で証明書署名要求（CSR）を生成する必要があります。生成した証明書署名要求は CA サーバー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。

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。

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 2 [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 3 [サーバー証明書（Server Certificate）] を選択します。

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

ステップ 5 **サーバー証明書ウィザード**を完了します。

a) [サーバー証明書（Server Certificate）] ウィンドウで [新しい証明書の作成（Create a new certificate）] を選択し、[次へ（Next）] を選択します。

b) [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。

c) [名前およびセキュリティ設定（Name and Security Settings）] で、デフォルトの Web サイト証明書名を受け入れ、ビット長として [1024] を選択し、[次へ（Next）] を選択します。

d) [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。

e) [サイトの一般名（Your Site's Common Name）] 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、[次へ（Next）] をクリックします。

（注） ここで入力する IIS 証明書の一般名は、IM and Presence Service 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。

f) [地理情報（Geographical Information）] ウィンドウで次のように地理情報を入力し、[次へ（Next）] を選択します。

- 国/地域（Country/region）
- 都道府県（State/province）
- 市区町村（City/locality）

g) [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、証明書署名要求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） 証明書署名要求は拡張子（.txt）なしで保存してください。この証明書署名要求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。

h) [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。

i) [Webサーバー証明書ウィザードの完了（Web Server Certificate Completion）] ウィンドウで、[完了（Finish）] をクリックします。

次のタスク

CA サーバー/認証局への証明書署名要求の送信

証明書署名要求の生成：Windows Server 2008 を実行している場合

Exchange の IIS で証明書署名要求（CSR）を生成する必要があります。生成した証明書署名要求は CA サーバー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）] ウィンドウを開きます。

ステップ 2 IIS マネージャの左ペインの [接続（Connections）] の下で、[Exchange Server] を選択します。

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

ステップ 4 IIS マネージャの右ペインにある [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 **証明書の要求**ウィザードを完了します。

a) [識別名プロパティ（Distinguished Name Properties）] ウィンドウで、次の情報を入力します。

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

b) 地理情報を次のように入力し、[次へ（Next）] をクリックします。

- 市区町村（City/locality）
- 都道府県（State/province）
- 国/地域（Country/region）

（注） ここで入力する IIS 証明書の一般名は、IM and Presence Service 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。

c) [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、デフォルトの暗号化サービスプロバイダを承認し、ビット長に [2048] を選択し、[次へ（Next）] をクリックします。

d) [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） 証明書署名要求は拡張子（.txt）なしで保存してください。この証明書署名要求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。

e) [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。

f) [証明書の要求を完了する（Request Certificate Completion）] ウィンドウで、[完了（Finish）] をクリックします。

次のタスク

CA サーバー/認証局への証明書署名要求の送信

CA サーバー/認証局への証明書署名要求の送信

IIS で Exchange 用に作成されるデフォルトの SSL 証明書には、Exchange Server の完全修飾ドメイン名（FQDN）を使用し、IM and Presence Service 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 からの証明書署名要求に署名できます。次の手順を CA サーバーで実行し、次の場所にある Exchange Server の FQDN を設定します。

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

始める前に

Exchange Server の IIS で証明書署名要求を生成します。

手順

ステップ 1 証明書要求ファイルを CA サーバーにコピーします。

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://*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 [証明書の要求（Request a certificate）] を選択します。

ステップ 4 [証明書の要求の詳細設定（advanced certificate request）] を選択します。

ステップ 5 [Base 64 エンコード CMC または PKCS #10 ファイルを使用して証明書の要求を送信するか、または Base 64 エンコード PKCS #7 ファイルを使用して更新の要求を送信する（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）] をクリックします。

ステップ 6 メモ帳などのテキスト エディタを使用して、作成した証明書署名要求を開きます。

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 証明書署名要求の内容を [証明書の要求（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、サーバー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サーバー（Web Server）] 証明書テンプレートを選択します。[Web サーバー（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）] をクリックします。

ステップ 11 [管理ツール（Administrative Tools）] ウィンドウで [スタート（Start）] > [管理ツール（Administrative Tools）] > [証明機関（Authority Certification）] > [CA 名] > [保留中の要求（Pending Request）] を選択し、[証明機関（Certification Authority）] ウィンドウを開きます。 > > > > > [証明機関（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 [発行した証明書（Issued certificates）] をクリックし、証明書が発行されたことを確認します。

次のタスク

署名付き証明書のダウンロード

署名付き証明書のダウンロード

始める前に

自己署名証明書：CA サーバーに証明書署名要求（CSR）を送信します。

サードパーティ証明書：認証局に証明書署名要求を要求します。

手順

ステップ 1 [管理ツール（Administrative Tools）] から [証明機関（Certification Authority）] を開きます。発行した証明書要求が [[発行済み要求（Issued Requests）] 領域に表示されます。

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 [ファイルにコピー（Copy to File）] を選択します。

ステップ 5 [証明書のエクスポート（Certificate Export）] ウィザードが表示されたら、[次へ（Next）] をクリックします。

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。

a) [エクスポートファイル形式（Export File Format）] ウィンドウで、[Base-64 encoded X.509] を選択し、[次へ（Next）] をクリックします。

b) [エクスポートするファイル（File to Export）] 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 を使用して `c:\cert.cer` を選択します。

c) [証明書エクスポートウィザードの完了（Certificate Export Wizard Completion）] ウィンドウで、概要を確認し、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 Service 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。

次のタスク

使用するサーバータイプ用の署名付き証明書をアップロードします。

- 署名付き証明書のアップロード：Windows 2003 を実行している場合
- 署名付き証明書のアップロード：Windows 2008 を実行している場合

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 を実行している場合

ここでは、署名付き証明書署名要求を 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 Service 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。

始める前に

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サイトのプロパティ（Default Web Site Properties）] 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) [サーバー証明書（Server Certificate）] を選択します。

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

ステップ 5 **サーバー証明書ウィザード**を完了します。

a) [保留中の証明書の要求（Pending Certificate Request）] ウィンドウで、[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）] をクリックします。

b) [保留中の証明書を処理（Process a Pending Request）] ウィンドウで、[参照（Browse）] をクリックして証明書を検索し、適切なパスとファイル名に移動します。

c) [SSLポート（SSL Port）] ウィンドウで、SSL ポートに 443 を入力し、[次へ（Next）] をクリックします。

d) [Webサーバー証明書ウィザードの完了（Web Server Certificate Completion）] ウィンドウで、[完了（Finish）] をクリックします。

Tip

証明書が信頼できる証明書ストアにない場合、署名付き証明書署名要求は信頼されません。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）] をクリックします。
- [詳細（Details）] > [ルート証明書の強調表示（Highlight root certificate）] > を選択し、[表示（View）] をクリックします。
- 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。

次のタスク

ルート証明書のダウンロード

署名付き証明書のアップロード：Windows 2008 を実行している場合

ここでは、署名付き証明書署名要求を 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 Service 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。

始める前に

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）] ウィンドウを開きます。

ステップ 2 IIS マネージャの左ペインの [接続（Connections）] の下で、[Exchange Server] を選択します。

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

ステップ 4 IIS マネージャの右ペインにある [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 [証明機関の応答を指定します（Specify Certificate Authority Response）] ウィンドウで次の操作を実行します。

a) 証明書を検索するには、省略記号（...）を選択します。
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] をクリックします。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 マネージャの右ペインにある [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）] を選択します。

ステップ 8 [サイトバインディングの編集（Edit Site Bindings）] 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、作成した証明書を選択します。証明書に適用した名前が表示されます。
b) [OK] をクリックします。

次のタスク

ルート証明書のダウンロード

ルート証明書のダウンロード

始める前に

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 サーバーのユーザーインターフェイスにログインし、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）] をクリックします。

ステップ 4 [エンコード方式（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。

Tip

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。

次のタスク

IM and Presence Service ノードへのルート証明書のアップロード

IM and Presence Service ノードへのルート証明書のアップロード

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 Server 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 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 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 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 Service 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 Server のホストとポートを指定すると、サーバー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 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。特定のタイプ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する場合は、**Cisco Unified Presence Administration** 内の証明書インポートツールのカスタマイズされたバージョンを表示することもできます（**Cisco Unified CM IM and Presence Administration** にログインし、**[プレゼンス（Presence）] > [ゲートウェイ（Gateways）]** を選択します）。	

証明書のアップロード方法	アクション
	1. **Cisco Unified CM IM and Presence Administration** のユーザーインターフェイスにログインします。 2. **[システム（System）] > [セキュリティ（Security）] > [証明書のインポートツール（Certificate Import Tool）]** を選択します。 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 Presence(IM/P) Trust] を選択します。このストアには、Exchange の統合に必要な Presence Engine 信頼証明書が保存されます。 4. Exchange Server 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 • Hostname • FQDN この [ピアサーバー（Peer Server）] フィールドに入力する値は、Exchange Server 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。 5. Exchange Server との通信に使用するポートを入力します。この値は、Exchange Server の使用可能なポートと一致している必要があります。 6. [送信（Submit）] をクリックします。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。 • ピアサーバーの到達可能性ステータス：IM and Presence Service が Exchange Server に到達（ping）できるかどうかを示します。「Exchange Server の接続ステータスに関するトラブルシューティング」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ーから証明書をダウ

証明書のアップロード方法	アクション
	ンロードすることに成功したかどうかと、IM and Presence Service とリモートサーバー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」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 サーバーでは 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 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証明書を提供しない場合、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。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 Operating System Administration** にログインし、**[Security（セキュリティ）]** > **[Certificate Management（証明書管理）]** を選択します）。	1. IM and Presence Service ノード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 IM and Presence Operating System Administration** ユーザーインターフェイスにログインします。 3. **[Security（セキュリティ）]** > **[Certificate Management（証明書管理）]** を選択します。 4. [証明書の一覧（Certificate List）] ウィンドウで、[証明書/証明書チェーンのアップロード（Upload Certificate/Certificate Chain）] を選択します。 5. [証明書/証明書チェーンのアップロード（Upload Certificate/Certificate Chain）] ダイアログボックスが開いたら、次の操作を実行します。 • [証明書名（Certificate Name）] ドロップダウンリストから [cup-xmpp-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。 6. [参照（Browse）] をクリックし、[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 証明書のインポート ツール（ステップ 1 （16 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 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、Exchange Server 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。

次のタスク

IM and Presence 予定表統合のタスクフロー

予定表統合の有効化

予定表統合は、管理者によって個別またはユーザーグループごとに有効化されます。

（注） プレゼンスゲートウェイが Cisco Unified Communications Manager 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 （1 ページ）」を参照してください。

個人ユーザーに対する予定表統合の有効化

この手順を使用して、個々のエンドユーザーの Microsoft Outlook 予定表統合を設定します。

手順

ステップ 1 **Cisco Unified CM Administration** の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）]** > **[エンドユーザー（End User）]** の順に選択します。

ステップ 3 [検索（Find）] をクリックしてエンドユーザーを選択します。

ステップ 4 [Unified CM IM and Presenceでのユーザーの有効化（Enable User for Unified CM IM and Presence）] チェックボックスをオンにします。

ステップ 5 [プレゼンスに会議情報を含める（Include meeting information in Presence）] 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。

予定表統合の一括有効化

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 予定表統合を一括有効化は、次のウィンドウから実行できます。

a) **[一括管理（Bulk Administration）] > [ユーザー（Users）] > [ユーザーの挿入（Insert Users）]**
b) **[一括管理（Bulk Administration）] > [ユーザー（Users）] > [ユーザーの更新（Update Users）] > [クエリー（Query）]**
c) **[一括管理（Bulk Administration）] > [ユーザー（Users）] > [ユーザーの更新（Update Users）] > [カスタムファイル（Custom File）]**

（注） 更新のさまざまなオプションの詳細については、『*Cisco Unified Communications Manager* 一括管理ガイド』を参照してください。

ステップ 3 予定表統合を有効にするすべてのエンドユーザーについて、次のエンドユーザー設定オプションがオンになっていることを確認してください。

- [Unified CM IM and Presenceのユーザーを有効にする（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、適切な [ユーザー（User）] 領域で [ファイル名（File Name）] を選択します。

（注） 正しいファイル形式の [サンプルファイルの表示（View Sample File）] をクリックします。

ステップ 5 [今すぐ実行（Run Immediately）] または [後で実行（Run Later）] をクリックします。

ステップ 6 [送信（Submit）] をクリックします。

[任意] Exchange Web サービスで送信される Exchange カレンダー通知の頻度の設定

（注） この手順は、Microsoft Exchange Server 2007、2010、または 2013 を Exchange Web サービス（EWS）経由で統合する場合にのみ必要となります。

[EWS ステータスの頻度（EWS Status Frequency）] パラメータは、Exchange Server が IM and Presence Service 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 Service 上の Presence Engine 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 Server および IM and Presence サーバーへの負荷も増加します。

手順

ステップ 1 **Cisco Unified CM IM and Presence Administration** の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 **[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 3 [サーバー（Server）] ドロップダウンリストから、[IM and Presence Service] ノードを選択します。

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

ステップ 5 [予定表の設定（すべてのサーバーに適用されるパラメータ）（Calendaring Configuration (Parameters that apply to all servers)）] 領域で、[EWSステータス頻度（EWS Status Frequency）] フィールドのパラメータ値を編集します。このパラメータの最大値は 1440 分です。このパラメータのデフォルト値は 60 分です。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

予定表の統合はユーザー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、すべてのユーザー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 Serviceability** のユーザーインターフェイスにログインします。**[Tools（ツール）] > [Service Activation（サービス アクティベーション）]** を選択します。

[任意] Microsoft Exchange 通知ポートの設定

このトピックは、Cisco Presence Engine において Exchange Server 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。

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。

始める前に

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 Administration** の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 **[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 3 [サーバー（Server）] ドロップダウンリストから、[IM and Presence Service] ノードを選択します。

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

ステップ 5 [予定表の設定（Calendaring Configuration）] 領域で、[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、[Save（保存）] をクリックします。

次のタスク

一度にすべてのユーザー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 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

- ポートをデフォルト以外に変更した場合、そのユーザーの Exchange サブスクリプションが更新されるまで、Cisco Presence Engine はユーザー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。Presence Engine がユーザー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ー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。

[任意] Microsoft Exchange カレンダー通知の接続時間の設定

デフォルトでは、Cisco Presence Engine は会議/取り込み中通知を発生から 50 秒で送信できます。ユーザー数が少ない場合は、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。

始める前に

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ーの最大数/100」に設定します。たとえば、ユーザーの最大数が 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 Administration** の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 **[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 3 [サーバー（Server）] ドロップダウンリストから、[IM and Presence Service] ノードを選択します。

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

ステップ 5 [予定表の設定（Calendaring Configuration）] 領域で、[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。このパラメータのデフォルト値は 50 です。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

[予定表スプレッド（Calendar Spread）] パラメータの変更は、ユーザー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、すべてのユーザー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 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 多数のユーザー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 カレンダーパラメータ

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 カレンダーパラメータには、他にも 3 つあります。

- [Exchange タイムアウト（秒）（Exchange Timeout (seconds)）]：Exchange Server 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。変更すると、Exchange 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。

不在ステータス

IM and Presence Service は、ユーザーの在席ステータスとして [不在（Out of Office）] をサポートします。そのため、特定の期間に Microsoft Outlook で不在通知を設定すると、Jabber のプレゼンス ステータスが [退席中（Away）] または [オフライン（Offline）] ではなく [不在（Out of Office）] と表示されます。

さらに、ユーザーステータス情報を収集する際のユーザー体験が向上し、不在であることを不在期間の開始日と終了日とともに他の人に知らせることができます。これにより、ユーザーのプレゼンス状態を明確かつ正確にプロビジョニングすることにより、インスタントメッセージング システムが強化され、ユーザー体験が向上します。

さらに、カスタムプレゼンス設定を使用して不在プレゼンス ステータスを上書きし、必要に応じてアクティブと不在のステータス間を切り替えることができます。これにより、緊急のコミュニケーションや重要な会議に効果的に対処できます。したがって、MS Exchange Server と Office 365 サーバーの両方をサポートするため、オンプレミスとクラウドベースの予定表サービスの間に生じるギャップがなくなります。

たとえば、休暇を取るカスタマーサポートのリードエグゼクティブであるジョン・スミスは、Office 365 で 20XX 年 12 月 10 日 0800 時から 20XX 年 12 月 20 日 2300 時の間に不在通知を設定しました。この機能を実装すると、12 月 10 日の Jabber での彼のプレゼンス ステータスは、「*2019* 年 *3* 月 *10* 日 *10:00 AM GMT* ～ *2019* 年 *3* 月 *12* 日 *6:00 PM GMT* 不在」のメッセージとともにアクティブ/退席中/オフライン（場合による）として表示されます。在席ステータスアイコンがオレンジ色に変わります（ジョンがオフラインの場合を除く）。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に、Jabber を介してビジネスクリティカルな会議に参加するように求められました。IM and Presence Service のこの新しい機能拡張により、ジョンは不在ステータスを一時的に無効にして、在席ステータスを手動でアクティブにして、顧客との会議に参加できます。会議が終了したら、予定された休暇が終了するまで、プレゼンス ステータスを不在に戻すことができます。

Jabber および Webex Teams の不在通知

MS Exchange や Office 365 などの予定表サービスで不在を設定すると、IM and Presence Service は、定義されたポーリング間隔中に不在通知をプルし、プレゼンス ステータスを不在として表示します。この期間中、ステータスアイコンはオレンジ色で表示されます。不在の期間はローカルタイムゾーンで表示されます。たとえば、メッセージには、*2019* 年 *3* 月 *10* 日 *10:00 AM GMT* から *2019* 年 *3* 月 *12* 日 *6:00 PM GMT* まで不在と表示されます。また、メッセージのローカライズも処理します。

ただし、不在時にオフラインになっている場合は、ステータスが [オフライン（Offline）] と表示され、不在メッセージが表示されます。

IM and Presence 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 パラメータは、IM クライアント アプリケーションでの不在時の在席ステータスの表示を有効または無効にするのに役立ちます。IM and Presence ノードで不在通知を有効にするには、次の手順を実行します。

（注） マルチモード IM and Presence 展開では、1 つのノードで不在通知オプションを有効にすると、クラスタの他のノードに適用できます。

1. Cisco Unified CM IM and Presence Administration で、[システム（System）] > [サービスパラメータ（Service Parameters）] を選択します。 >
2. [サービスパラメータの設定（Service Parameter Configuration）] ページで、IM and Presence ノードが展開されている**サーバー**を選択します。
3. [サービス（Service）] フィールドで、[Cisco Presence Engine] を選択します。
4. [予定表の設定（すべてのサーバーに適用されるパラメータ）（Calendaring Configuration (Parameters that apply to all servers)）] セクションで、[予定表の不在情報（Calendar Out of Office Information）] フィールドを [不在時の応答可否を表示する（Display Out of Office Availability）] に設定します。これはデフォルトで行われます。
5. [保存（Save）] をクリックします。

不在時の空き情報の表示を無効にするには、[予定表の不在情報（Calendar Out of Office Information）] フィールドで [不在時の応答可否を表示しない（Do not display out of office availability）] を選択し、[保存（Save）] をクリックします。これにより、クラスタ内のすべての IM and Presence 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、PE サービスを再起動する必要があります。

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。