



CHAPTER 3

Cisco Unified Presence と統合（EWS 経由） するための Microsoft Exchange Server 2007 および 2010 の設定



(注)

このモジュールでは、**Exchange Web Services (EWS; Exchange Web サービス)** 経由での Cisco Unified Presence と Microsoft Exchange Server 2007 および 2010 の統合について説明します。WebDAV 経由で Exchange Server 2003 または 2007 を統合する場合は、第 2 章「Cisco Unified Presence と統合（WebDAV 経由）するための Microsoft Exchange Server 2003 および 2007 の設定」を参照してください。2 種類の Exchange 統合の概要については、第 1 章「Cisco Unified Presence と Microsoft Exchange の統合の計画」を参照してください。

- 「Microsoft Exchange 2007 設定チェックリスト (EWS)」 (P.3-1)
- 「Exchange 2007 アカウントの権限の確認」 (P.3-4)
- 「Microsoft Exchange 2010 設定チェックリスト (EWS)」 (P.3-5)
- 「Exchange 2010 アカウントの権限の確認」 (P.3-7)
- 「Exchange 2007/2010 仮想ディレクトリの認証を有効にする方法」 (P.3-8)

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。

表 3-1 は、Windows Server 2003 および Window Server 2008 で実行される 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](http://technet.microsoft.com/en-us/library/bb124558(EXCHG.80).aspx)) を参照してください。

表 3-1 Microsoft Exchange 2007 コンポーネントの設定作業

作業	手順	重要な注意事項
ユーザにサービスアカウントにローカルでサインインするための権限を付与する。	<p>Windows Server 2003 上の Exchange 2007 設定</p> <ol style="list-style-type: none"> 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 [セキュリティ設定 (Security Settings)] で [ローカル ポリシー (Local Policies)] > [ユーザー権利の割り当て (User Rights Assignments)] を選択します。 4. コンソールの右側のフレームで [ローカル ログオンを許可する (Allow Log On Locally)] をダブルクリックします。 5. [ユーザー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。 <p>Windows Server 2008 上の Exchange 2007 設定</p> <ol style="list-style-type: none"> 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. [開始 (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。 6. 左側のフレームの [セキュリティ設定 (Security Settings)] で [ローカル ポリシー (Local Policies)] > [ユーザー権利の割り当て (User Rights Assignments)] を選択します。 7. コンソールの右側のフレームで [ローカル ログオンを許可する (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オンになっていることを確認します。 9. [ユーザー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)] を右クリックして [プロパティ (Properties)] を選択し、表示される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 <i>alias@FQDN</i> であることを確認します。そうでない場合は、User Principal Name (UPN; ユーザー プリンシパル名) を使用して偽装する必要があります。これは <i>alias@FQDN</i> と定義されます。 	<ul style="list-style-type: none"> • Exchange 偽装が動作するためには、すべての Exchange サーバが Windows Authorization Access Group のメンバーである必要があります。 • サービスアカウントは、Exchange 管理グループのメンバーであってはなりません。Microsoft Exchange は、Exchange 管理グループに属するすべてのアカウントについて、偽装を明示的に拒否します。

作業	手順	重要な注意事項
偽装権限をサーバレベルで設定する。	<p>Exchange Management Shell (EMS; Exchange 管理シェル) を使用する場合</p> <ol style="list-style-type: none"> 1. コマンドライン入力を行うために EMS を開きます。 2. 次の Add-ADPermission コマンドを実行してサーバに対する偽装権限を追加します。 <p>構文</p> <pre>Add-ADPermission -Identity (get-exchangeserver).DistinguishedName -User (Get-User -Identity User select-object).identity -AccessRights GenericAll -InheritanceType Descendants</pre> <p>例</p> <pre>Add-ADPermission -Identity (get-exchangeserver).DistinguishedName -User (Get-User -Identity Ex2007 select-object).identity -AccessRights GenericAll -InheritanceType Descendants</pre>	<ul style="list-style-type: none"> • これらのコマンドレットは、偽装権限をサーバレベルで付与します。データベース、ユーザ、および連絡先のレベルで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 と定義されていることを確認します。そうでない場合は、User Principal Name (UPN; ユーザー プリンシパル名) 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。
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。	<p>Exchange Management Shell (EMS; Exchange 管理シェル) を使用する場合</p> <ol style="list-style-type: none"> 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。 <p>構文</p> <pre>Add-ADPermission -Identity (get-exchangeserver).DistinguishedName -User (Get-User -Identity User select-object).identity -ExtendedRight ms-Exch-EPI-Impersonation</pre> <p>例</p> <pre>Add-ADPermission -Identity (get-exchangeserver).DistinguishedName -User (Get-User -Identity Ex2007 select-object).identity -ExtendedRight ms-Exch-EPI-Impersonation</pre> <ol style="list-style-type: none"> 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。 <p>構文</p> <pre>Add-ADPermission -Identity (get-exchangeserver).DistinguishedName -User (Get-User -Identity User select-object).identity -ExtendedRight ms-Exch-EPI-May-Impersonate</pre> <p>例</p> <pre>Add-ADPermission -Identity (get-exchangeserver).DistinguishedName -User (Get-User -Identity Ex2007 select-object).identity -ExtendedRight ms-Exch-EPI-May-Impersonate</pre>	<ul style="list-style-type: none"> • これらの権限は、偽装を実行するサービス アカウントについて (Client Access Server (CAS; クライアント アクセス サーバー) 上で) 設定する必要があります。 • CAS がロード バランサの背後に位置する場合は、ロード バランサの背後にあるすべての CAS サーバについて、Ex2007 アカウントに ms-Exch-EPI-Impersonation 権限を付与します。 • メールボックス サーバが CAS 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 サーバについて、Ex2007 アカウントに 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 ユーザーとコンピュータ (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	重要な注意事項
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。	<p>Exchange Management Shell (EMS; Exchange 管理シェル) を使用する場合</p> <p>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。</p> <p>構文</p> <pre>Add-ADPermission -Identity (get-exchangeserver).DistinguishedName -User (Get-User -Identity User select-object).identity -ExtendedRights Send-As</pre> <p>例</p> <pre>Add-ADPermission -Identity (get-exchangeserver).DistinguishedName -User (Get-User -Identity Ex2007 select-object).identity -ExtendedRights Send-As</pre>	<p>この手順を実行するために、Exchange Management Console (EMC; Exchange 管理コンソール) を使用することはできません。</p>
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。	<p>Exchange Management Shell (EMS; Exchange 管理シェル) を使用する場合</p> <p>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。</p> <p>構文</p> <pre>Add-ADPermission -Identity (get-exchangeserver).DistinguishedName -User (Get-User -Identity User select-object).identity -ExtendedRights Receive-As</pre> <p>例</p> <pre>Add-ADPermission -Identity (get-exchangeserver).DistinguishedName -User (Get-User -Identity Ex2007 select-object).identity -ExtendedRights Receive-As</pre>	<p>この手順を実行するために、Exchange Management Console (EMC; Exchange 管理コンソール) を使用することはできません。</p>

トラブルシューティングのヒント

Cisco Unified 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」 \(P.3-4\)](#)

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)] タブで次のことを確認します。
- サービス アカウントが表示されている。
 - 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 impersonation permission 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** に示すとおりに表示されていない場合は、サービス アカウントを再作成し、そのアカウントに必要な偽装権限を付与することが必要となることがあります。
- 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を有効にする方法」(P.3-8)

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

表 3-3 は、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チェックリストです。詳細については、Microsoft Server 2010 のマニュアル (<http://technet.microsoft.com/en-us/library/bb124558.aspx>) を参照してください。

はじめる前に

Microsoft Exchange 2010 サーバを EWS 経由で Cisco Unified Presence に統合する前に、Exchange サーバで次のスロットル 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 経由での Cisco Unified Presence との予定表統合が機能するために必要です。これらのパラメータ値を変更しないことを推奨します。

表 3-2 Microsoft Exchange の推奨スロットル ポリシー パラメータ値

パラメータ	推奨設定値
EWSMaxConcurrency	シスコが実施したテストにおいて、このスロットル ポリシー パラメータはデフォルト値のままです。予定表を使用する 50% のユーザをサポートするために十分であることが確認されました。ただし、CAS に対する EWS 要求の負荷が高い場合は、このパラメータを 100 に設定することを推奨します。
EWSPercentTimeInAD	50
EWSPercentTimeInCAS	90
EWSPercentTimeInMailboxRPC	60
EWSMaxSubscriptions	5000
EWSFastSearchTimeoutInSeconds	60
EWSFindCountLimit	1000

表 3-3 Microsoft Exchange 2010 コンポーネントの設定作業

作業	手順	重要な注意事項
特定のユーザまたはユーザのグループに Exchange 偽装権限を設定する。	<p>Exchange Management Shell (EMS; Exchange 管理シェル) を使用する場合</p> <ol style="list-style-type: none"> 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、指定したサービス アカウント (Ex2010 など) に他のユーザ アカウントを偽装する権限を付与します。 <p>構文</p> <pre>new-ManagementRoleAssignment -Name:_suImpersonateRoleAsg -Role:ApplicationImpersonation -User:user@domain</pre> <p>例</p> <pre>new-ManagementRoleAssignment -Name:_suImpersonateRoleAsg -Role:ApplicationImpersonation -User:Ex2010@domain</pre> <ol style="list-style-type: none"> 3. 次の New-ManagementRoleAssignment コマンドを実行して、偽装権限の適用範囲を定義します。この例では、Exch2010 アカウントに指定した Exchange サーバ上のすべてのアカウントを偽装する権限を付与します。 <p>構文</p> <pre>new-ManagementScope -Name:_suImpersonateScope -ServerList:<server name></pre> <p>例</p> <pre>new-ManagementScope -Name:_suImpersonateScope -ServerList:nw066b-227</pre>	EWS 自動検出サービスを使用するためには、Cisco Unified Communications Manager から Cisco Unified Presence に同期できるように、偽装ユーザに対して LDAP で明示的にメール ID が設定されていることが必要です。

次の作業

「Exchange 2010 アカウントの権限の確認」 (P.3-7)

関連事項

Microsoft Exchange サーバパラメータの詳細については、
<http://technet.microsoft.com/en-us/library/dd351045.aspx> を参照してください。

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 Management Shell (EMS; Exchange 管理シェル) 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.** 次のように、指定されたアカウントに役割「ApplicationImpersonation」が割り当てられ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

Name -----	Role -----	RoleAssigneeName -----	RoleAssignee Type -----	Assignment Method -----	EffectiveUser Name -----
_suImpersonate RoleAsg	ApplicationImpe rsonation	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適用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 -----	Recipient Filter -----	ServerFilter -----
_suImpersonate Scope	ServerScope	False			Distinguished Name

次の作業

「Exchange 2007/2010 仮想ディレクトリの認証を有効にする方法」(P.3-8)

Exchange 2007/2010 仮想ディレクトリの認証を有効にする方法

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 または /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 および WebDAV へのメールボックス アクセス要求を処理します。/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。

- 「Windows Server 2003 を実行する Exchange 2007 の認証の有効化」(P.3-8)
- 「Windows Server 2008 を実行する Exchange 2010 の認証の有効化」(P.3-9)

Windows Server 2003 を実行する Exchange 2007 の認証の有効化

手順

-
- ステップ 1 [Administrative Tools] から [Internet Information Services] を開き、サーバを選択します。
 - ステップ 2 [Web Sites] を選択します。
 - ステップ 3 [Default Web Site] を選択します。
 - ステップ 4 [Exchange] または [Exchweb] ディレクトリ フォルダを右クリックし、[Properties] を選択します。
 - ステップ 5 [Directory Security] タブを選択します。
 - ステップ 6 [Authentication and Access Control] で、[Edit] を選択します。
 - ステップ 7 [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]
-

次の作業

「Microsoft Exchange と統合する場合の Cisco Unified Presence でのプレゼンス ゲートウェイの設定」(P.4-1)

Windows Server 2008 を実行する Exchange 2010 の認証の有効化

手順

-
- ステップ 1 Exchange 管理コンソールで、統合 Windows 認証を有効にする仮想ディレクトリに移動します。
 - ステップ 2 [Server Configuration] を選択します。
 - ステップ 3 [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 作業ウィンドウで、統合 Windows 認証を有効に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 [Properties] を選択します。
 - ステップ 8 [Authentication] タブを選択します。
 - ステップ 9 [Use one or more standard authentication methods] を選択します。
 - ステップ 10 [Basic Authentication (password is sent in clear text)] をオンにします。
 - ステップ 11 [OK] を選択します。
-

次の作業

[「Microsoft Exchange と統合する場合の Cisco Unified Presence でのプレゼンス ゲートウェイの設定」\(P.4-1\)](#)

関連事項

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

