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 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 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）， 1 ページ
- Exchange 2007 アカウントの権限の確認， 9 ページ
- Microsoft Exchange 2010 設定チェックリスト（EWS）， 10 ページ
- Exchange 2010 アカウントの権限の確認， 12 ページ
- Exchange 2007/2010 仮想ディレクトリの認証， 13 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 *1*：*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 ポリシーの設定」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, （9 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, （9 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, （13 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 *2*：*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 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。
Exchange 2010 アカウントの権限の確認, （12 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 2：Microsoft Exchange のスロットル ポリシー パラメータの推奨値, （10 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 2：Microsoft Exchange のスロットル ポリシー パラメータの推奨値, （10 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, （13 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, （14 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, （15 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

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

関連トピック

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