



# 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

このモジュールでは、Exchange Web サービス（EWS）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 サーバ 2003 または 2007 と統合する場合は、第 3 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。各種の Exchange の統合の概要については、第 2 章「Cisco Unified Presence と Microsoft Exchange の統合の計画」を参照されることをお勧めします。

- 「Microsoft Exchange 2007 の設定（EWS）」（P.4-1）
- 「Exchange 2007 アカウントの権限の確認」（P.4-6）
- 「Microsoft Exchange 2010 の設定（EWS）」（P.4-7）
- 「Exchange 2010 アカウントの権限の確認」（P.4-10）
- 「Exchange 2007/2010 仮想ディレクトリの認証を有効にする方法」（P.4-11）

## Microsoft Exchange 2007 の設定（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。

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場合、次の手順を実行します。

- Windows のセキュリティポリシー設定を確認する
- 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付与する
- 偽装権限をサーバレベルで設定する
- 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
- 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
- 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

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。

## Windows のセキュリティ ポリシー設定を確認する

Cisco Unified Presence は、NTLMv1 Windows 統合認証のみサポートし、現在 NTLMv2 をサポートしていません。

NTLMV2 が有効ではないことを確認するには、次の手順に従ってください。

### 手順

- 
- ステップ 1** Exchange を実行している Windows サーバで [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)] を選択します。
  - ステップ 2** [セキュリティの設定 (Security Settings)] > [ローカル ポリシー (Local Policies)] > [セキュリティのオプション (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 (Network Security)] を選択 : NTLM SSP ベース (セキュア RPC を含む) サーバの最小セッション セキュリティ。
  - 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、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 を実行している Windows サーバをリポートします。
- 

### 次の作業

[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付与する](#)

## 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付与する

ユーザがサービス アカウントにローカルにサイン インするように設定するには、次のいずれかの手順を実行します。

### はじめる前に

- 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。

## Windows Server 2003 での Exchange 2007 の設定

### 手順

- 
- ステップ 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。

- ステップ 2** 左側のフレームにある [セキュリティの設定 (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)] に移動します。
  - ステップ 3** 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。
  - ステップ 4** [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。
  - ステップ 5** [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

### 手順

- ステップ 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。
  - ステップ 2** [スタート (Start)] を選択します。
  - ステップ 3** `gpmc.msc` と入力します。
  - ステップ 4** Enter を押します。
  - ステップ 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。
  - ステップ 6** 左側のフレームにある [セキュリティの設定 (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)] に移動します。
  - ステップ 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。
  - ステップ 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。
  - ステップ 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。
  - ステップ 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。
  - ステップ 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。
  - ステップ 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。
- 

### 次の作業

[偽装権限をサーバ レベルで設定する](#)

## 偽装権限をサーバレベルで設定する

次の手順のコマンドは、サーバレベルで偽装権限を許可することができます。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。

### はじめる前に

- 個々の Exchange サーバにアクセスする権限のみをサービス アカウントに付与する場合、「Get-OrganizationConfig」を文字列「Get-ExchangeServer -Identity ServerName」に置き換えます。ここで、ServerName は Exchange サーバの名前です。

#### 例

```
Add-ADPermission -Identity (Get-ExchangeServer -Identity
exchangeserver1).DistinguishedName -User (Get-User -Identity user ?
select-object).identity -ExtendedRights Send-As.
```

- ユーザの SMTP アドレスが alias@FQDN として定義されていることを確認します。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。

### 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** 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。

#### Syntax

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

#### Example

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

### 次の作業

[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](#)

## 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

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)。

### はじめる前に

- 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。

## 手順

- ステップ 1** Exchange 管理シェル (EMS) を開きます。
- ステップ 2** 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。

**Syntax**

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

**Example**

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User -Identity Ex2007 | select-object).identity -ExtendedRight ms-Exch-EPI-Impersonation
```

- ステップ 3** 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。

**Syntax**

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

**Example**

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User -Identity Ex2007 | select-object).identity -ExtendedRight ms-Exch-EPI-May-Impersonate
```

## 次の作業

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

# 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

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 権限を付与するには、次の手順に従ってください。



(注) 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。

## 手順

- ステップ 1** Exchange 管理シェル (EMS) を開きます。
- ステップ 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。

**Syntax**

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

**Example**

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User -Identity Ex2007 | select-object).identity -ExtendedRights Send-As
```

**次の作業**

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

## 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

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** 権限を付与するには、次の手順に従ってください。

**(注)**

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。

**手順**

- ステップ 1** Exchange 管理シェル (EMS) を開きます。
- ステップ 2** EMS で次の `Add-ADPermission` コマンドを実行して、サービス アカウントおよび関連するすべてのメールボックス ストアに **Receive As** 権限を付与します。

**Syntax**

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

**Example**

```
Add-ADPermission -Identity (Get-OrganizationConfig) .DistinguishedName -User (Get-User -Identity EX2007 | select-object) .identity -ExtendedRights Receive-As
```

**(注)**

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.4-6)

## 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。[Microsoft Exchange 2007 の設定 \(EWS\)](#)

## 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)] を確認し、[セキュリティ (Security)] タブで以下を確認します。
- サービス アカウントがリストされている。
  - 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。



(注)

アカウントまたは偽装権限が **ステップ 5** 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。

- 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。
- ステップ 7** 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.4-11)。

# Microsoft Exchange 2010 の設定 (EWS)

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場合、次の手順を実行します。

- Windows のセキュリティ設定の確認
- 特定のユーザまたはユーザ グループに Exchange の偽装権限を設定する

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 サーバと Cisco Unified 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 パラメータ値が設定されていることを確認します。これらは、Cisco Unified Presence と EWS 予定表の統合が正しく動作するために必要な値です。



(注)

デフォルトのスロットル ポリシー設定を修正する必要はありません。新しいポリシーが表の推奨値で作成できます。

表 4-1 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	5000
EWSFastSearchTimeoutInSeconds	60
EWSFindCountLimit	1000

## Windows のセキュリティ設定の確認

Cisco Unified Presence は、NTLMv1 Windows 統合認証のみサポートし、現在 NTLMv2 をサポートしていません。

NTLMV2 が有効ではないことを確認するには、次の手順を実行します。

### 手順

- ステップ 1** Exchange を実行している Windows サーバで [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)] を選択します。
- ステップ 2** [セキュリティの設定 (Security Settings)] > [ローカル ポリシー (Local Policies)] > [セキュリティのオプション (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 (Network Security)] を選択 : NTLM SSP ベース (セキュア RPC を含む) サーバの最小セッション セキュリティ。
- 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、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 を実行している Windows サーバをリブートします。



## 特定のユーザまたはユーザ グループに Exchange の偽装権限を設定する

特定のユーザまたはユーザ グループに Exchange の偽装権限を設定するには、Exchange 管理シェル (EMS) を使用して次の手順を実行します。

### 手順

- ステップ 1** Active Directory でアカウントを作成します。
- ステップ 2** コマンド ライン入力を行うために EMS を開きます。
- ステップ 3** EMS で New-ManagementRoleAssignment コマンドを実行し、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。

#### Syntax

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

#### Example

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

- ステップ 4** 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、Ex2010 アカウントに付与されます。

#### Syntax

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

#### Example

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

- ステップ 5** 表 4-1 で定義された推奨値を含む新しいスロットル ポリシーを作成するには、新しい ThrottlingPolicy コマンドを実行します。

#### Syntax

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

#### Example

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



(注)

サポートされる Exchange SP1 でのみ使用可能です。

- ステップ 6** 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。

#### Syntax

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

#### Example

```
Set-ThrottlingPolicyAssociation -Identity "Ex2010" -ThrottlingPolicy "Cisco Unified
Presence ThrottlingPolicy"
```

**次の作業**

「Exchange 2010 アカウントの権限の確認」(P.4-10)

**関連トピック**

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**

「Microsoft Exchange 2010 の設定」で指定された手順を実行します。「Microsoft Exchange 2010 の設定 (EWS)」(P.4-7)

**手順**

- ステップ 1** Active Directory サーバで、偽装アカウントが存在することを確認します。
- ステップ 2** コマンドライン入力を行うために Exchange 管理シェル (EMS) を開きます。
- ステップ 3** Exchange サーバで、サービス アカウントに必要な次の偽装権限が付与されていることを確認します。
- EMS で次のコマンドを実行します。

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

- 指定アカウントに対する役割「ApplicationImpersonation」の役割の割り当てがコマンド出力に示され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 4** 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。
- EMS で次のコマンドを実行します。
- ```
Get-ManagementScope _suImpersonateScope
```
- 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<br>-----           | ScopeRestrictionType<br>----- | Exclusive<br>----- | RecipientRoot<br>----- | Recipient<br>Filter<br>----- | ServerFilter<br>----- |
|-------------------------|-------------------------------|--------------------|------------------------|------------------------------|-----------------------|
| _suImpersonate<br>Scope | ServerScope                   | False              |                        |                              | Distinguished<br>Name |

**ステップ 5** 次のコマンドを実行して、ThrottlingPolicy パラメータが表 4-1 で定義されている内容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
```

## 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」\(P.4-11\)](#)

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

EWS 統合が正しく動作するためには、EWS 仮想ディレクトリ (/EWS) 上で基本認証または Windows 統合認証を有効にする必要があります。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 を実行する Exchange 2007 の認証の有効化」\(P.4-11\)](#)
- [「Windows Server 2008 を実行する Exchange 2010 の認証の有効化」\(P.4-12\)](#)

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

Windows Server 2003 を実行する Exchange 2007 で認証を有効にするには、次の手順を実行します。

## 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。次に適切なサーバを選択します。
- ステップ 2** [Web サイト (Web Sites)] を選択します。
- ステップ 3** [既定の Web サイト (Default Web Site)] を選択します。
- ステップ 4** EWS 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 5** [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 6** [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 7** [認証方法 (Authentication Methods)] の下で、次のチェックボックスがオフになっていることを確認します。
  - [匿名アクセスを有効にする (Enable anonymous access)]

- ステップ 8** [ 認証方法 (Authentication Methods) ] の [ 認証済みアクセス (Authenticated Access) ] の下で、次のチェックボックスのいずれかまたは両方がオンになっていることを確認します。
- [ 統合 Windows 認証 (Integrated Windows Authentication) ]
  - [ 基本認証 (Basic Authentication) ] (パスワードはクリア テキストで送信されます)。
- ステップ 9** [OK] を選択します。
- 

#### 次の作業

「Microsoft Exchange 統合のための Cisco Unified Presence のプレゼンス ゲートウェイの設定」(P.5-1)

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

Windows Server 2008 を実行する Exchange 2010 で認証を有効にするには、次の手順を実行します。

#### 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) ] を選択します。
- ステップ 3** [ 既定の Web サイト (Default Web Site) ] を選択します。
- ステップ 4** [EWS] を選択します。
- ステップ 5** [IIS] セクションで、[ 認証 (Authentication) ] を選択します。
- ステップ 6** 次の認証方法が有効になっていることを確認します。
- 匿名認証
  - **Windows 認証**や基本認証
- ステップ 7** 適切に設定するには、[ 操作 (Actions) ] カラムで有効または無効のリンクを使用します。
- 

#### 次の作業

「Microsoft Exchange 統合のための Cisco Unified Presence のプレゼンス ゲートウェイの設定」(P.5-1)

#### 関連トピック

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