Active Directory モジュール

管理者ガイド

AD モジュールのインストール、設定、および使用方法

目次

Chapter 1

イントロダクション

Sitecore CMS 6 は、ASP.NET 2.0 のプロバイダー モデルを基盤とした、自己完結型の強固なセキュリティ モデルを備えていますが、エンタープライズ ソリューションでは、複雑なセキュリティ インフラが必要な場合があります。多くの企業では、Active Directory などのディレクトリ サービスで既にドメインを設置しています。

Sitecore CMS Active Directory モジュールは、Sitecore CMS ソリューションに Active Directory のドメインを統合するものです。このモジュールをインストールおよび設定すると、ドメインのユーザーおよびグループを Sitecore CMS に直ちに取り込んで、Sitecore ユーザーおよび Sitecore ロールとして使用できます。また、Active Directory のカスタム プロパティでユーザー プロファイルを簡単に拡張できます。

この文書では、Active Directory モジュールのインストール、設定、および使用方法について説明します。また、使用している技術の背景となるアーキテクチャについても説明します。

この文書を読む前に、『CMS のロー レベルのセキュリティとカスタム プロバイダー』の内容を理解しておくことを強くお勧めします。

Chapter 2

インストールと設定

この章では、モジュールのインストールと設定の手順について説明します。Active Directory モジュールは、他の Sitecore CMS 6 モジュールとは違い、web.config ファイルを手動で修正する必要があります。

この章には次のセクションがあります。

- Sitecore CMS パッケージのインストール
- web.config ファイルの手動修正

2.1 Sitecore パッケージのインストール

Active Directory モジュールは、通常の Sitecore パッケージとして配布されています。インストールには、Sitecore デスクトップのリンク [Sitecore] » [開発ツール] » [インストール ウィザード] から起動するインストール ウィザードを使用できます。

2.2 web.config の修正

モジュールのインストールを完了するには、パッケージをインストールした後で、web.config ファイルに手動でいくつかの修正を加える必要があります。手動で修正が必要なのは次に示す部分のみです。

- `/App_Config/connectionStrings.config` ファイル
- `/App_Config/Security/domains.config` ファイル
- web.config ファイルの `system.web` セクションと `sitecore/switchingProviders` セクション

2.3 ファイアウォール設定の変更

LDAP の Well-known ポートは、LDAP が 389、LDAP SSL が 636 として確立されています。Active Directory プロバイダーは SSL を使用して Active Directory への接続を試みます。SSL による接続が失敗した場合、次にデジタル署名と暗号化を使用して Active Directory への接続を試みます。両方とも失敗した場合、プロバイダーのインスタンスは ProviderException 例外をスローします。

Active Directory を使用するには、ポート 389 または 636 を開いておく必要があります。

ポート 445 は必要ありません。

2.3.1 Active Directory ドメインへの接続文字列の追加

Active Directory モジュールの導入を決めた場合、接続先となる Active Directory ドメインはその時点で既に導入済みであるのが一般的です。多くの場合、これは企業のドメインで、全社的なセキュリティ基盤がその中に格納されています。

メインの `/App_Config/connectionstrings.config` の `<connectionStrings>` セクションに接続文字列を追加します。SQLite を使用している場合は、`/App_Config/connectionstringssqlite.config` ファイルにも同じ変更が必要です。記述内容の例を次に示します。

```
<connectionStrings>
   <add name="ManagersConnString"
        connectionString="LDAP://testsrv/OU=Managers,DC=testdomain,DC=sitecore,DC=net" />
</connectionStrings>
```

メモ

上で組織単位 (OU) として指定した "Managers" は例にすぎません。使用する環境に合わせて実際の OU を指定する必要があります。

設定コードの内容を確認します。

`<connectionStrings>` 要素では複数の接続文字列を定義できます。それぞれの定義には `<add>` タグを使用します。この要素にはいくつかの属性がありますが、ここで使用するのは次の 2 つのみです。

属性	説明
Name	接続文字列の名前。この接続文字列を使用するエンティティはこの名前を指定します。
connectionString	接続文字列。

Active Directory モジュールがサポートするのは、次のような LDAP 形式の接続文字列です。

- 各文字列の先頭は LDAP:// というプレフィックスです。

- プレフィックスの後に、コンポーネントの接続先サーバー名を指定します。ドメイン名の後にはスラッシュ（/）が必要です。
- 接続文字列の最後の部分で、ユーザーとグループの取得元となる Active Directory コンテナーの完全なパスを指定します。

重要
一部の例外を回避し、Active Directory への接続を安定させるために、Active Directory サーバーの名前は、ポート番号付きの完全修飾ドメイン名（FQDN）で指定してください。たとえば、ADServer.domain.name:389 のような形式です。この場合、接続文字列は次のようになります。

LDAP://ADServer.domain.name:389/OU=Managers,DC=ADDomain,DC=company,DC=com

たとえば、Managers という組織単位 (OU) を使用している企業が、この OU のメンバーを Sitecore CMS に取り込む場合を考えます。また、Active Directory サーバー名は ADServer で、ADDomain.company.com というドメインに設置されているものとします。

この場合、接続文字列は次のようになります。

```
LDAP://ADServer/OU=Managers,DC=ADDomain,DC=company,DC=com
```

Support Managers というサブ OU を使用する場合は、接続文字列は次のように変わります。

```
LDAP://ADServer/OU=Support Managers,OU=Managers,DC=ADDomain,DC=company,DC=com
```

逆にドメイン全体を使用する場合は、接続文字列は次のように変わります。

```
LDAP://ADServer/DC=ADDomain,DC=company,DC=com
```

LDAP 接続文字列の形式の詳細については、MSDN のこの記事を参照してください。

2.3.2 ASP.NET のセキュリティ プロバイダーの設定

Active Directory モジュールは ASP.NET のセキュリティ モデル アーキテクチャを基盤としています。そのため、このモジュールには、ユーザー、ロール、およびプロファイルのプロパティを管理するための基本的なプロバイダーが用意されています。

次の表は、それぞれのプロバイダーの概要です。

サービス	説明
メンバーシップ プロバイダー	ユーザーの取得、作成、更新、および削除や、ユーザー名とパスワードによるユーザーの検証、ユーザーのパスワードの変更などを行うための一連の操作を提供します。メンバーシップ サービスの詳細については、MSDN ライブラリを参照してください。

サービス	説明
ロール プロバイダー	ロールの取得、作成、削除、ロールへのユーザーの追加、およびロールからのユーザーの削除を行うための一連の操作を提供します。ロール サービスの詳細については、MSDN ライブラリを参照してください。
プロファイル プロバイダー	ユーザー プロファイルのプロパティの取得/設定や、プロファイル オブジェクトに対するその他の処理 (プロファイルの削除/検索など) を行うための一連の操作を提供します。プロファイル サービスの詳細については、MSDN ライブラリを参照してください。

メンバーシップ プロバイダーの設定

`web.config` ファイルを開き、`<system.web>` セクション内の `<membership>` 要素を検索して、その中に次のコードを貼り付けます (順序は重要ではありません)。

```
                <add name="ad"
                     type="LightLDAP.SitecoreADMembershipProvider"
                     connectionStringName="ManagersConnString"
                     applicationName="sitecore"
                     minRequiredPasswordLength="1"
                     minRequiredNonalphanumericCharacters="0"
                     requiresQuestionAndAnswer="false"
                     requiresUniqueEmail="false"
                     connectionUsername="[put the username here]"
                     connectionPassword="[put the password here]"
                     connectionProtection="Secure"
                     attributeMapUsername="sAMAccountName"
                     enableSearchMethods="true"
                    />
```

次の表は、このプロバイダー定義の各属性の説明です。

属性	説明
name	プロバイダー名。通常、プロバイダー名には、メンバーシップ プロバイダー セット内で一意となる任意の文字列値を使用できます。しかし、設定の一部が自動で行われるため、この要素に関しては、各項目を変更しないでおくために、`ad` という名前を使用する必要があります。
type	プロバイダー クラスの完全な名前。
connectionStringName	接続文字列の名前。この例では `ManagersConnString` としています。
applicationName	すべてのプロバイダーの標準的な属性で、プロバイダー データの認識可能範囲を定義します。この例では `sitecore` とする必要があります。詳細については、MSDN のドキュメントを参照してください。
minRequiredPasswordLength	ユーザーのパスワードに必要な最小文字数。デフォルト値は `1` です。

属性	説明
minRequiredNonalphanumericCharacters	ユーザーのパスワードに必要な非英数字の最小文字数。デフォルト値は `0` です。
requiresQuestionAndAnswer	ユーザーのパスワードに対する質問と回答の設定をプロバイダーが要求するかどうかを定義します。デフォルトは `false` です。
requiresUniqueEmail	各ユーザーに対して一意の Email を設定するようプロバイダーが要求するかどうかを定義します。デフォルトは `false` です。
connectionUsername	Active Directory (AD) ドメインに接続するためには、必要な操作を実行するための十分な権限を持つユーザーを指定する必要があります。これらの資格情報は、AD ドメインに接続するときにプロバイダーが使用します。ここでユーザー名を定義します。
connectionPassword	ユーザーのパスワード。
connectionProtection	プロバイダーのシステム属性。必ず `Secure` (デフォルト値) に設定します。
attributeMapUsername	ユーザー名として使用する Active Directory 属性を定義する属性。デフォルトは `sAMAccountName` です。
enableSearchMethods	`true` (デフォルト値) に設定すると、プロバイダーの検索機能が有効になります。

重要なメモ

- パスワードの入力誤りが所定の回数を超えてもユーザーをロックできない場合は、使用する AD ドメインでアカウント ロックアウト ポリシーが正しく設定されていることを確認してください。

- パスワードをリセットする機能を有効にするためには、上の設定で `enablePasswordReset` 属性を指定し、その値を `true` に設定する必要があります。そのほか、プロバイダーの要件として、Active Directory のプロパティにいくつかの属性をマッピングする必要があります。詳細については、このトピックに関する MSDN の記事を参照してください。また、新しいパスワードが、使用する AD ドメインのパスワードに関するドメイン セキュリティ ポリシーの要件を満たしていることを確認してください。

- `connectionProtection` 属性を `Secure` に設定する場合は、`<system.web>` セクションに次のような要素を 1 つまたは複数追加する必要があります (このセクション内の任意の位置に配置できます)。

```
<!-- Machine key attributes -->
<machineKey
validationKey="BDDFE367CD36AAA81E195761BEFB073839549FF7B8E34E42C0DEA4600851B0065856B211719ADEFC76F3F3A556BC61A5FC8C9F28F958CB1D3BD8EF9518143DB6"
decryptionKey="0DAC68D020B8193DF0FCEE1BAF7A07B4B0D40DCD3E5BA90D" validation="SHA1" />
```

- このキーは、クライアントと Active Directory サーバーの間でやり取りするデータの暗号化/復号化に使用されます。このキーを web.config に貼り付けるか、または、このページかこのページで独自のキーを生成します。

- 上で説明した .config の修正を実行する前に Sitecore CMS シェルにログインしていた場合、"パディングが有効ではありません" というエラー メッセージが表示されることがあります。これは、システム キーを追加して接続の保護レベルを変更したことによるものです。このエラーが表示されないようにするには、ブラウザーの Cookie を消去します。それでもエラーになる場合は、ブラウザーを再起動します。

ロール プロバイダーの設定

web.config ファイルを開き、<system.web> セクション内の <roleManager> 要素を検索して、その中に次の定義を貼り付けます (順序は重要ではありません)。

```
<add name="ad" type="LightLDAP.SitecoreADRoleProvider"
connectionStringName="ManagersConnString"
     applicationName="sitecore" username="[put the username here]"
     password="[put the password here]"
     attributeMapUsername="sAMAccountName" />
```

この要素の属性は前掲の表のとおりで、ロール プロバイダーの場合も意味は同じです。

attributeMapUsername は、共通の接続文字列を使用するすべてのプロバイダーで同じ値にする必要があります。

プロファイル プロバイダーの設定 (オプション)

Active Directory モジュールには、追加のプロパティを Active Directory ドメインに格納するオプションが用意されています。この設定には、web.config でのプロバイダーの設定とは別に、追加の手順が必要です。その方法については、この文書の「高度なプロファイル設定」のセクションで説明します。

メモ
Active Directory のカスタム属性でユーザー プロファイルを拡張する必要がない場合は、「高度なプロファイル設定」の章の手順は省略できます。

スイッチング プロバイダーの有効化

ユーザーとロールの取得元が他にも存在することをシステムに認識させるには、スイッチングの仕組みを有効化する必要があります。それには、次の手順に従います。

- web.config ファイルで、<system.web> セクションの <membership> 要素に移動し、sitecore というプロバイダーを見つけて、realProviderName 属性を switcher に設定します。

- web.config ファイルで、<system.web> セクションの <roleManager> 要素に移動し、sitecore というプロバイダーを見つけて、realProviderName 属性を switcher に設定します。

この操作の結果は、サービスのルート要素 (membership または roleManager) の defaultProvider 属性を変更した場合と同じです。しかし、CMS システムの動作上、sitecore という名前のプロバイダーが必要です。詳細については、『CMS のロー レベルのセキュリティとカスタム プロバイダー』の記事を参照してください。

新規ドメインの追加

App_Config/Security/Domains.config.xml ファイルを開き、ルート要素に次の行を追加します。

```
        <domain name="ad" ensureAnonymousUser="false"/>
```

ドメインとプロバイダーのマッピングの追加

web.config ファイルを開き、<sitecore> セクションの <switchingProviders> 要素に移動します。この中には、<membership>、<roleManager>、および <profile> という 3 つのグループがあります。

- <membership> グループに次の行を追加します (順序は重要ではありません)。
  ```
  <provider providerName="ad" storeFullNames="false" wildcard="*"
  domains="ad" />
  ```

- <roleManager> グループに次の行を追加します (順序は重要ではありません)。
  ```
  <provider providerName="ad" storeFullNames="false" wildcard="*"
  domains="ad" />
  ```

- (オプション) <profile> グループに次の行を追加します (このグループの最初の定義として追加する必要があります。この機能の詳細については、この文書の「高度なプロファイル設定」のセクションを参照してください)。
  ```
  <provider providerName="ad" storeFullNames="false" wildcard="*"
  domains="ad" />
  ```

"順序は重要ではありません" という但し書きは、順序を変えても定義の機能が変わらないことを表します。唯一、順序によって違いが生じるのは、Sitecore CMS 6 のセキュリティ ツールでのユーザー/ロールの順序です。たとえば、ad のメンバーシップのマッピングを sql よりも前に配置すると、ユーザー マネージャーでは、デフォルトの Sitecore CMS ユーザーよりも Active Directory ユーザーの方が先に表示されます。

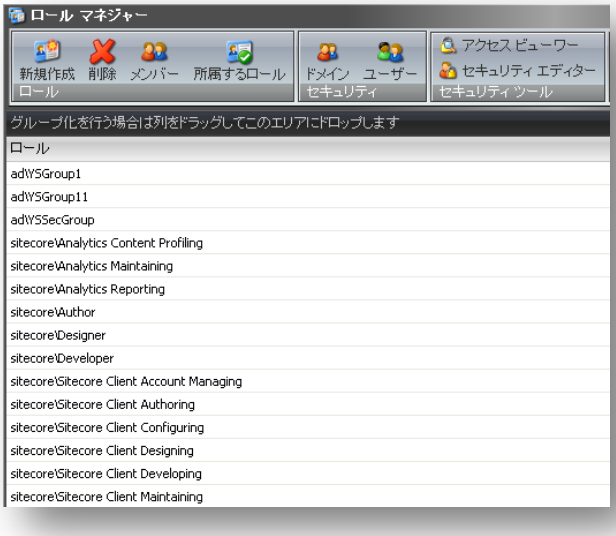
Chapter 3

基本的な操作

注意
Sitecore CMS で加えた変更は、Active Directory ユーザーに即座に反映されます。つまり、実際の Active Directory オブジェクトに変更が直ちに適用されます。唯一の例外はユーザーのロックアウトです。ユーザーは Sitecore CMS のみでロックアウトされ、Active Directory ドメインでは引き続き有効です。

設定の手順が完了したら、Sitecore CMS を起動し、管理者アカウントでデスクトップ インターフェースにログインします。

ロール マネージャー アプリケーションを起動します ([Sitecore] » [セキュリティ ツール] » [ロール マネージャー])。Active Directory から取得したロールが、Sitecore CMS のロールと共に表示されます。



"ad¥" というプレフィックスは、ad という Sitecore ドメインに属するロールであることを表します。Sitecore CMS の各ドメインには単一のプロバイダーを通じて対応できます。詳細については、『CMS のロー レベルのセキュリティとカスタム プロバイダー』の記事を参照してください。

ユーザー マネージャーを起動すると、Active Directory ユーザーが同様に表示されます。

メモ
Active Directory モジュールをインストールする前に比べると、ロール マネージャーまたはユーザー マネージャーのアプリケーションの起動に時間がかかることがあります。この時間は、接続した Active Directory ドメインのエンティティ数に応じて変わります。ユーザーやロールが多いほど、時間は長くかかります。

3.1 ロールとユーザーの管理

Active Directory ドメインから取得したユーザーに対しても、通常の Sitecore CMS ユーザーと同様に変更を加えることができます。この操作は、標準のロール マネージャーおよびユーザー マネージャーを使用して実行できます。

たとえば、ad¥john というユーザーが Sitecore CMS デスクトップにログインできるようにするには、sitecore¥Sitecore Client Users ロールにこのユーザーを追加するだけです。こうすると、ad¥john ユーザーとしてログインして Sitecore デスクトップを使用できるようになります。

メモ
ログイン時には、ドメイン名を含む完全なユーザー名を指定する必要があります。

特定の Active Directory ロールを持つすべてのユーザーが Sitecore シェルにログインできるようにするには、そのロールを sitecore¥Sitecore Client Users ロールに追加します。この場合は、ロール内ロールの機能によって目的の操作が可能となります。

この部分に関しては、ある制約が存在します。Active Directory のロールに追加するユーザーは、同じ Active Directory ドメインに属するユーザーでなくてはならないというものです。したがって、Sitecore CMS のユーザーは Active Directory のロールに追加できません。しかしこの制約は、ロール内ロールの機能によって簡単に回避できます。つまり、目的の Sitecore CMS ユーザーを Sitecore CMS のロールに追加したうえで、そのロールを Active Directory のロールに追加するという方法です。ロール内ロールのサービスは ASP.NET プロバイダー上で機能するため、このような方法が可能です。

3.1.1 ユーザー/ロールの作成

Active Directory にユーザーまたはロールを作成するには、[新規ユーザー] または [新規ロール] ダイアログで適切なドメイン (この例では ad) を選択します。

3.1.2 ユーザー固有の操作

パスワードの変更、有効化、ロックなどの操作は、Active Directory ユーザーに対しても、通常の Sitecore CMS ユーザーと同様に適用されます。

Chapter 4

高度なプロファイル設定

Active Directory モジュールでは、ユーザー プロファイルのカスタム プロパティを、対応するドメイン ユーザー オブジェクトの属性に格納できます。たとえば、Active Directory で各ユーザーに電話番号を設定している場合、Sitecore CMS で各ユーザーに対してこのプロパティを表示できます。

このセクションでは、このような機能を有効化する方法について、順を追って説明します。

4.1 プロファイル プロバイダーの設定

まず、プロファイル プロバイダーの定義を追加する必要があります。web.config ファイルを開き、<system.web> セクションの <profile> 要素に移動します。

profile/providers 要素の中に次のプロバイダー定義を貼り付けます (順序は重要ではありません)。

```
<add name="ad" type="LightLDAP.SitecoreADProfileProvider"
connectionStringName="ManagersConnString"
     applicationName="sitecore" username="[put the username here]"
     password="[put the password here]" />
```

次に、<profile> 要素の defaultProvider 属性を switcher に変更します。

通常の設定手順では、プロファイル プロバイダーに対しても、他のサービスと同様にマッピングの対応を指定する必要があります。前の設定時にこの手順を省略した場合は、ここで行います。それには、メインの web.config ファイルで switchingProviders/profile 要素に移動し、次のコードを追加します。

```
        <provider providerName="ad" storeFullNames="false" wildcard="*" domains="ad" />
```

技術メモ

この要素はセクションの先頭に配置する必要があります。その理由は明白です。プロファイル サービスのデフォルトである SQL Server プロバイダーは非常に汎用的であり、適切なプロファイル プロパティが見つからない場合、カスタム プロパティであるものとみなして、カスタム テーブルに格納します。このため、SQL Server プロバイダーがセクションの先頭にあると、必ずすべてのプロパティを処理してしまいます。AD プロバイダーがプロパティを処理して AD ドメインの情報を提供できるようにするためには、その定義をこのセクションの先頭に配置する必要があります。

4.2 カスタム プロパティの設定

プロファイルの拡張に使用するカスタム プロパティは、<profile> 要素の <properties> グループで定義する必要があります。この例では、ここに telephoneNumber プロパティを配置します。そこで、web.config ファイルの <system.web> セクションの <profile> 要素に移動し、その中の <properties> グループを見つけて、次のコードを追加します (順序は重要ではありません)。

```
<add type="System.String" name="Telephone" customProviderData="ad|unicode
string|telephoneNumber" />
```

次の表は、この定義の各属性の説明です。

属性	説明
Name	プロパティの一意の名前。
Type	プロパティの .NET 型。ASP.NET 環境でこのプロパティが持つ型です。ad のプロファイル プロパティでは、このパラメーターは必ず System.String とします。Sitecore はすべてのプロパティを文字列型で処理します。
customProviderData	このプロパティを処理するプロバイダーが必要とする任意のデータ。この例で指定した ad とは、このプロパティを ad プロバイダーが処理するという意味です。unicode string は、Active Directory でのこのプロパティのネイティブ型を表します。telephoneNumber は、対応する Active Directory 属性の名前を表します。通常、この属性には任意の形式を使用できます。ad プロバイダーでは、属性の各部分がパイプ文字 (|) で区切られているものと見なします。

Active Directory モジュールでは、customProviderData は ad|[native type name]|[ad native name] という形式であるものとします。native type name は、Active Directory でのこのプロパティの型です。サポートされているのは、基本型の unicode string, boolean および integer です。他の値を指定した場合は、代わりに unicode string 型が使用されます。最後の ad native name という部分は省略可能で、Active Directory の対応するプロパティの実際の名前を表します。省略した場合は、name 属性の値が使用されます。

メモ

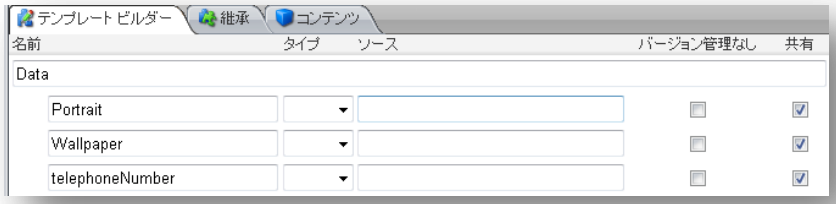
Active Directory モジュールでは、Active Directory のカスタム属性を Sitecore CMS のロールに反映する処理はサポートされていません。Sitecore CMS のセキュリティは .NET のセキュリティ モデルを基盤としており、そのエンジンでは、ロールに対して何らかのプロファイルを設定するオプションが用意されていません。そのような反映は、Sitecore CMS でも Active Directory モジュールでもサポートされていません。

4.3 Sitecore テンプレートの拡張

web.config ファイルでカスタム プロパティを定義したら、Sitecore CMS セキュリティ アプリケーションからそれらのプロパティを利用できるように Sitecore テンプレートを拡張します。

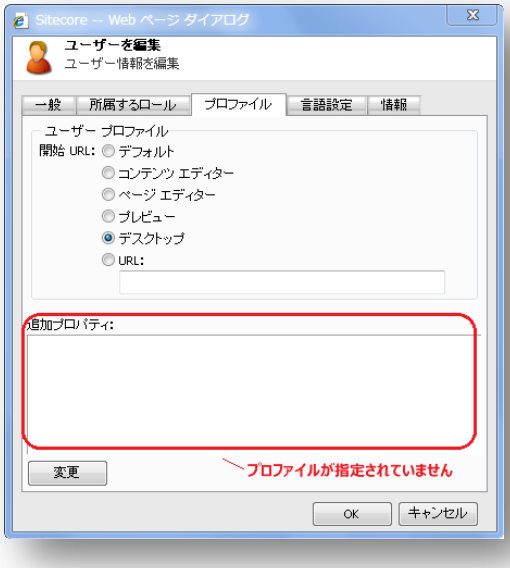
その手順は次のとおりです。

- Sitecore CMS を起動し、管理者の資格情報でログインして、`core` データベースに切り替えます。
- コンテンツ エディターを開き、コンテンツ ツリーで `/sitecore/templates/System/Security/User` テンプレートを参照します。
- このテンプレートに `Telephone` という新しいフィールド（web.config の適切なプロパティ名と完全に一致）を追加します。タイプは `Single-Line Text` とし、`Shared` はオンにします。



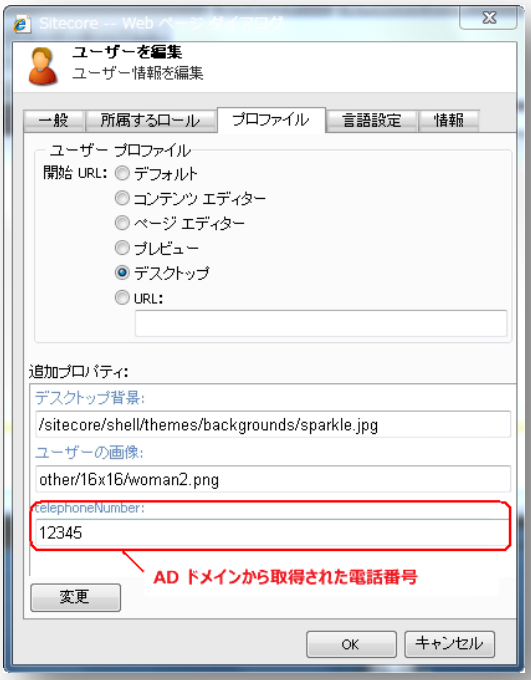
- 変更を保存し、`master` データベースに切り替えます。
- ユーザー マネージャーを開き、Active Directory ドメインの任意のユーザー (たとえば `ad\john`) を編集します。

- [プロファイル] タブに切り替えます。



- [変更] ボタンをクリックしてユーザー テンプレートを選択します。
- このウィンドウを閉じます。

ユーザー ad¥john を再度編集して [プロファイル] タブに切り替えると、プロファイルが拡張され、telephoneNumber プロパティが追加されています。



このプロパティには Active Directory ユーザーの `telephoneNumber` 属性の値が設定されます。この機能の詳細について、およびプロファイルの拡張をサポートするためにプロバイダーが満たすべき必要条件については、『CMS のロー レベルのセキュリティとカスタム プロバイダー』の記事を参照してください。

デフォルト以外のプロファイルを AD ユーザーに自動で割り当てる方法

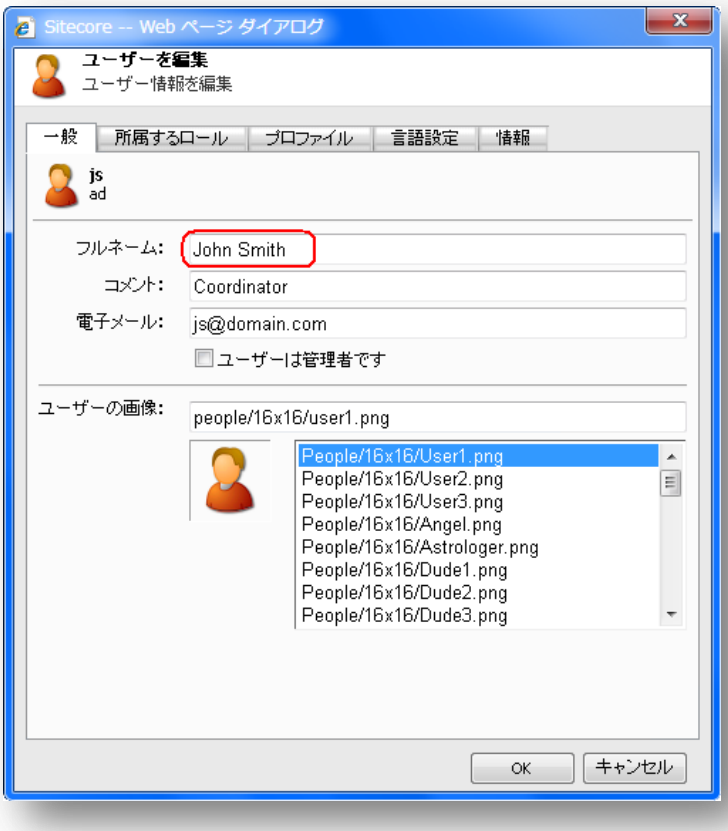
上で説明した Sitecore プロファイル テンプレートの拡張手順には、プロファイル アイテムをユーザーに割り当てる操作があります。そのような手動の操作を数百人のユーザーに対して行うことは、明らかに現実的ではありません。そのため、Sitecore には、共通のプロファイル アイテムをドメイン レベルで設定できる機能があります。

/App_Config/Security/Domains.config.xml ファイルを開き、domains 要素に次の行を追加します。`<domain name="ad" ensureAnonymousUser="false" defaultProfileItemID="{DDEDA46F-169B-4A70-8732-DBD3F407AF2E}"/>` defaultProfileItemID 属性は、当該ドメインのユーザーにプロファイルが明示的に設定されていない場合に使用されるプロファイル アイテムを定義します。

4.4 Active Directory の "表示名" の属性と Sitecore の Full Name プロパティのマッピング

AD ユーザーの DisplayName プロパティの値は、デフォルトの Full Name フィールドに自動的に渡されます。

このプロパティに対応する新しいフィールドでユーザーのプロファイル テンプレートを拡張する必要はありません。[ユーザーを編集] ダイアログの [一般情報] タブの [フルネーム] ボックスに次のように値が表示されます。



Full Name フィールドに別の AD プロパティをマッピングする場合は、App_config/Include/ldap.config ファイルを使用します。LDAP.FullName に適切な値を次のように設定します。

```
<!-- FULL NAME PROPERTY NAME
     Determines the full name property mapping.
-->
<setting name="LDAP.FullName" value="ad|unicode string|displayName" />
```

メモ

このマッピングをサポートするために、前に説明した方法で高度なプロファイルの機能を設定しておく必要があります。

Chapter 5

機能

Active Directory モジュールには、セキュリティへの対応を簡単かつ便利にするための追加機能が用意されています。主な機能を次に示します。

- シングル サインオン
- ステータス ページ
- デバッグ モード
- 複数ドメインへの接続
- 間接メンバーシップ

5.1 シングル サインオン

通常、ドメイン コントローラーを設置している組織では、各ワークステーションはそのドメインに属しています。ここで、Managers という組織単位と Sitecore CMS の間で接続を確立したとすると、この組織単位のメンバーは、Sitecore CMS で自らのロールに応じた操作を実行できます。当然、これらのユーザーにとっては、Sitecore CMS に自動でログインできた方が便利です。ユーザーが Sitecore CMS の操作を開始するときには、自らの組織のドメインにも必ずログインしています。

この機能をシングル サインオンといい、Active Directory モジュールにはそのための方法が用意されています。

5.1.1 必要条件

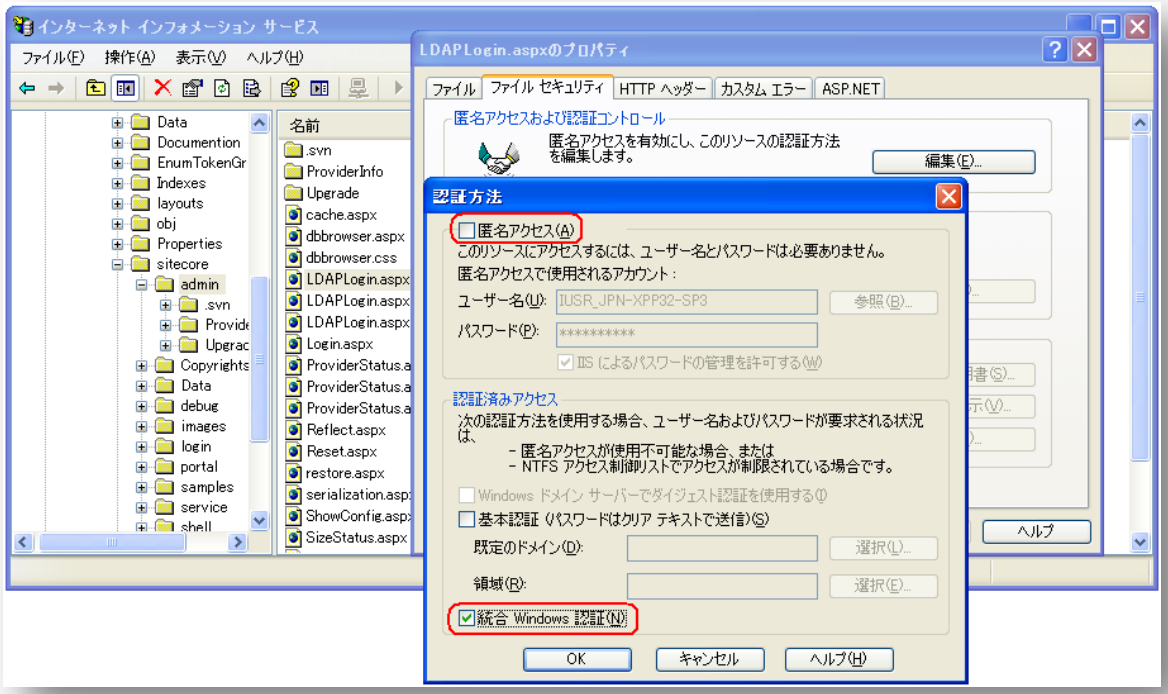
この機能を使用するには、次のような必要条件があります。

- ワークステーションは対象となるドメインのメンバーである必要があります。
- `/sitecore/admin/ldaplogin.aspx` ページへの匿名アクセスが無効で、統合 Windows セキュリティ モードが有効である必要があります。

IIS で匿名アクセスを無効にするには、次の手順に従います。

- IIS を起動します。
- 対象の Web サイトを展開します。
- `/sitecore/admin` フォルダーに移動し、`LDAPLogin.aspx` ページを選択します。
- LDAPLogin.aspx ページを右クリックし、[プロパティ] をクリックします。
- [ファイル セキュリティ] タブをクリックし、匿名アクセスのチェック ボックスをオフにします。

この結果、IIS の設定は次のようになります。

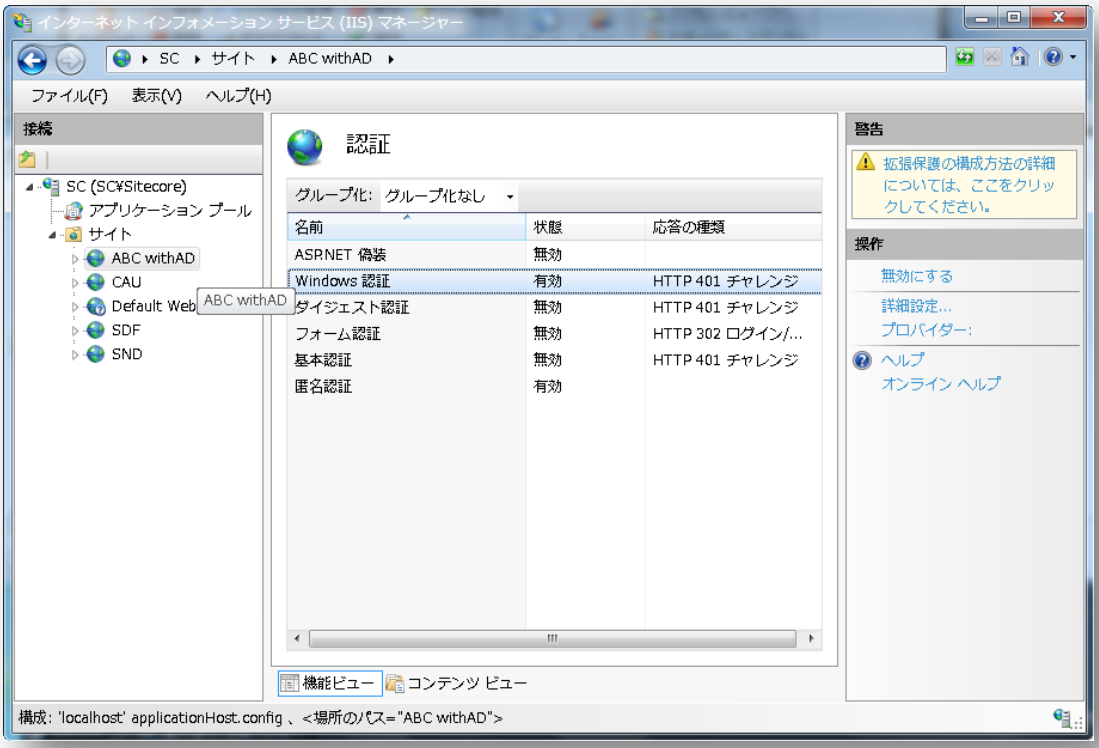


IIS 7 の設定

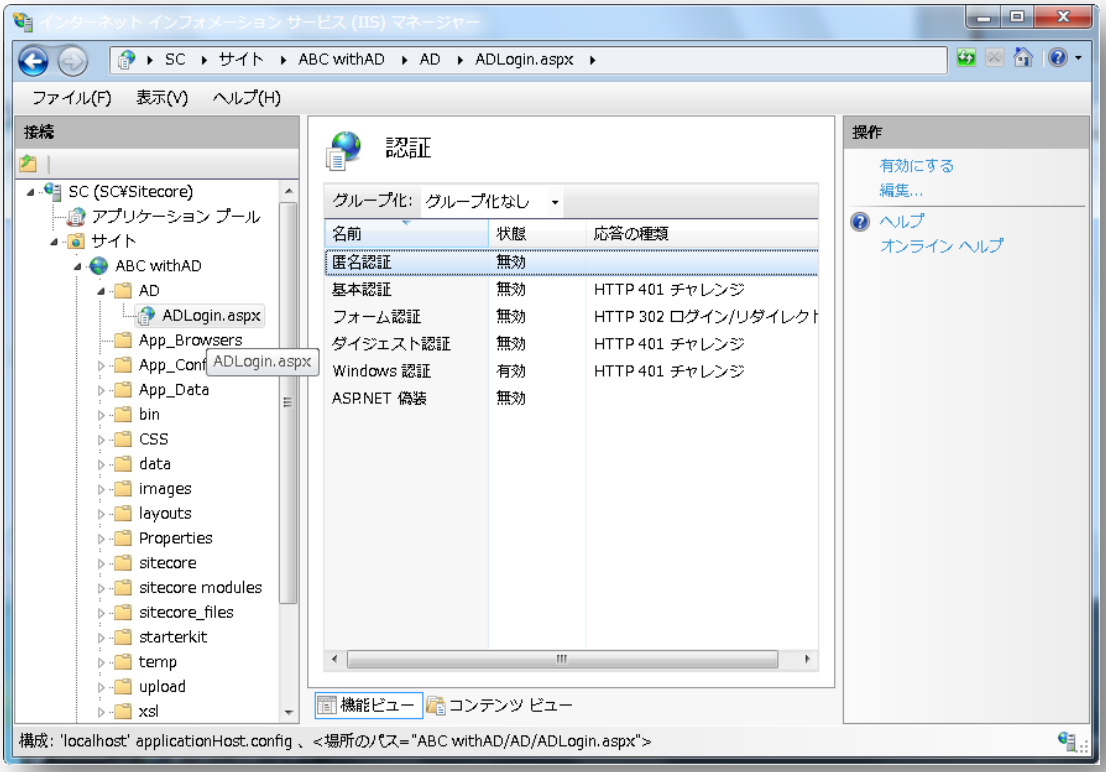
IIS 7 の場合は設定が若干異なります。このバージョンの IIS の場合は、次の手順を参考にしてください。

まず IIS 7 では、混合認証モードがサポートされていません。このため、サイトに対して複数の種類の認証を有効にすることができません。

Windows 認証を使用するには、次に示すように、サイトのフォーム認証 (Sitecore のデフォルト) を無効にし、Windows 認証を有効にする必要があります。



次の手順は基本的です。AD ログイン ページに移動し、次に示すように、このページへの匿名アクセスを無効にする必要があります。

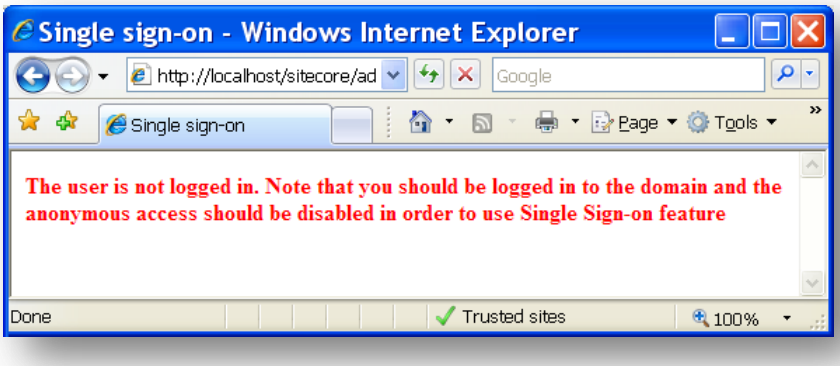


5.1.2 使用方法

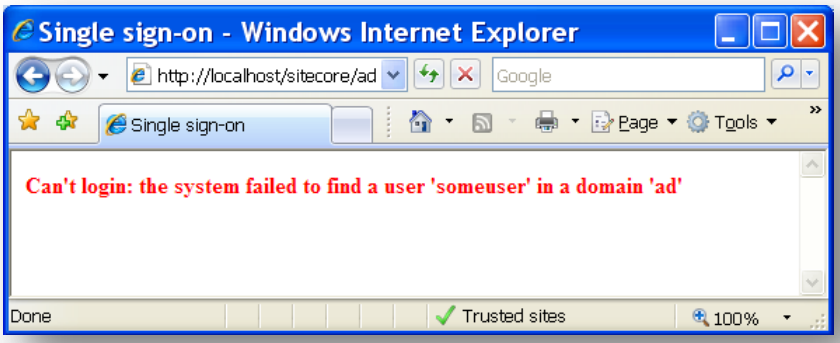
必要条件を満たしたら、ユーザーの資格情報を手動で入力しなくても、システムのアカウントで Sitecore CMS にログインできます。ブラウザーで次の URL を開きます。`http://[yoursite]/sitecore/admin/LDAPLogin.aspx`

メモ
デフォルトの Sitecore シェルのログイン ページ (`http://[yoursite]/sitecore`) を開くことで、これまで同様に通常の方法でログインすることもできます。

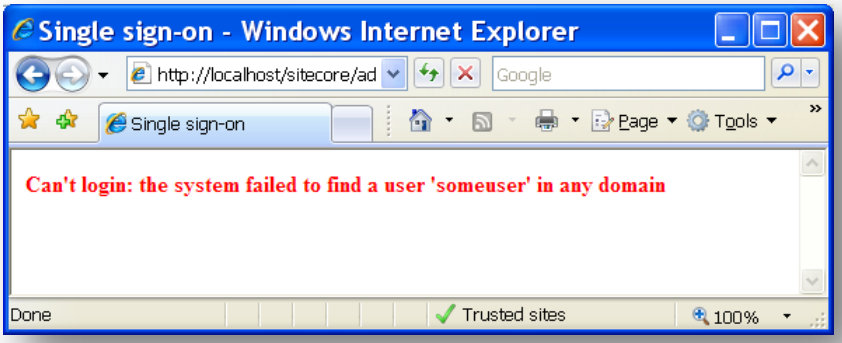
必要条件の確認を忘れて、マシンがドメインに属していない場合や、ログイン ページの匿名アクセスが無効になっていない場合には、システムによる自動ログインは行われず、その理由が次のように表示されます。



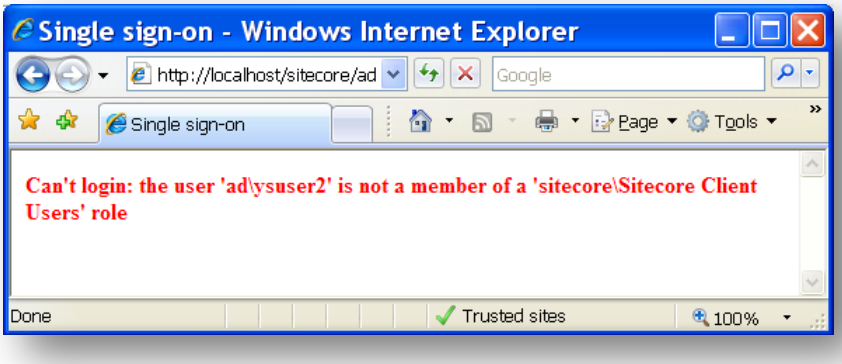
ユーザーの資格情報をシステムが解析する段階でエラーが発生することもあります。たとえば、ドメイン名は正しく、ユーザーは Active Directory ドメインのメンバーでもあるが、Sitecore と接続した Managers という組織単位のメンバーではない、という場合には、次のような警告が表示されます。



実際のドメイン名が Sitecore CMS で入力したドメイン名と異なる場合もあります。たとえば、実際には Company.com という Active Directory ドメインのユーザーだが、Sitecore CMS ではこのドメインを ad として接続しているとします (これがデフォルト設定です)。この場合システムは、ログインの処理は拒否しないものの、存在する Sitecore CMS ドメインの中から該当するユーザーを探し続けます。ユーザーが見つからない場合は、次のような警告が表示されます。



Active Directory ドメインでユーザーが見つかっても、Sitecore CMS シェル インターフェースにログインする権限がない場合 (ユーザーが sitecore¥Sitecore Client Users ロールに含まれていない場合)、ログインは拒否され、次のようなメッセージが表示されます。



すべてが問題なく進み、ユーザーがログインを許可された場合には、自動でログインが行われ、Sitecore CMS デスクトップにリダイレクトされます。

メモ

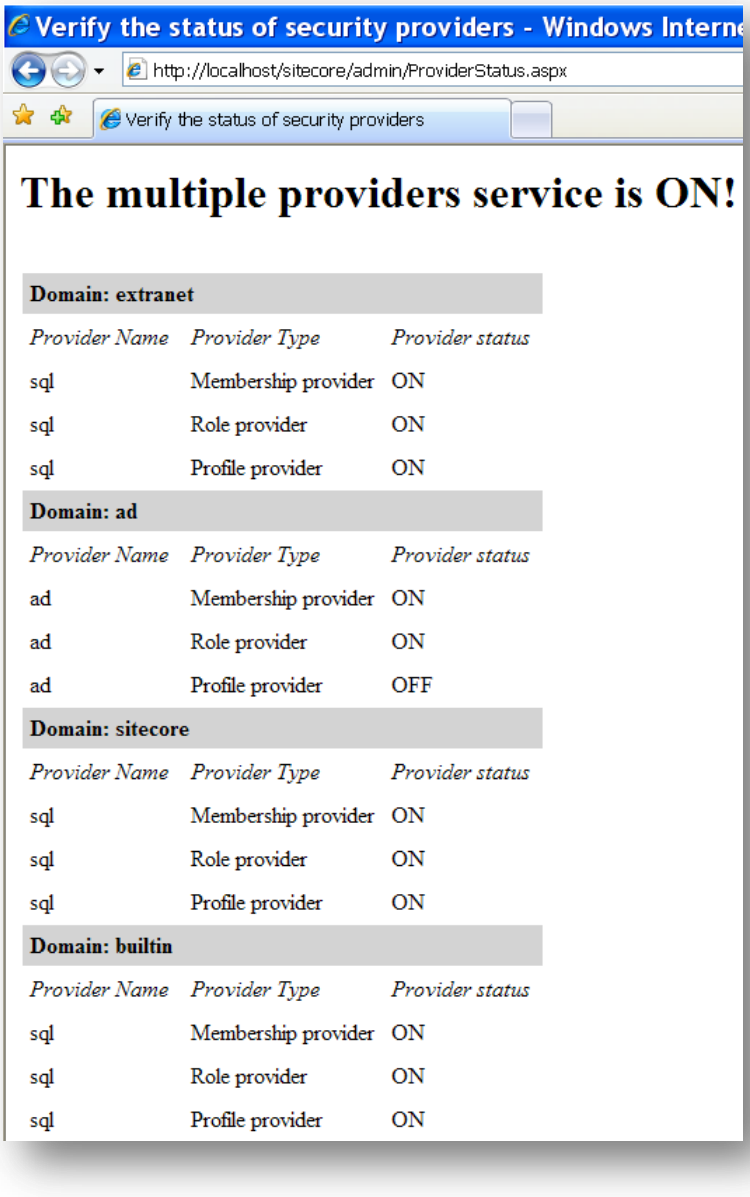
デバッグ モードを使用している場合、Sitecore CMS でメンバーとして属しているロールの一覧がまず表示されます。また、続いてログインを実行するためのボタンが有効になります。詳細については、後述のデバッグ モードの説明を参照してください。

5.2 ステータス ページ

セキュリティに関連する問題のトラブルシューティングを行うための追加オプションとして、モジュールには特別なステータス ページが用意されています。このページは次の URL で開くことができます。

```
http://[yoursite]/sitecore/admin/ProviderStatus.aspx
```

次のようなページが表示されます。



このページでは、ドメインとセキュリティ プロバイダーに関する基本的な情報を確認できます。各ドメインと、それに対応するプロバイダーの一覧が表示されています。また、各プロバイダーのステータス情報の概要が次のように表示されています。

- ステータスが ON の場合、プロバイダーは動作中で、要求を処理できます。
- ステータスが OFF の場合、プロバイダーが単純な要求を拒否したため、システムはこのプロバイダーが正常な状態ではないと認識しています。

発生した問題によっては、このページを必ずしも表示できない場合もあります。プロバイダーの設定にエラーがあると、アプリケーション全体が正常に起動できないこともあります。しかし、Active Directory モジュールの設定やセキュリティ プロバイダーの定義の全般に関するトラブルシューティングを行うときには、このページが最初のステップとなります。OFF と表示されたプロバイダーがあるときには、そのプロバイダーは動作しておらず、設定の修正が必要です。トラブルシューティングの次のステップは、ログ ファイルの調査です。

デベロッパー メモ

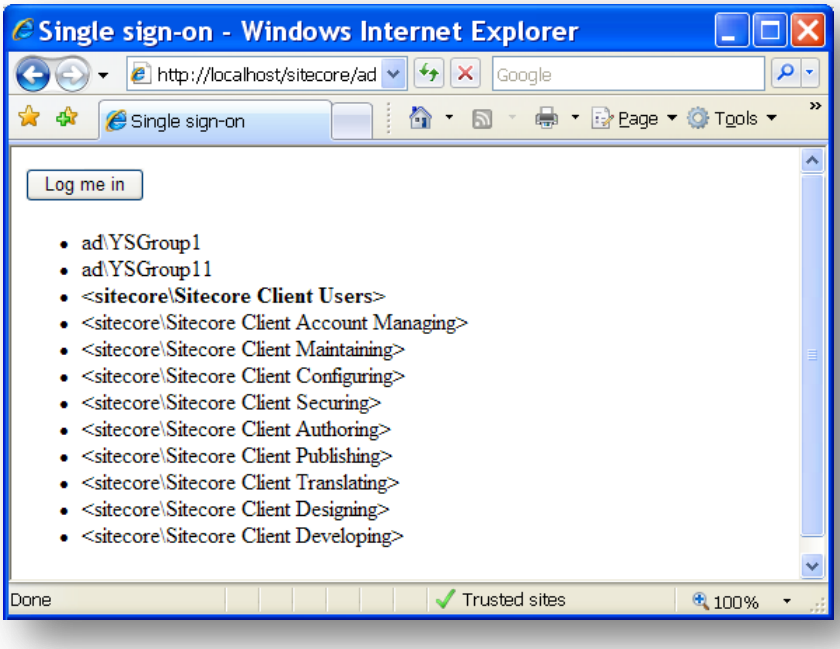
ステータス ページでは、対象のプロバイダーに対し、有効な入力パラメーターを必要としない簡単なメソッド呼び出しを行うことで、プロバイダーが動作しているかどうかを判断しています。たとえば、メンバーシップ プロバイダーの場合は GetAllUsers() メソッドを呼び出します。メソッドが例外をスローした場合、ステータスは自動で OFF に設定されます。

5.3 デバッグ モード

Active Directory モジュールには、「デバッグ モード」も用意されています。これは、ログ ファイルに詳細情報が記録され、ログイン ページに表示されるという特別なモードです。システムによっては、このような手法を詳細ロギングと呼んでいるものもあります。デバッグ モードを使用すると、管理者が詳細なログ ファイルを調査して、潜んでいる問題を自ら特定するのに便利です。また、テクニカル サポートにも非常に役立ちます。エラーの種類と場所を十分に特定できる情報が詳細ログに記録されているからです。

デバッグ モードを有効にするには、`/App_Config/Include/ldap.config` ファイルを開き、`LDAP.Debug` の設定に移動して、その値を `true` に設定します。この設定はデフォルトでは `false` です。プラグ可能な .config ファイルに加えた変更は直ちに適用されるため、次にこのモジュールが呼び出されたときには、それまでよりはるかに多くの情報が Sitecore CMS のログ ファイルに記録されます。

`LDAP.Debug` の設定はモジュール全体に適用されます。しかし、シングル サインオン機能に対してのみこのモードを有効にするためのオプションもあります。それには、ログイン ページの URL にクエリ文字列パラメーター `?debug=true` を追加します。デバッグ モードでログインするときには、アカウントに関するメンバーシップ情報がまず表示されます。この情報には、ユーザーが属する直接および間接のロールが含まれます。また、ログインの権限があるユーザーの場合には [`Log me in`] ボタンも表示され、このボタンをクリックするとログインできます。



5.4 複数ドメインへの接続

Active Directory モジュールと Sitecore セキュリティ モデルでは、複数の AD ドメインへの接続を、必要に応じていくつでも確立できます。たとえば、本社の幹部と支社のデベロッパーを 1 つの Sitecore CMS に取り込むことができます。これを実現するには、web.config ファイルでプロバイダーの追加セットを次のように設定する必要があります。

- 新しい AD ドメインへの接続文字列を追加します。
- メンバーシップ プロバイダー定義を追加します。
- ロール プロバイダー定義を追加します。
- プロファイル プロバイダー定義を追加します (ユーザー プロファイルを共有する場合)。
- 新しい Sitecore CMS ドメインを追加し、新しい一連のプロバイダーに対応付けます。

追加のセキュリティ プロバイダー設定の詳細については、『CMS のロー レベルのセキュリティとカスタム プロバイダー』の記事を参照してください。

5.5 キャッシュの設定

このモジュールでは、一部の情報をキャッシュすることでパフォーマンスを向上しています。キャッシュの設定は App_Config/include/ldap.config ファイルの次の項目で行います。

- `LDAP.Caching.UserCache` - ユーザー情報のキャッシュ サイズを指定します。
- `LDAP.Caching.MemberOfCache` - memberOf の情報のキャッシュ サイズを指定します。
- `LDAP.Caching.MembersCache` - members の情報のキャッシュ サイズを指定します。

5.6 LDAP.config のその他の設定

`/App_Config/Include/ldap.config` ファイルには、その他に次のような設定があります。

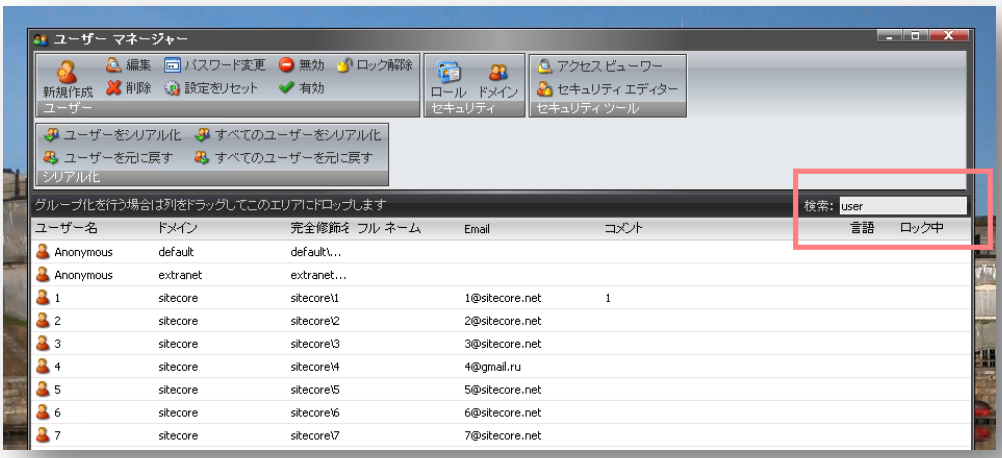
- LDAP.EnableSorting - 並べ替えを有効にするかどうかを定義します。デフォルト値は false です。

注意: Windows Server 2008 では並べ替えは動作しません。

- LDAP.SortKey - AD ユーザーの並べ替えに使用する AD 属性の名前を定義します。この設定は AD のパフォーマンスに影響します。AD でこのフィールドの値の種類が多いほど、要求されたユーザーを AD サーバーで並べ替える処理に時間がかかります。デフォルト値は codePage です。

- LDAP.SizeLimit - 検索パターン "*" に対して AD が返すユーザーの最大数。つまり、ユーザー マネージャーが表示するユーザーの数は、AD ドメインごとの LDAP.SizeLimit の値以下となります。この設定はパフォーマンス向上のために追加されました。デフォルト値は 1000 です。検索条件を絞り込むことで、目的のユーザーを見つけることができます。

- LDAP.FindSizeLimit – 他の検索パターンに対して AD が返すユーザーの最大数。つまり、ユーザーが検索操作を実行している場合、ユーザー マネージャーが表示するユーザーの数は、AD ドメインごとの LDAP.FindSizeLimit の値以下となります。この設定はパフォーマンス向上のために追加されました。デフォルト値は 100 です。



- LDAP.SettingsPropertyValueFactory - デフォルトでは、ユーザー プロファイルの AD プロパティで使用できる型は、boolean、unicode string、および integer です。必要な場合は、その他の AD プロパティの型を使用可能にするクラスを実装できます。

- LDAP.ReconnectPeriod - 通知用接続が切れた場合に、モジュールが接続を回復する時間を定義します（最新のキャッシュ データを保持するために、モジュールは AD サーバーから変更についての通知を受けます）。

- LDAP.NotificationTimeOut - 通知用接続のタイムアウトを定義します。
- LDAP.DeleteScope - モジュールによる AD オブジェクトの削除が、AD ツリー全体に対して可能か、それとも接続文字列の組織単位 (1 レベル) の配下のみ可能かを定義します。

5.7 Active Directory の変更通知

このモジュールでは、DirectoryNotificationControl (http://msdn.microsoft.com/en-us/library/system.directoryservices.protocols.directorynotificationcontrol.aspx) を使用して、Active Directory ドメイン サービスでオブジェクトが変更されたときに通知を受け取っています。

AD の変更をすべて Sitecore アプリケーションからのみ行う場合は、この機能を無効にできます。

web.config ファイルで、AD のロール プロバイダーおよびメンバーシップ プロバイダーすべてに対し、次のように useNotification="false" 属性を設定します。

```
                <add name="ad"
                     type="LightLDAP.SitecoreADMembershipProvider"
                     connectionStringName="ManagersConnString"
                     applicationName="sitecore"
                     minRequiredPasswordLength="1"
                     minRequiredNonalphanumericCharacters="0"
                     requiresQuestionAndAnswer="false"
                     requiresUniqueEmail="false"
                     connectionUsername="[put the username here]"
                     connectionPassword="[put the password here]"
                     connectionProtection="Secure"
                     attributeMapUsername="sAMAccountName"
                     enableSearchMethods="true"
                    useNotification="false"
                    />


<add name="ad" type="LightLDAP.SitecoreADRoleProvider"
connectionStringName="ManagersConnString"
     applicationName="sitecore" username="[put the username here]"
     password="[put the password here]" useNotification="false"/>
```

5.8 カスタム フィルター

AD サーバーに対するすべての要求に適用するカスタム フィルターを配置できます。これはプロバイダー レベルで設定できます。

```
 <add name="ad"
type="LightLDAP.SitecoreADMembershipProvider"
connectionStringName="ManagersConnString"
applicationName="sitecore"
minRequiredPasswordLength="1"
minRequiredNonalphanumericCharacters="0"
requiresQuestionAndAnswer="false"
requiresUniqueEmail="false"
connectionUsername="user"
connectionPassword="12345"
attributeMapUsername="sAMAccountName"
enableSearchMethods="true"
customFilter="(memberOf=cn=test role 1,OU=CRM,DC=VM)"
/>
```

フィルターの構文については、次に示すページの解説を参照してください。

http://msdn.microsoft.com/en-us/library/ms675768%28VS.85%29.aspx

カスタム フィルターを使用すると、複数の AD コンテナー (OU) からのすべてのユーザーおよびロールを単一のドメインにプラグインできます。ユーザーおよびロールは、共通の属性を持つか、共通のロールのメンバーである必要があります。次の例では、mydc ドメイン コントローラーから、"test role" のメンバーであるすべてのユーザーおよびロールを取得します。test role は Users 組織単位の下に配置されています。

customFilter="(memberOf=cn=test role,OU=Users,DC=mydc)"

customFilter 属性は、メンバーシップ、ロール、およびプロファイル プロバイダーに対して有効です。

注意: 共通の接続文字列を使用するメンバーシップ、ロール、およびプロファイル プロバイダーは、同じカスタム フィルターを使用する必要があります。

5.9 新規 AD エンティティのパイプラインの作成

カスタム フィルターを使用している場合に、Sitecore から新規ユーザーおよびロールを作成すると、それらはカスタム フィルターに一致せず、したがって Sitecore に表示されません。

これを修正するには、ldap.config ファイルでパイプラインを 2 つ使用します。initializeAdUserEntry と initializeAdRoleEntry です。

```
              <initializeAdUserEntry>
                <!--
                Use the processor if all new user should have a predefiled value in a property.
                The PropertyName parameter defines the name of the property.
                The DefaultValue parameter defines the default value of the property.
                -->
                <!--
                <processor type="LightLDAP.Pipelines.InitializeAdEntry.SetPropertyValue,
LightLDAP">
                  <PropertyName desc="AD property name ">type the property name
here</PropertyName>
                  <DefaultValue desc="AD property name ">type the default property value
here</DefaultValue>
                </processor>
                -->
                <!--
                  Use the processor if all new roles should be a member of the predefined role.
                  The RoleName parameter defines the name of the main role.
                -->
                <!--
                <processor type="LightLDAP.Pipelines.InitializeAdEntry.AddToRole, LightLDAP">
                  <RoleName desc="AD group">type role name here</RoleName>
                </processor>
                -->
                <processor type="LightLDAP.Pipelines.InitializeAdEntry.CommitChanges,
LightLDAP"/>
              </initializeAdUserEntry>
              <initializeAdRoleEntry>
                <!--
                Use the processor if all new user should have a predefiled value in a property.
                The PropertyName parameter defines the name of the property.
                The DefaultValue parameter defines the default value of the property.
                -->
                <!--
                <processor type="LightLDAP.Pipelines.InitializeAdEntry.SetPropertyValue,
LightLDAP">
                  <PropertyName desc="AD property name ">type the property name
here</PropertyName>
                  <DefaultValue desc="AD property name ">type the default property value
here</DefaultValue>
                </processor>
                -->
                <!--
                  Use the processor if all new roles should be a member of the predefined role.
                  The RoleName parameter defines the name of the main role.
                -->
                <!--
                <processor type="LightLDAP.Pipelines.InitializeAdEntry.AddToRole, LightLDAP">
                  <RoleName desc="AD group">type role name here</RoleName>
                </processor>
                -->
                <processor type="LightLDAP.Pipelines.InitializeAdEntry.CommitChanges,
LightLDAP"/>
              </initializeAdRoleEntry>
```

LightLDAP.Pipelines.InitializeAdEntry.SetPropertyValue では、ユーザーまたはロールのプロパティを所定の値で初期化します。

LightLDAP.Pipelines.InitializeAdEntry.AddToRole では、ユーザーまたはロールをメインのロールに追加します。

5.10 ネストされたグループ (間接メンバーシップ)

Sitecore の Active Directory モジュールでは、Active Directory ドメインの内部のメンバーシップを適用することによって、間接メンバーシップに対応しています。たとえば、John というユーザーがいるとします。このユーザーは Professional Service グループのメンバーで、さらにこのグループは Solution Department という親グループのメンバーであるものとします。この場合、John が Sitecore にログインできるようにするには、Solution Department グループを sitecore¥Sitecore Client Users デフォルトロールに追加する必要があります。さらに、それと共に、間接メンバーシップ機能を有効にする必要があります。それには、`/App_Config/Include/ldap.config` ファイルを開き、`LDAP.IndirectMembership` の値を true に設定します。

メモ

間接メンバーシップのオプションはログイン処理に適用されますが、Sitecore CMS セキュリティ ツールでは、このようなメンバーシップに該当するユーザーや、間接メンバーシップを実装したロールに該当するユーザーが完全には表示されません。技術面では、ロールプロバイダーの IsUserInRole メソッドは間接メンバーシップを認識していますが、その他のメソッドは認識していません。この部分に関してモジュールを拡張することは、Sitecore CMS に完全な Active Directory マネージャー アプリケーションを装備するのと同じことであり、Active Directory モジュールの対象範囲からは外れます。

5.11 AD オブジェクトに最低限必要なプロパティ

AD ユーザーには次のプロパティが必須です。

securityIdentifier
userPrincipalName
sAMAccountName
comment
whenCreated
mail
pwdLastSet
UserAccountControl
msDSUserAccountControlComputed
cn
DN
objectCategory
objectClass
isdeleted
lastknownparent
lockoutTime
primaryGroupID
pwdLastSet
tokenGroups
usnchanged
usncreated

AD グループには次のプロパティが必須です。
sAMAccountName
cn
primaryGroupToken
whenCreated
usncreated
usnchanged

Chapter 6

質問と回答

この章では、よく寄せられる質問とその回答を紹介します。

6.1 モジュールの動作に関する質問

このセクションでは、モジュールの正常な動作に関する質問を示します。

Q: Sitecore CMS から Active Directory ドメインにユーザーを作成しようとしていますが、ユーザーを作成できないと表示されます。必須フィールドはすべて入力しましたが、うまくいきません。なぜでしょうか。

A: 考えられる理由の 1 つは、そのユーザーが既に存在するということです。該当するユーザーがユーザー マネージャーに表示されていない場合には、Active Directory ドメイン全体ではなく、単一の組織単位のみを Sitecore CMS に取り込んでいる可能性が考えられます。その場合、別の組織単位に同じユーザーが存在しているものと推測されます。モジュールでユーザーを作成するときには、ドメイン全体で一意のユーザー名かどうかが検証されるという点に注意してください。

Q: Sitecore CMS で Active Directory ドメインにユーザーを作成するときに、コメント フィールドには値を指定していません。しかし、作成されたユーザーを見ると、"ここにコメントを入力してください" という文字列が入っています。なぜ自動的に値が設定されるのでしょうか。これを回避する方法はありますか。

A: 同じ現象は、ユーザーの更新時にコメント フィールドを空白にした場合にも起こります。Sitecore CMS の Active Directory プロバイダーは Microsoft のデフォルト Active Directory プロバイダーを基盤としており、そこで、ユーザー情報の更新時にコメントを空白としないよう定められています。このため、空白のままにしたときにはデフォルト値が設定されます。ここには独自の値をいつでも設定できます。

Q: ユーザーを作成したところ、役職と部署が "未定義" となりました。なぜですか。

A: これは、プロバイダーの定義要素の requiresQuestionAndAnswer 属性を true に設定しているためです。この場合、パスワードの質問と回答を AD の属性にマッピングする追加の属性も配置しておく必要があります。たとえば、質問と回答を、役職と部署の属性にそれぞれマッピングしたとします。ユーザーを作成したとき、パスワードの質問と回答を必須に設定すると、これらのフィールドを空や null のままにすることはできません。そこで、これらのフィールドが "未定義" に設定されます。この動作を回避するには、requiresQuestionAndAnswer 属性を false に設定します。

Chapter 7

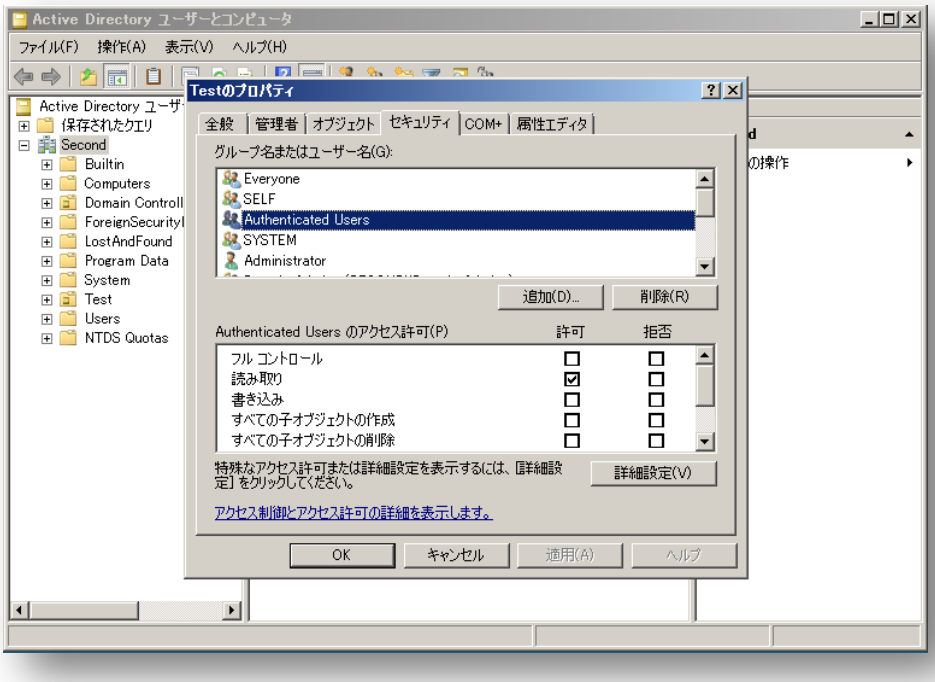
その他の情報

この章では、その他の有用な情報を紹介します。

7.1 必要なユーザー権限

このモジュールは、AD サーバーとのやり取りに資格情報を使用します。"書き込み" のアクセス権は必ずしも必要ありません。

組織単位の [プロパティ] ダイアログを表示して、必要な権限を設定します。



次のいずれかのアクセス レベルを使用して、設定を変更できます。

- 読み取り専用
- 限定的読み書き
- パスワードの変更
- 完全な読み書き

7.1.1 読み取り専用

このアクセス レベルでは以下が可能です。

- ユーザー/ロールの読み取り

- プロファイルのプロパティの読み取り

最低限必要な権限は次のとおりです。

- 内容の一覧表示
- すべてのプロパティの読み取り

7.1.2 限定的読み書き

このアクセス レベルでは、読み取り専用の操作に加えて、以下が可能です。

- プロファイルのプロパティの変更
- パスワード操作
- 電子メールの変更
- AD ロールへの AD ユーザーの追加

最低限必要な権限は次のとおりです。

- 内容の一覧表示
- すべてのプロパティの読み取り
- すべてのプロパティの書き込み

7.1.3 パスワードの変更

このアクセス レベルでは以下の権限が追加で必要です。

- すべてのプロパティの読み取り
- パスワードの変更
- パスワードのリセット (パスワードのリセット操作用)

また、AD コンテナー (Authenticated Users ロール) に権限を追加する必要があります。

- 内容の一覧表示
- すべてのプロパティの読み取り

重要:

いずれかの権限が設定されていない場合、次の例外が表示されます。
例外の詳細: System.DirectoryServices.DirectoryServicesCOMException: サーバーにそのようなオブジェクトはありません。

7.1.4 完全な読み書き

このアクセス レベルでは、限定的読み書きとパスワード変更の操作に加えて、以下が可能です。

- ユーザー/ロールの作成
- ユーザー/ロールの削除

最低限必要な権限は次のとおりです。

- 内容の一覧表示
- すべてのプロパティの読み取り
- すべてのプロパティの書き込み
- グループ オブジェクトの作成
- グループ オブジェクトの削除
- ユーザー オブジェクトの作成
- ユーザー オブジェクトの削除
- すべての拡張権限

7.2 インストールされるエンティティ

このモジュール パッケージに含まれるのはファイルのみです。アイテムやセキュリティ エンティティは含まれていません。一覧を以下に示します。

- /bin/LightLDAP.dll (モジュールのメイン アセンブリ)
- /bin/LightLDAPClient.dll (モジュールのクライアント アセンブリ)
- /App_Config/Include/ldap.config (モジュールのプラグ可能な設定ファイル)
- /sitecore/admin/LDAPLogin.aspx (シングル サインオン機能のログイン ページ)
- /sitecore/admin/ProviderStatus.aspx (プロバイダーのステータス情報ページ)

7.3 FAQ

このセクションでは、よく寄せられる質問を紹介します。

1. **質問:** ユーザーの名前を変更したところ、セキュリティの割り当てが直ちに失われました。しかし、元の名前に戻すと、セキュリティの割り当ても元に戻りました。なぜでしょうか。
   回答: この動作は、.NET のセキュリティでのユーザー名の扱い方によるものです。完全修飾ユーザー名は一意識別子の役割を果たします。Sitecore CMS ではアイテムのセキュリティ設定の格納にこの名前を使用しているため、ユーザー名を変更すると、ユーザーを新規作成した場合と同様の状態になります。通常、セキュリティ割り当てがある場合には、ユーザー名は変更しないことをお勧めします。
2. **質問:** Active Directory から取得したプロファイルのプロパティにはどのような方法でアクセスできますか。
   回答: 他のプロファイルのプロパティと同様に、次のようにしてアクセスできます。
   `user.Profile["property_name"] = "property_value";`
   上のコードは、ユーザーが `Sitecore.Security.Accounts.User` クラスのオブジェクトであると想定しています。
3. **質問:** Active Directory のグループ属性の一部を Sitecore のロールに反映したいと考えています。可能でしょうか。
   回答: この方法は、Active Directory モジュールでも Sitecore CMS でもサポートされていません。Sitecore のセキュリティは .NET のセキュリティ モデルを基盤としており、そのエンジンでは、ロールに対してある種のプロファイルを設定するオプションが用意されていないからです。

7.4 デベロッパー メモ

7.4.1 ユーザー数が 1,000,000 以上の AD でのタイムアウト警告の可能性

AD のユーザー数が 1,000,000 以上の場合、ユーザーの検索時にタイムアウト警告が発生する可能性があります。

回避方法: メンバーシップ定義に serverPageTimeLimit 属性を次のように追加します。

```
<add name="ad"
     type="LightLDAP.SitecoreADMembershipProvider"
     connectionStringName="ManagersConnString"
     applicationName="sitecore"
     minRequiredPasswordLength="1"
     minRequiredNonalphanumericCharacters="0"
     requiresQuestionAndAnswer="false"
     requiresUniqueEmail="false"
     connectionUsername="[put the username here]"
     connectionPassword="[put the password here]"
     connectionProtection="Secure"
     attributeMapUsername="sAMAccountName"
     enableSearchMethods="true"
    serverPageTimeLimit ="5"
    />
```

この属性は、サーバーが個別ページの結果を検索するときの時間制限を示します。

デフォルト値は -1 秒です。この場合、AD はすべてのユーザーを分析するまで検索を続けます。

7.4.2 Windows 2008 での並べ替え

LDAP.EnableSorting を true に設定している場合、ユーザー マネージャーで次のエラーが表示されます。

"サーバーは要求された重大な拡張子をサポートしていません。"

Windows 2008 では並べ替えを無効にする必要があります。