LDAP サーバでの AAA の設定

この章では、AAA で使用される LDAP サーバを設定する方法について説明します。次の項目を取り上げます。

- 「LDAP および ASA に関する情報」（P.36-1）
- 「LDAP サーバのライセンス要件」（P.36-4）
- 「注意事項と制約事項」（P.36-4）
- 「LDAP サーバの設定」（P.36-5）
- 「LDAP サーバによる認証および許可のテスト」（P.36-9）
- 「LDAP サーバのモニタリング」（P.36-10）
- 「LDAP サーバの機能履歴」（P.36-10）

LDAP および ASA に関する情報

ASA はほとんどの LDAPv3 ディレクトリ サーバと互換性があり、それには次のものが含まれます。

- Sun Microsystems JAVA System Directory Server（現在は Oracle Directory Server Enterprise Edition の一部、旧名 Sun ONE Directory Server）
- Microsoft Active Directory
- Novell
- OpenLDAP

デフォルトでは、ASA によって Microsoft Active Directory、Sun LDAP、Novell、OpenLDAP、または汎用 LDAPv3 ディレクトリ サーバに接続しているかどうかが自動検出されます。ただし、LDAP サーバ タイプの自動検出による決定が失敗した場合は、手動で設定できます。

LDAP サーバ ガイドライン

LDAP サーバを設定する場合、次の点に注意してください。

- Sun ディレクトリ サーバにアクセスするように ASA で設定されている Distinguished Name（DN; 認定者名）は、そのサーバのデフォルト パスワード ポリシーにアクセスできる必要があります。DN として、ディレクトリ管理者、またはディレクトリ管理者権限を持つユーザを使用することを推奨します。または、デフォルト パスワード ポリシーに ACL を設定できます。
- Microsoft Active Directory および Sun サーバでのパスワード管理をイネーブルにするために LDAP over SSL を設定する必要があります。

- ASA では、Novell、OpenLDAP、およびその他の LDAPv3 ディレクトリ サーバを使用したパスワード管理はサポートされません。
- VPN 3000 コンセントレータと ASA/PIX 7.0 ソフトウェアでは、認証作業に Cisco LDAP スキーマが必要でした。バージョン 7.1.x 以降では、ASA は、ネイティブ LDAP スキーマを使用して認証および許可を行うため、Cisco スキーマは必要なくなりました。

LDAP での認証方法

認証中、ASA は、ユーザの LDAP サーバへのクライアント プロキシとして機能し、プレーン テキストまたは Simple Authentication and Security Layer（SASL）プロトコルのいずれかを使って LDAP サーバに対する認証を行います。デフォルトで、ASA は、通常はユーザ名とパスワードである認証パラメータを LDAP サーバにプレーン テキストで渡します。

ASA では、次の SASL メカニズムをサポートしています。次に、強度の低い順番に示します。

- Digest-MD5：ASA は、ユーザ名とパスワードから計算した MD5 値を使用して LDAP サーバに応答します。
- Kerberos：ASA は、GSSAPI Kerberos メカニズムを使用して、ユーザ名とレルムを送信することで LDAP サーバに応答します。

ASA と LDAP サーバは、これらの SASL メカニズムの任意の組み合わせをサポートします。複数のメカニズムを設定した場合、ASA ではサーバに設定されている SASL メカニズムのリストが取得され、認証メカニズムは ASA とサーバの両方に設定されているメカニズムのなかで最も強力なものに設定されます。たとえば、LDAP サーバと ASA の両方がこれら両方のメカニズムをサポートしている場合、ASA は、強力な方の Kerberos メカニズムを選択します。

ユーザ LDAP 認証が成功すると、LDAP サーバは認証されたユーザの属性を返します。VPN 認証の場合、通常これらの属性には、VPN セッションに適用される許可データが含まれます。この場合、LDAP の使用により、認証と許可を 1 ステップで実行できます。

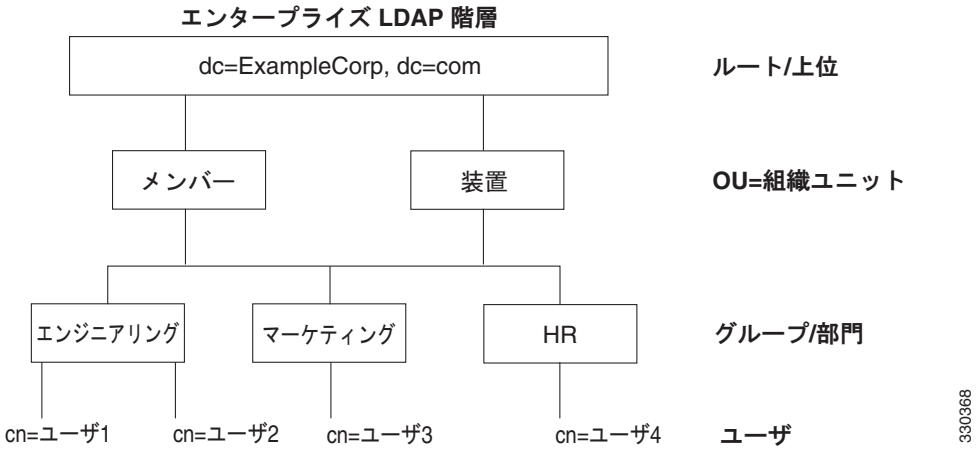
（注）　LDAP プロトコルの詳細については、RFC 1777、2251、および 2849 を参照してください。

LDAP の階層について

LDAP コンフィギュレーションは、組織の論理階層が反映されたものにする必要があります。たとえば、Example Corporation という企業の従業員 Employee1 を例に考えてみます。Employee1 は Engineering グループに従事しています。この企業の LDAP 階層は 1 つ以上のレベルを持つことができます。たとえば、シングルレベル階層をセットアップします。この中で、Employee1 は Example Corporation のメンバーであると見なされます。あるいは、マルチレベル階層をセットアップします。この中で、Employee1 は Engineering 部門のメンバーであると見なされ、この部門は People という名称の組織ユニットのメンバーであり、この組織ユニットは Example Corporation のメンバーです。マルチレベル階層の例については、図 36-1 を参照してください。

マルチレベル階層の方が詳細ですが、検索結果が速く返されるのはシングルレベル階層の方です。

図 36-1　マルチレベルの LDAP 階層



LDAP 階層の検索

ASA では、LDAP 階層内での検索を調整できます。ASA に次の 3 種類のフィールドを設定すると、LDAP 階層での検索開始場所とその範囲、および検索する情報のタイプを定義できます。これらのフィールドは、ユーザの権限が含まれている部分だけを検索するように階層の検索を限定します。

- LDAP Base DN では、サーバが ASA から許可要求を受信したときに LDAP 階層内のどの場所からユーザ情報の検索を開始するかを定義します。
- Search Scope では、LDAP 階層の検索範囲を定義します。この指定では、LDAP Base DN よりもかなり下位のレベルまで検索します。サーバによる検索を直下の 1 レベルだけにするか、サブツリー全体を検索するかを選択できます。シングルレベルの検索の方が高速ですが、サブツリー検索の方が広範囲に検索できます。
- Naming Attribute では、LDAP サーバのエントリを一意に識別する RDN を定義します。一般的な名前属性には、cn（一般名）、sAMAccountName、および userPrincipalName を含めることができます。

図 36-1 に、Example Corporation の LDAP 階層の例を示します。この階層が指定されると、複数の方法で検索を定義できます。表 36-1 に、2 つの検索コンフィギュレーションの例を示します。

最初のコンフィギュレーションの例では、Employee1 が IPSec トンネルを確立するときに LDAP 許可が必要であるため、ASA から LDAP サーバに検索要求が送信され、この中で Employee1 を Engineering グループの中で検索することが指定されます。この検索は短時間でできます。

2 番目のコンフィギュレーションの例では、ASA から送信される検索要求の中で、Employee1 を Example Corporation 全体の中で検索することが指定されています。この検索には時間がかかります。

表 36-1　検索コンフィギュレーションの例

No.	LDAP Base DN	検索範囲	名前属性	結果
1	group= Engineering,ou=People,dc=ExampleCorporation, dc=com	1 レベル	cn=Employee1	検索が高速
2	dc=ExampleCorporation,dc=com	サブツリー	cn=Employee1	検索に時間がかかる

LDAP サーバへのバインディングについて

ASA は、ログイン DN とログイン パスワードを使用して、LDAP サーバとの信頼（バインド）を築きます。Microsoft Active Directory の読み取り専用操作（認証、許可、グループ検索など）を行うとき、ASA では特権の低いログイン DN でバインドできます。たとえば、ログイン DN には、AD の「Member Of」の指定が Domain Users の一部であるユーザを指定することができます。VPN のパスワード管理操作では、ログイン DN にはより高い特権が必要となり、AD の Account Operators グループの一部を指定する必要があります。

次に、ログイン DN の例を示します。

```
cn=Binduser1,ou=Admins,ou=Users,dc=company_A,dc=com
```

ASA は次の認証方式をサポートしています。

- 暗号化されていないパスワードを使用したポート 389 での簡易 LDAP 認証
- ポート 636 でのセキュアな LDAP（LDAP-S）
- Simple Authentication and Security Layer（SASL）MD5
- SASL Kerberos

ASA は匿名認証をサポートしていません。

（注）　LDAP クライアントとしての ASA は、匿名のバインドや要求の送信をサポートしていません。

LDAP サーバのライセンス要件

モデル	ライセンス要件
すべてのモデル	基本ライセンス

注意事項と制約事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

IPv6 のガイドライン

IPv6 をサポートします。

LDAP サーバの設定

この項では、次のトピックについて取り上げます。

- 「LDAP サーバを設定するためのタスク フロー」（P.36-5）
- 「LDAP 属性マップの設定」（P.36-5）
- 「LDAP サーバ グループの設定」（P.36-7）
- 「LDAP サーバのグループへの追加」（P.36-8）

LDAP サーバを設定するためのタスク フロー

ステップ 1　LDAP サーバ グループを追加します。「LDAP サーバ グループの設定」（P.36-7）を参照してください。

ステップ 2　サーバをグループに追加し、サーバ パラメータを設定します。「LDAP サーバのグループへの追加」（P.36-8）を参照してください。

ステップ 3　LDAP 属性マップを設定します。「LDAP 属性マップの設定」（P.36-5）を参照してください。LDAP サーバを LDAP サーバ グループに追加する前に、属性マップを追加する必要があります。

LDAP 属性マップの設定

ASA では、次の目的での認証のために LDAP ディレクトリを使用できます。

- VPN リモート アクセス ユーザ
- ファイアウォール ネットワークのアクセス / カットスルー プロキシ セッション
- ACL、ブックマーク リスト、DNS または WINS 設定、セッション タイマーなどのポリシーの権限（または許可属性と呼ばれる）の設定。
- ローカル グループ ポリシーのキー属性の設定

ASA は、LDAP 属性マップを使用して、ネイティブ LDAP ユーザ属性をシスコ ASA 属性に変換します。それらの属性マップを LDAP サーバにバインドしたり、削除したりすることができます。また、属性マップを表示または消去することもできます。

ガイドライン

LDAP 属性マップは複数値属性をサポートしません。たとえば、あるユーザが複数の AD グループのメンバで、LDAP 属性マップが複数のグループと一致する場合、選択される値は一致するエントリのアルファベット順に基づくものです。

属性マッピング機能を適切に使用するには、LDAP 属性の名前と値およびユーザ定義の属性の名前と値を理解する必要があります。

頻繁にマッピングされる LDAP 属性の名前と、一般にマッピングされるユーザ定義の属性のタイプは次のとおりです。

- IETF-Radius-Class（ASA バージョン 8.2 以降における Group_Policy）：ディレクトリ部門またはユーザ グループ（たとえば、Microsoft Active Directory memberOf）属性値に基づいてグループ ポリシーを設定します。ASDM バージョン 6.2/ASA バージョン 8.2 以降では、IETF-Radius-Class 属性の代わりにグループ ポリシー属性が使用されます。

- IETF-Radius-Filter-Id：VPN クライアント、IPSec、SSL に対するアクセス コントロール リスト（ACL）に適用されます。
- IETF-Radius-Framed-IP-Address：VPN リモート アクセス クライアント、IPSec、および SSL にスタティック IP アドレスを割り当てます。
- Banner1：VPN リモート アクセス ユーザのログイン時にテキスト バナーを表示します。
- Tunneling-Protocols：アクセス タイプに基づいて、VPN リモート アクセス セッションを許可または拒否します。

（注） 1 つの LDAP 属性マップに、1 つ以上の属性を含めることができます。特定の LADP サーバからは、1 つの LDAP 属性のみをマップすることができます。

LDAP 機能をマップするには、次の手順を実行します。

手順の詳細

ステップ 1 ローカル ユーザの場合は [Configuration] > [Remote Access VPN] > [AAA Local Users] > [LDAP Attribute Map] の順に、その他の全ユーザの場合は [Configuration] > [Device Management] > [Users/AAA] > [LDAP Attribute Map] の順に選択して、[Add] をクリックします。

[Map Name] タブが表示された状態で [Add LDAP Attribute Map] ダイアログボックスが開きます。

ステップ 2 [Name] フィールドに、この属性マップの名前を作成します。

ステップ 3 [LDAP Attribute Name] フィールドに、マッピングする LDAP 属性の名前を入力します。

ステップ 4 [Cisco Attribute Name] ドロップダウン リストから、Cisco 属性を選択します。

ステップ 5 [Add] をクリックします。

ステップ 6 属性がマップされます。さらに属性をマップする場合は、ステップ 1 ～ 5 を繰り返します。

ステップ 7 マップされている Cisco 属性の新しい値に LDAP 属性の値をマップする場合は、[Map Value] タブをクリックします。

ステップ 8 [Add] をクリックします。

[Add Mapping of Attribute Name] ダイアログボックスが表示されます。

ステップ 9 ドロップダウン リストから LDAP 属性を選択します。

ステップ 10 [LDAP Attribute Value] フィールドに、LDAP サーバから返されると予想されるこの LDAP 属性の値を入力します。

ステップ 11 [Cisco Attribute Value] フィールドに、この LDAP 属性が以前の LDAP 属性値を含める場合に、Cisco 属性で使用する値を入力します。

ステップ 12 [Add] をクリックします。

値がマップされます。

ステップ 13 さらに値をマップする場合は、ステップ 8 ～ 12 を繰り返します。

ステップ 14 [OK] をクリックして [Map Value] タブに戻り、再度 [OK] をクリックしてダイアログボックスを閉じます。

ステップ 15 [LDAP Attribute Map] ペインで [Apply] をクリックして、実行コンフィギュレーションにマップする値を保存します。

LDAP サーバ グループの設定

認証、許可、アカウンティングに外部 LDAP サーバを使用する場合は、まず少なくとも 1 つの LDAP サーバ グループを作成して、各グループに 1 つ以上のサーバを追加する必要があります。LDAP サーバ グループは名前で識別されます。各サーバ グループは、各サーバ タイプによって異なります。

ガイドライン

- シングルモードの場合は最大 100 台の LDAP サーバ グループを使用でき、マルチモードの場合は各コンテキストで最大 4 台の LDAP サーバ グループを使用できます。
- 各グループには、シングル モードで最大 16 台、マルチ モードで最大 4 台の LDAP サーバを含めることができます。
- ユーザがログインすると、コンフィギュレーション内で指定されている最初のサーバから順に、サーバが応答するまで LDAP サーバが 1 つずつアクセスされます。グループ内のすべてのサーバが使用できない場合、ASA は、ローカル データベースがフォールバック方式として設定されていると、ローカル データベースに接続しようとします（管理認証および許可限定）。フォールバック方式として設定されていない場合、ASA は引き続き LDAP サーバにアクセスしようとします。

手順の詳細

次に、LDAP サーバ グループを作成し、このグループに LDAP サーバを追加する方法を示します。

ステップ 1　[Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups]、または VPN ユーザの場合は [Configuration] > [Remote Access VPN] > [AAA/Local Users] > [AAA Server Groups] の順に選択します。

ステップ 2　[AAA Server Groups] 領域で、[Add] をクリックします。

[Add AAA Server Group] ダイアログボックスが表示されます。

ステップ 3　[AAA Server Group] フィールドで、この AAA サーバ グループの名前を指定します。

ステップ 4　[Protocol] ドロップダウン リストから、LDAP サーバのタイプを選択します。

ステップ 5　[Reactivation Mode] フィールドで、目的のモードに対応するオプション ボタン（[Depletion] または [Timed]）をクリックします。

[Depletion] モードの場合、障害が発生したサーバは、グループ内のサーバがすべて非アクティブになったときに限り、再アクティブ化されます。

Timed モードでは、障害が発生したサーバは 30 秒の停止時間の後で再アクティブ化されます。

a.　[Depletion] 再アクティブ化モードを選択した場合は、[Dead Time] フィールドに時間間隔を入力します。

[Dead Time] には、グループ内の最後のサーバがディセーブルになってから、すべてのサーバが再びイネーブルになるまでの時間間隔を分単位で指定します。

ステップ 6　[Max Failed Attempts] フィールドに、サーバに接続するための試行の許容失敗回数を指定します。

このオプションで設定するのは、応答のないサーバを非アクティブと宣言するまでに許可される接続試行の失敗回数です。

ステップ 7　[OK] をクリックします。

[Add AAA Server Group] ダイアログボックスが閉じ、新しいサーバ グループが [AAA Server Groups] テーブルに追加されます。

ステップ 8　変更内容を保存する場合は、[AAA Server Groups] ダイアログボックスで、[Apply] をクリックします。

変更内容が実行コンフィギュレーションに保存されます。

LDAP サーバのグループへの追加

ステップ 1　[Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups]、または VPN ユーザの場合は [Configuration] > [Remote Access VPN] > [AAA/Local Users] > [AAA Server Groups] の順に選択し、[AAA Server Groups] 領域で、サーバを追加するサーバ グループを選択します。

ステップ 2　選択されたグループのサーバ リストの横にある [Add] をクリックします。

サーバ グループに対応する [Add AAA Server] ダイアログボックスが表示されます。

ステップ 3　[Interface Name] ドロップダウン リストから、LDAP サーバに接続するインターフェイスの名前を選択します。

ステップ 4　[Server Name or IP Address] フィールドに、LDAP サーバのサーバ名または IP アドレスを追加します。

ステップ 5　[Timeout] フィールドで、タイムアウト値を入力します。デフォルト値をそのまま使用することもできます。[Timeout] フィールドには、バックアップ サーバへ要求を送信した ASA が、プライマリ サーバからの応答を待機する時間を秒単位で指定します。

ステップ 6　認証および承認の領域の LDAP パラメータで、次のフィールドを設定します。

- [Enable LDAP over SSL]（セキュア LDAP または LDAP-S とも呼ばれる）: ASA と LDAP サーバの間のセキュアな通信に SSL を使用する場合にオンにします。

（注）　SASL プロトコルを設定しない場合は、SSL を使用して LDAP 通信のセキュリティを確保することを強く推奨します。

- [Server Port]：ASA から LDAP サーバへアクセスする際、単純認証（セキュアでない認証）に使用される TCP ポート番号 389 またはセキュアな認証（LDAP-S）に使用される TCP ポート番号 636 を指定します。LDAP サーバはすべて、認証および許可をサポートしています。Microsoft AD サーバおよび Sun LDAP サーバに限っては、さらに、LDAP-S を必要とする VPN リモート アクセス パスワード管理機能もサポートしています。
- [Server Type]：ドロップダウン リストから LDAP サーバ タイプを指定します。使用できるオプションは、次のとおりです。
  - Detect Automatically/Use Generic Type
  - Microsoft
  - Novell
  - OpenLDAP
  - Sun（現在では Oracle Directory Server Enterprise Edition の一部）
- **Base DN**：ベース識別名、または LDAP 要求を受け取ったサーバで検索が開始される LDAP 階層内の位置を指定します（例：OU=people, dc=cisco, dc=com）。
- **Scope**：ドロップダウン リストからの認証要求を受信する場合に、LDAP 階層内でサーバの実行が必要な検索範囲を指定します。次のオプションを使用できます。

  - [One Level]：ベース DN の 1 レベル下だけを検索します。このオプションを選択すると、検索の実行時間が短縮されます。
  - [All Levels]：ベース DN の下にあるすべてのレベル（つまりサブツリー階層全体）が検索対象となります。このオプションを選択すると、検索の実行に時間がかかります。
- [Naming Attribute（s）]：LDAP サーバのエントリを一意に識別する Relative Distinguished Name 属性を入力します。共通の名前付き属性は、Common Name（CN）、sAMAccountName、userPrincipalName、および User ID（uid）です。
- [Login DN and Login Password]：ASA は、LDAP サーバとの信頼（バインド）を確立するために、ログイン DN とログイン パスワードを使用します。ログイン DN のユーザ アカウントのパスワードをログイン パスワードとして指定します。入力した文字はアスタリスクに置き換えられます。
- [LDAP Attribute Map]：この LDAP サーバで使用するために作成された属性マップの 1 つを選択します。これらの属性マップは、LDAP 属性名をシスコの属性名と値にマップします。
- [SASL MD5 authentication]：ASA と LDAP サーバの間の通信を認証するための SASL の MD5 メカニズムをイネーブルにします。
- [SASL Kerberos authentication]：ASA と LDAP サーバの間のセキュアな認証通信のための SASL の Kerberos メカニズムをイネーブルにします。このオプションを有効にするためには、Kerberos サーバを定義しておく必要があります。
- [LDAP Parameters for Group Search]：この領域のフィールドは、ASA が AD グループを要求する方法を設定します。
  - [Group Base DN]：この DN により、LDAP 階層内で AD グループ（つまり、memberOf 列挙のリスト）の検索を開始する位置が指定されます。このフィールドの設定を行わない場合、ASA では、AD グループの取得にベース DN が使用されます。ASDM では、取得した AD グループのリストに基づいて、ダイナミック アクセス ポリシーの AAA 選択基準が定義されます。詳細については、「**show ad-groups** コマンド」を参照してください。
  - [Group Search Timeout]：使用できるグループについてのクエリーに対して AD サーバから応答があるまでの最長待機時間を指定します。

ステップ 7　[OK] をクリックします。

[Add AAA Server] ダイアログボックスが閉じ、AAA サーバが AAA サーバ グループに追加されます。

ステップ 8　[AAA Server Groups] ペインで [Apply] をクリックし、変更内容を実行コンフィギュレーションに保存します。

VPN 設定ガイドで、トンネル グループが記載されている場所を確認します。ASDM の手順を確認します。可能な場合は移動します。

LDAP サーバによる認証および許可のテスト

ASA において LDAP サーバへのアクセスやユーザの認証および許可が実行できるかどうかを判定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] ペインで、サーバが常駐するサーバ グループを選択します。

ステップ 2　[Selected Group] 領域のの [Servers] から、テストするサーバをクリックします。

ステップ 3　[Test] をクリックします。

選択したサーバに対応する [Test AAA Server] ダイアログボックスが表示されます。

ステップ 4　実行するテストのタイプ（[Authentication] または [Authorization]）をクリックします。

ステップ 5　ユーザ名を入力します。

ステップ 6　認証をテストする場合は、ユーザ名のパスワードを入力します。

ステップ 7　[OK] をクリックします。

認証または許可のテスト メッセージが ASA からサーバへ送信されます。テストが失敗した場合は、ASDM によりエラー メッセージが表示されます。

LDAP サーバのモニタリング

LDAP サーバをモニタするには、次の手順を実行します。

ステップ 1　ASDM で、[Monitoring] > [Properties] > [AAA Servers] を選択します。

ステップ 2　LDAP サーバの状態を更新するには、[Update Server Statistics] でクリックして選択します。

ドロップダウン リストで選択された LDAP サーバを含む [Update AAA Server Status] ダイアログボックスが表示されます。

ステップ 3　[OK] をクリックします。

ステップ 4　現在表示されている統計情報を更新するには、[Clear Server Statistics] をクリックします。

LDAP サーバの機能履歴

表 36-2 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 36-2　AAA サーバの機能履歴

機能名	プラットフォーム リリース	機能情報
AAA の LDAP サーバ	7.0(1)	LDAP サーバの AAA のサポートと LDAP サーバの設定方法について説明します。 次の画面が導入されました。 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] [Configuration] > [Remote Access VPN] > [AAA Local Users] > [LDAP Attribute Map]