

AAA の LDAP サーバー

この章では、AAA で使用される LDAP サーバーの設定方法について説明します。

- LDAP および ASA について （1 ページ）
- AAA の LDAP サーバーのガイドライン （6 ページ）
- AAA の LDAP サーバーの設定 （6 ページ）
- LDAP サーバーによる認証および許可のテスト （11 ページ）
- AAA の LDAP サーバーのモニタリング （12 ページ）
- AAA の LDAP サーバーの履歴 （12 ページ）

LDAP および ASA について

ASA はほとんどの LDAPv3 ディレクトリサーバーと互換性があり、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 サーバーに接続しているかどうかが自動検出されます。ただし、LDAP サーバー 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 での認証方法

認証中、ASA は、ユーザーの LDAP サーバーへのクライアント 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 サーバーに対する認証を行います。デフォルトで、ASA は、通常はユーザー名とパスワードである認証パラメータを LDAP サーバーにプレーン 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、ユーザー名とレルムを送信することで LDAP サーバーに応答します。

ASA と LDAP サーバーは、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 ではサーバーに設定されている SASL メカニズムのリストが取得され、認証メカニズムは ASA とサーバー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 サーバーと 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。

ユーザー LDAP 認証が成功すると、LDAP サーバーは認証されたユーザーの属性を返します。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認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。

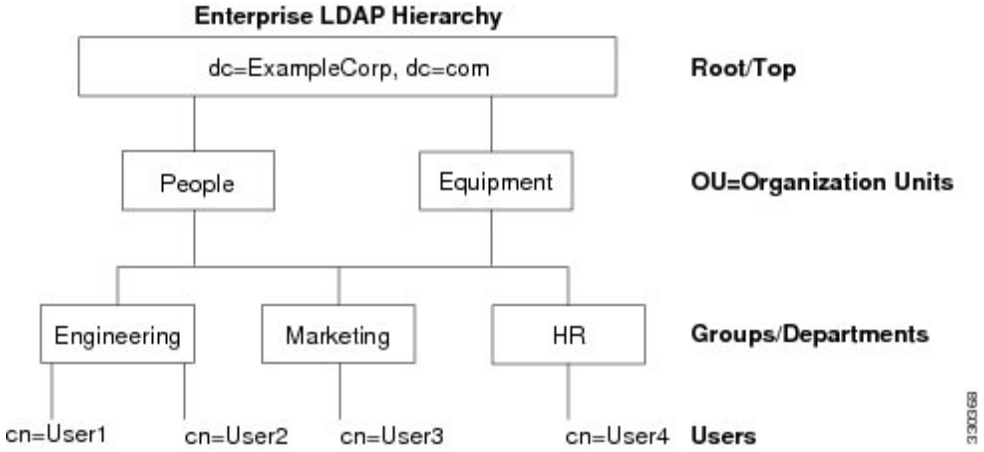
（注） LDAP プロトコルの詳細については、RFC 1777、2251、および 2849 を参照してください。

LDAP 階層

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、次の図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 *1* : マルチレベルの *LDAP* 階層



LDAP 階層の検索

ASA 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、ユーザー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、サーバーが ASA から認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ー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。サーバー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 サーバー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。

次の図に、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。次の表に、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 認可が必要であるため、ASA から LDAP サーバー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 *1*：検索コンフィギュレーションの例

番号	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 サーバーへのバインド

ASA は、ログイン DN とログイン パスワードを使用して、LDAP サーバーとの信頼（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、Login 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、Login 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。

（注） Firepower 1000/2100 デバイスに LDAP 認証を構成する場合、バインドパスワードにバックスラッシュ（「\」）を使用しないでください。パスワードにバックスラッシュが含まれていると、LDAP バインドプロセスが失敗し、外部認証が失敗します。

次に、Login 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 属性マップ

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 ユーザー
- 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 ユーザー属性を ASA 属性に変換します。それらの属性マップを LDAP サーバーにバインドしたり、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。

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、あるユーザーが複数の 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ー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ー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ー 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 group-policy 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 ユーザー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 サーバーからは、1 つの LDAP 属性のみをマップすることができます。

AAA の LDAP サーバーのガイドライン

この項では、AAA の LDAP サーバーを設定する前に確認する必要のあるガイドラインおよび制限事項について説明します。

IPv6

AAA サーバーは、IPv4 または IPv6 アドレスを使用できます。

その他のガイドライン

- Sunディレクトリ サーバーにアクセスするためにASAに設定されているDNが、サーバー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ー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サーバー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 は、Novell、OpenLDAP およびその他の LDAPv3 ディレクトリ サーバーによるパスワード管理をサポートしません。
- バージョン 7.1（x）以降、ASA はネイティブ LDAP スキーマを使用して認証および認可を行うため、Cisco スキーマは必要なくなりました。
- シングル モードで最大 200 個のサーバー グループ、またはマルチ モードでコンテキストごとに 4 つのサーバー グループを持つことができます。
- 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 8 台のサーバーを含めることができます。
- ユーザーがログインすると、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ーから順に、サーバーが応答するまでLDAPサーバーが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ー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（管理認証および認可限定）。フォールバック メソッドとして設定されていない場合、ASA は LDAP サーバーに引き続きアクセスしようとします。

AAA の LDAP サーバーの設定

この項では、AAA に LDAP サーバーを設定する方法について説明します。

手順

ステップ 1 LDAP 属性マップを設定します。LDAP 属性マップの設定 （7 ページ）を参照してください。

ステップ 2 LDAP サーバー グループを追加します。LDAP サーバー グループの設定 （8 ページ）を参照してください。

ステップ 3 サーバーをグループに追加し、サーバーパラメータを設定します。LDAP サーバーのサーバーグループへの追加 （9 ページ）を参照してください。

LDAP 属性マップの設定

LDAP 属性マップを設定するには、次の手順を実行します。

手順

ステップ 1 ローカル ユーザーの場合は **[Configuration]** > **[Remote Access VPN]** > **[AAA Local Users]** > **[LDAP Attribute Map]** の順に選択し、その他すべてのユーザーの場合は **[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 [Mapping of Attribute Name] ダイアログボックスが開きます。

ステップ 2 この属性マップの名前を作成します。

ステップ 3 マッピングする LDAP 属性の 1 つの名前を追加します。

ステップ 4 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 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 [Mapping of Attribute Value] タブをクリックして、マップされた Cisco 属性の新しい値に LDAP 属性の値をマッピングします。

ステップ 8 [Add] をクリックして、[Add Mapping of Attribute Value] ダイアログボックスを表示します。

ステップ 9 LDAP サーバー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 10 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 11 [Add] をクリックします。

ステップ 12 さらに属性値をマップする場合は、ステップ 8 ～ 11 を繰り返します。

ステップ 13 [OK] を 2 回クリックして、各ダイアログボックスを閉じます。

ステップ 14 [Apply] をクリックし、実行コンフィギュレーションの設定を保存します。

LDAP サーバー グループの設定

LDAP サーバー グループを作成して設定し、LDAP サーバーをそのグループに追加するには、次の手順を実行します。

始める前に

LDAP サーバーを LDAP サーバー 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。

手順

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

ステップ 2 [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 サーバー グループの名前を入力します。

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

ステップ 5 使用する再アクティブ化モードのオプション 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ーは、グループ内のサーバー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ーは 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。

デッド時間には、グループ内の最後のサーバーがディセーブルになってから、すべてのサーバー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。デッドタイムは、ローカルデータベースへのフォールバックを設定した場合にのみ適用されます。認証は、デッドタイムが経過するまでローカルで試行されます。

ステップ 6 サーバーで許容できる AAA トランザクションの失敗の最大回数を追加します。

これは、応答のないサーバー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、新しいサーバー グループが AAA サーバー グループに追加されます。

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

LDAP サーバーのサーバー グループへの追加

LDAP サーバーをサーバー グループに追加するには、次の手順を実行します。

手順

ステップ 1 次のいずれかを選択します。

- VPN ユーザーの場合は、[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [AAA Server Groups]。
- [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups]

ステップ 2 サーバーを追加するサーバー グループを選択し、**Add** をクリックします。

選択したサーバー 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 LDAP サーバー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 LDAP サーバーのサーバー名または IP アドレスを追加します。

ステップ 5 タイムアウト値を追加するか、デフォルト値をそのまま使用します。[Timeout] フィールドには、バックアップ サーバーへ要求を送信する前に、ASA がプライマリ サーバー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 [LDAP Parameters for authentication/authorization] 領域で、次の設定を行います。

- [Enable LDAP over SSL]（セキュア LDAP または LDAP-S とも呼ばれる）：ASA と LDAP サーバーの間のセキュアな通信に SSL を使用する場合に、このチェックボックスをオンにします。

（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。

- [参照ID名（Reference Identity Name）]：LDAP サーバー ID を検証するための参照 ID 名を入力します。
- [Server Port]：ASA から LDAP サーバーへアクセスする際、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 サーバーはすべて、認証および認可をサポートしています。Microsoft AD サーバーおよび Sun LDAP サーバーに限っては、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 サーバー 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（DN）、または LDAP 要求を受け取ったサーバー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 階層内でサーバー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 つ下のレベルだけ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 サーバーのエントリを一意に識別する相対識別名属性を入力します。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 サーバーとの信頼（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 のユーザー 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。
- [LDAP Attribute Map]：この LDAP サーバー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 サーバー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 サーバー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 サーバー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 サーバーから応答があるまでの最長待機時間を指定します。

- [LDAP SSL クライアント証明書/クライアント ID 証明書トラストポイント（LDAP SSL Client Certificate/Client Identity Certificate Trustpoint）]：LDAP over SSL を有効にする場合、認証のために ASA クライアントから LDAP サーバーに提示する必要がある証明書トラストポイントを選択できます。トラストポイントは、クライアント証明書を認証するように LDAP サーバーを設定する場合に必要です。証明書を設定しないと、ASA は LDAP サーバーから要求されたときに証明書を提示しません。LDAP サーバーがピア証明書を要求するように設定されている場合、セキュア LDAP セッションが完了せず、認証/許可要求が失敗します。

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 サーバーが AAA サーバー グループに追加されます。

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

LDAP サーバーによる認証および許可のテスト

ASA が LDAP サーバーに接続してユーザーを認証または承認できるかどうかを判別するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[AAA Server Groups]** の順に選択します。

ステップ 2 サーバーが存在するサーバー グループを選択します。

ステップ 3 テストするサーバーを選択します。

ステップ 4 [Test] をクリックします。

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

ステップ 5 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 6 ユーザー名を入力します。

ステップ 7 認証をテストする場合は、ユーザー名のパスワードを入力します。

ステップ 8 [OK] をクリックします。

認証または認可のテスト メッセージが ASA からサーバーへ送信されます。テストが失敗した場合は、エラー メッセージが表示されます。

AAA の LDAP サーバーのモニタリング

AAA の LDAP サーバーのモニタリングについては、次のコマンドを参照してください。

- **[Monitoring] > [Properties] > [AAA Servers]**

  このペインは、設定された AAA サーバーの統計情報を表示します。

- **[Tools] > [Command Line Interface]**

  このペインでは、さまざまな非インタラクティブ コマンドを発行し、結果を表示することができます。

AAA の LDAP サーバーの履歴

表 *2 : AAA* サーバーの履歴

機能名	プラットフォームリリース	説明
AAA の LDAP サーバー	7.0(1)	LDAP サーバーの AAA のサポートと LDAP サーバー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]。
AAA 向けの IPv6 アドレス LDAP サーバー	9.7(1)	AAA サーバーに IPv4 または IPv6 アドレスを使用できるようになりました。

機能名	プラットフォームリリース	説明
グループごとの AAA サーバー グループとサーバーの制限が増えました。	9.13(1)	より多くの AAA サーバー グループを設定できます。シングルコンテキストモードでは、200 個の AAA サーバーグループを設定できます（以前の制限は 100）。マルチコンテキストモードでは、8 個設定できます（以前の制限は 4）。 さらに、マルチコンテキストモードでは、グループごとに 8 台のサーバーを設定できます（以前の制限はグループごとに 4 台のサーバー）。シングル コンテキスト モードのグループごとの制限の 16 は変更されていません。 これらの新しい制限を受け入れるために、AAA 画面が変更されました。
相互l LDAPS 認証。	9.18(1)	ASA が認証のために証明書を要求したときに LDAP サーバーに提示するように ASA のクライアント証明書を設定できます。この機能は、LDAP over SSL を使用する場合に適用されます。LDAP サーバーがピア証明書を要求するように設定されている場合、セキュア LDAP セッションが完了せず、認証/許可要求が失敗します。 次の画面が変更されました。[設定（Configuration）] > [デバイス管理（Device Management）] > [ユーザー/AAA（Users/AAA）] [] > [AAAサーバーグループ（AAA Server Groups）] > [LDAPサーバーの追加/編集（Add/Edit LDAP server）]

AAA の LDAP サーバーの履歴

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。