CHAPTER 11

LDAP との統合

概要

企業の LDAP ディレクトリ（例：Microsoft Active Directory、SunONE Directory Server、または OpenLDAP ディレクトリなど）のエンド ユーザのパスワードおよび電子メール エイリアスを管理する場合、LDAP ディレクトリを使用して次のユーザを認証することができます。

- Cisco IronPort スパム隔離にアクセスするエンド ユーザおよび管理ユーザ。

  ユーザが Cisco IronPort スパム隔離の Web UI にログインする場合、LDAP サーバはログイン名とパスワードを検証し、AsyncOS は対応する電子メール エイリアスのリストを取得します。そのユーザの電子メール エイリアスのいずれかに送信された隔離メッセージは、アプライアンスが書き換えない限り Cisco IronPort スパム隔離で表示できます。

  「Cisco IronPort スパム隔離と連携させるための LDAP の設定」（P.11-1）を参照してください。

- 外部認証が有効に設定されている場合、シスコのコンテンツセキュリティ管理アプライアンスに署名する管理ユーザ。

  「LDAP を使用した管理ユーザの外部認証の設定」（P.11-14）を参照してください。

Cisco IronPort スパム隔離と連携させるための LDAP の設定

シスコ コンテンツ セキュリティ アプライアンスを LDAP ディレクトリと連携させるには、以下の手順に従って、受け入れ、ルーティング、エイリアシング、およびマスカレードを設定する必要があります。

手順

ステップ 1　**LDAP サーバ プロファイルを設定します。**

サーバ プロファイルの内容は、AsyncOS から LDAP サーバに接続するための、次のような情報です。

- サーバ名およびポート
- ベース DN
- サーバをバインディングするための認証要件

サーバ プロファイルの設定方法の詳細については、「LDAP サーバ プロファイルの作成」（P.11-2）を参照してください。

LDAP サーバ プロファイルを作成するときに、AsyncOS からの接続先となる LDAP サーバを複数設定できます。詳細については、「AsyncOS を複数の LDAP サーバと連携させるための設定」（P.11-11）を参照してください。

ステップ 2　**LDAP クエリーを設定します。**

LDAP サーバ プロファイル用に生成されたデフォルトのスパム隔離クエリーを使用するか、または実際に使用する LDAP の実装とスキーマに合わせて自分のクエリーを作成することができます。次に、スパム通知、および隔離へのエンドユーザ アクセス検証に使用するアクティブ クエリーを指定します。

クエリーの詳細については、「LDAP クエリーの設定」（P.11-4）を参照してください。

ステップ 3　**Cisco IronPort スパム隔離に対して、LDAP エンドユーザ アクセスおよびスパム通知をイネーブルにします。**

Cisco IronPort スパム隔離に対するエンドユーザ アクセスをイネーブルにして、エンドユーザが隔離メッセージを表示したり管理したりできるようにします。ユーザが複数の通知を受信しないように、スパム通知のエイリアス統合をイネーブルにすることもできます。

詳細については、「中央集中型スパム隔離の設定」（P.7-2）を参照してください。

LDAP サーバ プロファイルの作成

LDAP ディレクトリを使用するように AsyncOS を設定した場合は、LDAP サーバに関する情報を保存するために LDAP サーバ プロファイルを作成します。

手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [LDAP] を選択します。

ステップ 2　[LDAP サーバ プロファイルを追加（Add LDAP Server Profile）] をクリックします。

ステップ 3　[LDAP サーバ プロファイル名（LDAP Server Profile Name）] テキスト フィールドにサーバ プロファイルの名前を入力します。

ステップ 4　[ホスト名（Host Name(s)）] テキスト フィールドに、LDAP サーバのホスト名を入力します。

複数のホスト名を入力すると、LDAP サーバのフェールオーバーやロード バランシングができるようになります。複数のエントリを指定する場合は、カンマで区切ります。詳細については、「AsyncOS を複数の LDAP サーバと連携させるための設定」（P.11-11）を参照してください。

ステップ 5　認証方式を選択します。匿名認証を使用することも、ユーザ名とパスワードを指定することもできます。

（注）　レポート上のクライアント IP アドレスではなくクライアント ユーザ ID を表示するには、LDAP 認証を設定する必要があります。LDAP 認証を使用しない場合、システムでは IP アドレスによるユーザの参照のみができます。[パスワードを使用（Use Password）] オプション ボタンを選択して、ユーザ名とパスワードを入力します。[内部ユーザのサマリー（Internal Users Summary）] ページにユーザ名が表示されます。

ステップ 6　LDAP サーバ タイプを、[Active Directory]、[OpenLDAP]、または [不明またはそれ以外（Unknown or Other）] から選択します。

ステップ 7　ポート番号を入力します。

デフォルト ポートは 3268 です。これは、複数台のサーバ環境でグローバル カタログへのアクセスをイネーブルにする Active Directory 用のデフォルト ポートです。

ステップ 8　LDAP サーバのベース DN（識別名）を入力します。

ユーザ名とパスワードで認証を行う場合、ユーザ名にはパスワードが含まれているエントリの完全 DN が含まれている必要があります。たとえば、電子メール アドレスが joe@example.com というユーザがマーケティング グループのユーザだとします。このユーザ用のエントリは、次のエントリのようになります。

```
uid=joe, ou=marketing, dc=example dc=com
```

ステップ 9　[拡張（Advanced）] で、LDAP サーバとの通信に SSL を使用するかどうかを選択します。

ステップ 10　キャッシュ存続可能時間を入力します。この値は、キャッシュを保持する時間の長さです。

ステップ 11　保持するキャッシュ エントリの最大数を入力します。

ステップ 12　同時接続の最大数を入力します。

ロード バランシングのために LDAP サーバ プロファイルを設定する場合、これらの接続はリストで指定された LDAP サーバ間で配分されます。たとえば、同時接続数を 10 と設定し、3 台のサーバを使用して接続のロード バランシングを行う場合は、AsyncOS によってサーバへの接続が 10 ずつ作成され、接続の総数は 30 となります。詳細については、「ロード バランシング」（P.11-13）を参照してください。

（注）　同時接続の最大数には、LDAP クエリーに使用される LDAP 接続が含まれます。ただし、Cisco IronPort スパム隔離のための LDAP 認証をイネーブルにする場合、アプライアンスはエンド ユーザ隔離に対して 20 の追加接続を許可し、接続の総数は 30 となります。

ステップ 13　サーバへの接続をテストするために、[テスト サーバ（Test Server(s)）] ボタンをクリックします。複数の LDAP サーバを指定した場合は、すべてのサーバのテストが実行されます。テストの結果が [接続ステータス（Connection Status）] フィールドに表示されます。詳細については、「LDAP サーバのテスト」（P.11-4）を参照してください。

ステップ 14　スパム隔離クエリーを作成します。該当するチェックボックスをオンにして、フィールドに入力します。

ユーザがエンドユーザ隔離にログインするときにそのユーザを検証する、隔離エンドユーザ認証クエリーを設定できます。エンドユーザが電子メール エイリアスごとに隔離通知を受け取らないように、エイリアス統合クエリーを設定できます。これらのクエリーを使用するには、[有効なクエリとして指定する（Designate as the active query）] チェックボックスをオンにします。詳細については、「LDAP クエリーの設定」（P.11-4）を参照してください。

ステップ 15　[クエリのテスト（Test Query）] ボタンをクリックして、スパム隔離クエリーをテストします。

テスト パラメータを入力して [テストの実行（Run Test）] をクリックします。テストの結果が [接続ステータス（Connection Status）] フィールドに表示されます。クエリーの定義や属性に変更を加えた場合は、[更新（Update）] をクリックします。

（注） 空パスワードでのバインドを許可するように LDAP サーバが設定されている場合は、パスワード フィールドが空でもクエリーのテストは合格となります。

ステップ 16　変更を送信し、保存します。

Active Directory サーバ設定では、Windows 2000 で TLS 経由の認証が許可されません。これは、Active Directory の既知の問題です。Active Directory および Windows 2003 の TLS 認証は、動作します。

（注） サーバ設定の数は無制限ですが、サーバごとに、エンドユーザ認証クエリーを 1 つとエイリアス統合クエリーを 1 つだけ設定できます。

LDAP サーバのテスト

[LDAP サーバ プロファイルを追加/編集（Add/Edit LDAP Server Profile）] ページの [テスト サーバ（Test Server(s)）] ボタン（または CLI の `ldapconfig` コマンドの `test` サブコマンド）を使用して、LDAP サーバへの接続をテストします。サーバ ポートへの接続に成功したか失敗したかを示すメッセージが表示されます。複数の LDAP サーバを設定した場合は、AsyncOS によって各サーバがテストされ、結果が個別に表示されます。

LDAP クエリーの設定

次のセクションで、Cisco IronPort スパム隔離クエリーのタイプごとに、デフォルトのクエリー文字列と設定の詳細を示します。

- **スパム隔離へのエンドユーザ認証のクエリー。**詳細については、「スパム隔離へのエンドユーザ認証のクエリー」（P.11-5）を参照してください。
- **スパム隔離のエイリアス統合のクエリー。**詳細については、「スパム隔離のエイリアス統合クエリー」（P.11-7）を参照してください。

隔離でエンドユーザ アクセスまたはスパム通知の LDAP クエリーを使用するには、[有効なクエリとして指定する（Designate as the active query）] チェックボックスをオンにします。隔離アクセスを制御するエンドユーザ認証クエリーを 1 つと、スパム通知用のエイリアス統合クエリーを 1 つ指定できます。既存のアクティブ クエリーはすべてディセーブルになります。セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [LDAP] ページを選択します。アスタリスク（*）がアクティブ クエリーの横に表示されます。

ドメインベースのクエリーまたはチェーン クエリーも、アクティブなエンドユーザ アクセス クエリーまたはスパム通知クエリーとして指定できます。詳細については、「ドメインベース クエリー」（P.11-8）および「チェーン クエリー」（P.11-10）を参照してください。

（注）　[LDAP] ページの [クエリのテスト（Test Query）] ボタン（または **ldaptest** コマンド）を使用して、クエリーから返される結果が期待したとおりであることを確認します。

LDAP クエリーの構文

LDAP パス内でスペースを使用できます。引用符で囲む必要はありません。CN と DC の構文では、大文字と小文字は区別されません。

Cn=First Last,oU=user,dc=domain,DC=COM

クエリーに入力する変数名では、大文字と小文字が区別されます。また、正しく動作するためには、LDAP 実装と一致している必要があります。たとえば、プロンプトで **mailLocalAddress** と入力したときに実行されるクエリーは、**maillocaladdress** と入力したときとは異なります。

トークン

次のトークンを LDAP クエリー内で使用できます。

- {a} ユーザ名 @ ドメイン名
- {d} ドメイン
- {dn} 識別名
- {g} グループ名
- {u} ユーザ名
- {f} MAILFROM: アドレス

（注）　{f} トークンを使用できるのは、受け入れクエリーのみです。

たとえば、メールを受け入れるための Active Directory LDAP サーバに対するクエリーは、**(|(mail={a})(proxyAddresses=smtp:{a}))** になります。

（注）　作成したクエリーは、[LDAP] ページの [テスト（Test）] 機能（または **ldapconfig** コマンドの **test** サブコマンド）を使用してテストすることを強く推奨します。期待したとおりの結果が返されることを確認してから、リスナーに対して LDAP 機能をイネーブルにしてください。詳細については、「LDAP クエリーのテスト」（P.11-8）を参照してください。

スパム隔離へのエンドユーザ認証のクエリー

エンドユーザ認証のクエリーとは、ユーザが Cisco IronPort スパム隔離にログインするときにユーザを検証するためのクエリーです。トークン {u} は、ユーザを示します（ユーザのログイン名を表します）。トークン {a} は、ユーザの電子メール アドレスを示します。LDAP クエリーによって「SMTP:」が電子メール アドレスから除去されることはありません。ただし、AsyncOS はこの部分をアドレスから除去します。

サーバ タイプに基づいて、次のデフォルト クエリー文字列がエンドユーザ認証クエリーに使用されます。

- **Active Directory：**`(sAMAccountName={u})`

- **OpenLDAP：**`(uid={u})`
- [不明またはそれ以外（Unknown or Other）] :（ブランク）

デフォルトでは、プライマリ メール属性は **mail** です。独自のクエリーとメール属性を入力できます。クエリーを CLI で作成するには、**ldapconfig** コマンドの `isqauth` サブコマンドを使用します。

（注）　ユーザのログイン時に各自の電子メール アドレス全体を入力させる場合は、`(mail=smtp:{a})` というクエリー文字列を使用します。

Active Directory エンドユーザ認証の設定の例

ここでは、Active Directory サーバとエンドユーザ認証クエリーの設定の例を示します。この例では、Active Directory サーバのパスワード認証、Active Directory サーバのためのエンドユーザ認証のデフォルト クエリー文字列、`mail` および `proxyAddresses` メール属性を使用します。

表 11-1　LDAP サーバとスパム隔離へのエンドユーザ認証の設定例：Active Directory

認証方式	パスワードを使用 （検索用にバインドするための低特権のユーザを作成するか、匿名検索を設定する必要があります）
サーバ タイプ	Active Directory
ポート	3268
ベース DN	（ブランク）
接続プロトコル	（ブランク）
クエリー文字列	`(sAMAccountName={u})`
メール属性	`mail,proxyAddresses`

OpenLDAP エンドユーザ認証の設定の例

ここでは、OpenLDAP サーバとエンドユーザ認証クエリーの設定の例を示します。この例では、OpenLDAP サーバの匿名認証、OpenLDAP サーバのためのエンドユーザ認証のデフォルト クエリー文字列、`mail` および `mailLocalAddress` メール属性を使用します。

表 11-2　LDAP サーバとスパム隔離へのエンドユーザ認証の設定例：OpenLDAP

認証方式	匿名
サーバ タイプ	OpenLDAP
ポート	389
ベース DN	（ブランク）（古いスキーマでは具体的なベース DN の使用が要求されることがあります）
接続プロトコル	（ブランク）
クエリー文字列	`(uid={u})`
メール属性	`mail,mailLocalAddress`

スパム隔離のエイリアス統合クエリー

スパム通知を使用する場合は、スパム隔離のエイリアス統合クエリーを使用して電子メール エイリアスを 1 つにまとめると、受信者がエイリアスごとに隔離通知を受け取ることはなくなります。たとえば、ある受信者がメール アドレス john@example.com、jsmith@example.com、および john.smith@example.com のメールを受け取るとします。エイリアス統合を使用すると、受信者が受け取るスパム通知は 1 通だけとなります。送信先は、このユーザのエイリアスすべてに送信されるメッセージのプライマリ メール アドレスとして選択されたアドレスです。

メッセージを統合してプライマリ メール アドレスに送信するには、受信者の代替の電子メール エイリアスを検索するためのクエリーを作成してから、受信者のプライマリ メール アドレスを [メール属性（Email Attribute）] フィールドに入力します。

Active Directory サーバの場合は、デフォルトのクエリー文字列は `(|(proxyAddresses={a})(proxyAddresses=smtp:{a}))` で、デフォルトのメール属性は `mail` です。OpenLDAP サーバの場合は、デフォルトのクエリー文字列は `(mail={a})` で、デフォルトのメール属性は `mail` です。独自のクエリーとメール属性を定義することもできます。属性が複数の場合は、カンマで区切ります。入力するメール属性が複数ある場合は、最初のメール属性として、変動する可能性のある値を複数持つ属性（たとえば `proxyAddresses`）ではなく、値を 1 つだけ使用する一意の属性（たとえば `mail`）を入力することを推奨します。

クエリーを CLI で作成するには、`ldapconfig` コマンドの `isqalias` サブコマンドを使用します。

Active Directory エイリアス統合の設定の例

ここでは、Active Directory サーバとエイリアス統合クエリーの設定の例を示します。この例では、Active Directory サーバに対して匿名認証を使用し、Active Directory サーバに対するエイリアス統合用のクエリー文字列を指定し、メール属性は `mail` を使用します。

表 11-3　LDAP サーバとスパム隔離のエイリアス統合の設定例：Active Directory

認証方式	**匿名**
サーバ タイプ	Active Directory
ポート	3268
ベース DN	（ブランク）
接続プロトコル	Use SSL
クエリー文字列	(|(mail={a})(mail=smtp:{a}))
メール属性	`mail`

OpenLDAP エイリアス統合の設定の例

ここでは、OpenLDAP サーバとエイリアス統合クエリーの設定の例を示します。この例では、OpenLDAP サーバに対して匿名認証を使用し、OpenLDAP サーバに対するエイリアス統合用のクエリー文字列を指定し、メール属性は `mail` を使用します。

表 11-4　LDAP サーバとスパム隔離のエイリアス統合の設定例：OpenLDAP

認証方式	**匿名**
サーバ タイプ	OpenLDAP
ポート	389
ベース DN	（ブランク）（古いスキーマでは具体的なベース DN の使用が要求されることがあります）

表 11-4　LDAP サーバとスパム隔離のエイリアス統合の設定例：OpenLDAP （続き）

接続プロトコル	Use SSL
クエリー文字列	`(mail={a}))`
メール属性	`mail`

LDAP クエリーのテスト

[LDAP サーバ プロファイルを追加/編集（Add/Edit LDAP Server Profile）] ページの [クエリのテスト（Test Query）] ボタン（または CLI の `ldaptest` コマンド）を使用して、クエリーをテストします。AsyncOS に、クエリー接続テストの各ステージの詳細が表示されます。たとえば、最初のステージの SMTP 認証に成功したか失敗したか、バインド照合の返された結果が true か false か、などです。

`ldaptest` コマンドは、次の例のようにバッチ コマンドとして使用できます。

```
ldaptest LDAP.isqalias foo@cisco.com
```

クエリーに入力する変数名では、*大文字と小文字が区別されます*。また、正しく動作するためには、LDAP 実装と一致している必要があります。たとえば、メール属性に `mailLocalAddress` と入力すると、`maillocaladdress` と入力する場合とは異なるクエリーを実行します。

クエリーをテストするには、テスト パラメータを入力して、[テストの実行（Run Test）] をクリックします。[テスト接続（Test Connection）] フィールドに結果が表示されます。エンドユーザ認証クエリーが成功した場合、「Success: Action: match positive」という結果が表示されます。エイリアス統合クエリーの場合は、統合されたスパム通知の電子メール アドレスと共に、「Success: Action: alias consolidation」という結果が表示されます。クエリーが失敗すると、一致する LDAP レコードが見つからない、一致したレコードにメール属性が含まれていないなど、失敗の原因が表示されます。複数の LDAP サーバを使用している場合、シスコ コンテンツ セキュリティ アプライアンスは、LDAP サーバごとにクエリーをテストします。

ドメインベース クエリー

ドメインベース クエリーとは、LDAP クエリーをタイプ別にグループ化し、ドメインに関連付けたものです。複数の別の LDAP サーバが異なるドメインに関連付けられているが、エンドユーザ隔離アクセスに対し、すべての LDAP サーバでクエリーを実行する必要がある場合、ドメインベース クエリーの使用を推奨します。たとえば、Bigfish という名前の会社が Bigfish.com、Redfish.com、および Bluefish.com というドメインを所持していて、それぞれのドメインに関連する従業員用に別の LDAP サーバを管理するとします。Bigfish は、ドメインベース クエリーを使用して、3 つのドメインすべての LDAP ディレクトリに対してエンドユーザを認証することができます。

ドメインベース クエリーを使用してエンドユーザ アクセスまたは Cisco IronPort スパム隔離の通知を制御するには、次の手順を実行します。

手順

ステップ 1　ドメインベース クエリーで使用する各ドメインについて LDAP サーバ プロファイルを作成します。各サーバ プロファイルでは、ドメインベース クエリーで使用するクエリーを設定します。詳細については、「LDAP サーバ プロファイルの作成」（P.11-2）を参照してください。

ステップ 2　ドメインベース クエリーを作成します。ドメインベース クエリーを作成するときに、各サーバ プロファイルからクエリーを選択し、ドメインベース クエリーを Cisco IronPort スパム隔離のアクティブ クエリーとして指定します。クエリーの作成方法の詳細については、「ドメインベース クエリーの作成」（P.11-9）を参照してください。

ステップ 3　Cisco IronPort スパム隔離に対して、エンドユーザ アクセスまたはスパム通知をイネーブルにします。詳細については、「中央集中型スパム隔離の設定」（P.7-2）を参照してください。

ドメインベース クエリーの作成

手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [LDAP] を選択します。

ステップ 2　[LDAP] ページで、[拡張（Advanced）] をクリックします。

ステップ 3　ドメインベース クエリーの名前を入力します。

ステップ 4　クエリーのタイプを選択します。

（注）　ドメインベース クエリーを作成するときは、シングル クエリー タイプを指定します。クエリーのタイプを選択すると、該当するクエリーが LDAP サーバ プロファイルからクエリー フィールド ドロップダウン リストに含まれるようになります。

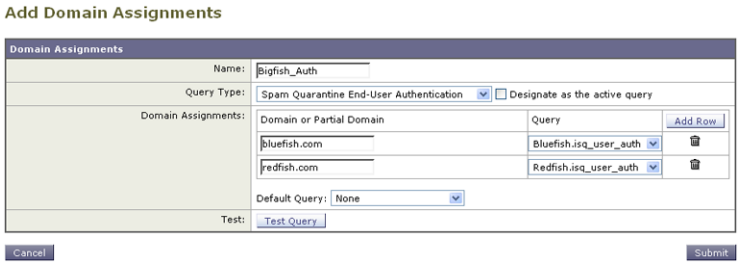
ステップ 5　[ドメイン割り当て（Domain Assignments）] フィールドに、ドメインを入力します。

ステップ 6　このドメインに関連付けるクエリーを選択します。

ステップ 7　行を追加して、ドメインベース クエリーのドメインごとにクエリーを選択します。

ステップ 8　どのクエリーにも一致しないときに実行する、デフォルトのクエリーを入力します。デフォルトのクエリーを入力しない場合は、[なし（None）] を選択します。

図 11-1　ドメインベース クエリーの例



ステップ 9　[クエリのテスト（Test Query）] ボタンをクリックし、[テスト パラメータ（Test Parameters）] フィールドにテストするユーザのログインとパスワード、または電子メール アドレスを入力して、クエリーをテストします。[接続ステータス（Connection Status）] フィールドに結果が表示されます。

ステップ 10　Cisco IronPort スパム隔離でドメインベース クエリーを使用するには、[有効なクエリとして指定する（Designate as the active query）] チェックボックスをオンにします。

（注）　ドメインベース クエリーが、指定されたクエリー タイプのアクティブ LDAP クエリーになります。たとえば、ドメインベース クエリーがエンドユーザ認証に使用されている場合は、Cisco IronPort スパム隔離のアクティブ エンドユーザ認証クエリーになります。

ステップ 11　[送信（Submit）] をクリックし、[確定する（Commit）] をクリックして変更を保存します。

（注）　同じ設定をコマンドライン インターフェイスで行うには、コマンド ライン プロンプトで、`ldapconfig` コマンドの `advanced` サブコマンドを入力します。

チェーン クエリー

チェーン クエリーは、AsyncOS が連続して実行する一連の LDAP クエリーです。AsyncOS は LDAP サーバから肯定的なレスポンスが返されると、または最後のクエリーで否定的なレスポンスが返されるか失敗するまで、シリーズ内の各クエリー、「チェーン」内の各クエリーを実行します。チェーン クエリーが役立つのは、LDAP ディレクトリ内のエントリにおいて、さまざまな属性に類似の（または同一の）値が格納されている場合です。たとえば、組織の各部門が、異なるタイプの LDAP ディレクトリを使用していることがあります。IT 部門が OpenLDAP を使用し、営業部門が Active Directory を使用しているとします。クエリーが両方のタイプの LDAP ディレクトリに対して実行されていることを確認するために、チェーン クエリーを使用できます。

チェーン クエリーを使用してエンドユーザ アクセスまたは Cisco IronPort スパム隔離の通知を制御するには、次の手順を実行します。

手順

ステップ 1　チェーン クエリーで使用するクエリーごとに 1 つずつ、LDAP サーバ プロファイルを作成します。このサーバ プロファイルのそれぞれについて、チェーン クエリーに使用するクエリーを設定します。詳細については、「LDAP サーバ プロファイルの作成」（P.11-2）を参照してください。

ステップ 2　チェーン クエリーを作成し、Cisco IronPort スパム隔離のアクティブ クエリーとして指定します。詳細については、「チェーン クエリーの作成」（P.11-10）を参照してください。

ステップ 3　Cisco IronPort スパム隔離に対して、LDAP エンドユーザ アクセスまたはスパム通知をイネーブルにします。スパム隔離の詳細については、「中央集中型スパム隔離の設定」（P.7-2）を参照してください。

チェーン クエリーの作成

ヒント　CLI から、`ldapconfig` コマンドの `advanced` サブコマンドも使用できます。

手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [LDAP] > [LDAP サーバ（LDAP Server）] を選択します。

ステップ 2　[LDAP サーバ プロファイル（LDAP Server Profiles）] ページの [拡張（Advanced）] をクリックします。

ステップ 3　[連鎖クエリを追加（Add Chained Query）] をクリックします。

ステップ 4　チェーン クエリーの名前を入力します。

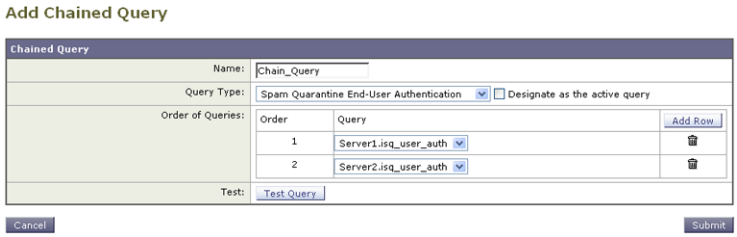
ステップ 5　クエリーのタイプを選択します。

チェーン クエリーを作成するときは、そのコンポーネントのクエリーすべてを同じクエリー タイプにします。クエリーのタイプを選択すると、該当するクエリーが LDAP からクエリー フィールド ドロップダウン リストに表示されます。

ステップ 6　チェーンの最初のクエリーを選択します。

シスコ コンテンツ セキュリティ アプライアンスによって、ここで設定した順にクエリーが実行されます。チェーン クエリーに複数のクエリーを追加する場合は、詳細なクエリーの後に広範なクエリーが続くように順序付けることを推奨します。

図 11-2　チェーン クエリーの例



ステップ 7　[クエリのテスト（Test Query）] ボタンをクリックし、[テスト パラメータ（Test Parameters）] フィールドにユーザのログインとパスワード、または電子メール アドレスを入力して、クエリーをテストします。[接続ステータス（Connection Status）] フィールドに結果が表示されます。

ステップ 8　Cisco IronPort スパム隔離でドメイン クエリーを使用するには、[有効なクエリとして指定する（Designate as the active query）] チェックボックスをオンにします。

（注）　チェーン クエリーが、指定されたクエリー タイプのアクティブ LDAP クエリーになります。たとえば、チェーン クエリーがエンドユーザ認証に使用されている場合は、Cisco IronPort スパム隔離のアクティブ エンドユーザ認証クエリーになります。

ステップ 9　変更を送信し、保存します。

（注）　同じ設定をコマンドライン インターフェイスで行うには、コマンド ライン プロンプトで、`ldapconfig` コマンドの `advanced` サブコマンドを入力します。

AsyncOS を複数の LDAP サーバと連携させるための設定

LDAP プロファイルを設定するときに、シスコ コンテンツ セキュリティ アプライアンスからの接続先となる複数の LDAP サーバをリストとして設定できます。複数の LDAP サーバを使用するには、格納されている情報、構造、使用する認証情報を同一にする必要があります。レコードを統合できる製品がサード パーティから提供されています。

次の機能を使用する場合は、冗長 LDAP サーバに接続するようにシスコ コンテンツ セキュリティ アプライアンスを設定します。

- **フェールオーバー**。シスコ コンテンツ セキュリティ アプライアンスが LDAP サーバに接続できない場合、リストで次に指定されているサーバに接続します。
- **ロード バランシング**。シスコ コンテンツ セキュリティ アプライアンスは、LDAP クエリーを実行するときに、リストで指定されている LDAP サーバの間で接続を分散します。

冗長 LDAP サーバを設定するには、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [LDAP] ページまたは CLI の `ldapconfig` コマンドを使用します。

サーバとクエリーのテスト

[LDAP サーバ プロファイルを追加 / 編集（Add/Edit LDAP Server Profile）] ページの [テスト サーバ（Test Server(s)）] ボタン（または CLI の `test` サブコマンド）を使用して、LDAP サーバへの接続をテストします。複数の LDAP サーバを使用する場合は、各サーバのテストが実行されて、各サーバの結果が個別に表示されます。各 LDAP サーバでのクエリーのテストも実行されて、結果が個別に表示されます。

フェールオーバー

LDAP サーバで確実にクエリーを解決できるようにするには、フェールオーバー用に LDAP プロファイルを設定できます。

シスコ コンテンツ セキュリティ アプライアンスアプライアンスは、LDAP サーバ リスト内の最初のサーバへの接続を、所定の時間が経過するまで試行します。アプライアンスがリスト内の最初の LDAP サーバに接続できない場合は、リスト内の次の LDAP サーバへの接続が試行されます。シスコ コンテンツ セキュリティ アプライアンスが確実にプライマリ LDAP サーバにデフォルトで接続するようにするには、そのサーバが LDAP サーバ リストの先頭に入力されていることを確認してください。

シスコ コンテンツ セキュリティ アプライアンスが 2 番目の、または後続の LDAP サーバに接続する場合、そのサーバへの接続は所定の時間が経過するまで維持されます。この時間が経過すると、アプライアンスはリスト内の最初のサーバに対して再接続を試行します。

LDAP フェールオーバーのためのシスコのコンテンツ アプライアンスの設定

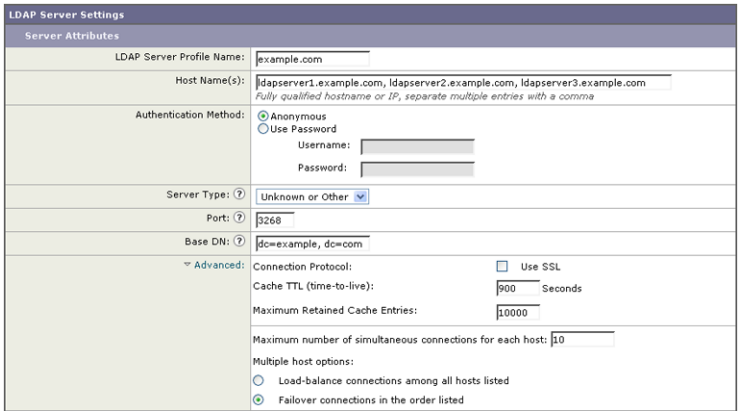
手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [LDAP] を選択します。

ステップ 2　編集する LDAP サーバ プロファイルを選択します。

次の例で、LDAP サーバ名は example.com です。

図 11-3　LDAP フェールオーバー コンフィギュレーションの例



ステップ 3　[ホスト名（Hostname）] テキスト フィールドに、LDAP サーバ（**ldapserver.example.com** など）を入力します。

ステップ 4　[各ホストの最大同時接続数（Maximum number of simultaneous connections for each host）] テキスト フィールドに、最大接続数を入力します。

この例では、最大接続数が **10** です。

ステップ 5　[一覧されている順序での接続のフェールオーバー（Failover connections in the order list）] の横にあるオプション ボタンをクリックします。

ステップ 6　その他の LDAP オプションを必要に応じて設定します。

ステップ 7　変更を送信し、保存します。

ロード バランシング

LDAP 接続をグループ内の LDAP サーバ間に分散させるには、ロード バランシングのための LDAP プロファイルを設定します。

ロード バランシングを使用した場合、シスコ コンテンツ セキュリティ アプライアンスからの接続はリスト内の LDAP サーバに分散されます。接続に失敗したときやタイムアウトしたときは、アプライアンスは使用可能な LDAP サーバを判断して、使用可能なサーバに再接続します。アプライアンスは、管理者が設定した最大同時接続数に基づいて、同時に確立する接続の数を決定します。

リストで指定された LDAP サーバの 1 つが応答しなくなった場合は、アプライアンスからの接続の負荷は残りの LDAP サーバに分散されます。

ロード バランシングのためのシスコのコンテンツ アプライアンスの設定

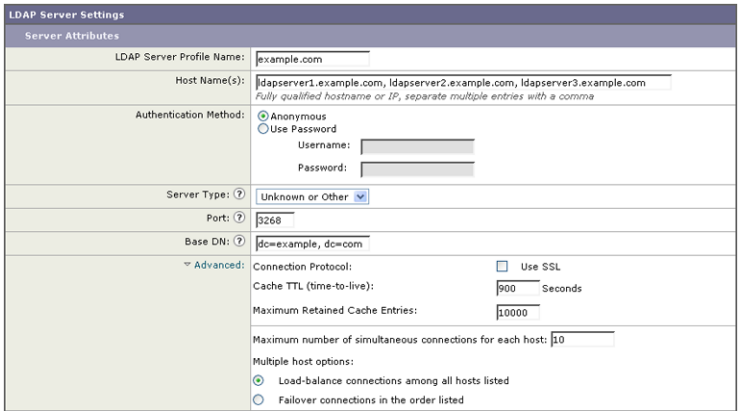
手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [LDAP] を選択します。

ステップ 2　編集する LDAP サーバ プロファイルを選択します。

次の例で、LDAP サーバ名は example.com です。

図 11-4　ロード バランシング コンフィギュレーションの例



ステップ 3　[ホスト名（Hostname）] テキスト フィールドに、LDAP サーバ（**ldapserver.example.com** など）を入力します。

ステップ 4　[各ホストの最大同時接続数（Maximum number of simultaneous connections for each host）] テキスト フィールドに、最大接続数を入力します。

この例では、最大接続数が **10** です。

ステップ 5　[すべてのホスト間での負荷分散接続（Load balance connections among all hosts）] の横にあるオプション ボタンをクリックします。

ステップ 6　その他の LDAP オプションを必要に応じて設定します。

ステップ 7　変更を送信し、保存します。

LDAP を使用した管理ユーザの外部認証の設定

ネットワーク上の LDAP ディレクトリを使用して管理ユーザを認証するようにアプライアンスを設定できます。このように設定すると、ユーザが各自の LDAP ユーザ名とパスワードを使用して、シスコ コンテンツ セキュリティ アプライアンスにログインできるようになります。

手順

ステップ 1　**LDAP サーバ プロファイルを設定します。**「LDAP サーバ プロファイルの作成」（P.11-2）を参照してください。

ステップ 2　**ユーザ アカウントを見つけるためのクエリーを作成します。**LDAP サーバ プロファイルの、[外部認証クエリ（External Authentication Queries）] セクションで、クエリーを作成して LDAP ディレクトリ内のユーザ アカウントを検索します。「管理ユーザの認証のためのユーザ アカウント クエリー」（P.11-15）を参照してください。

ステップ 3　**グループ メンバーシップ クエリーを作成します。**あるユーザがディレクトリ グループのメンバーであるかどうかを判断するクエリーを作成し、あるグループのすべてのメンバーを検索する別のクエリーを作成します。詳細ついては、「管理ユーザの認証のためのグループ メンバーシップ クエリー」（P.11-16）およびご使用の電子メール セキュリティ アプライアンスのマニュアルまたはオンライン ヘルプを参照してください。

（注）　そのページの [外部認証クエリ（External Authentication Queries）] セクションにある [テスト クエリ（Test Queries）] ボタン（または `ldaptest` コマンド）を使用して、クエリーから返される結果が期待したとおりであることを確認します。関連情報については、「LDAP クエリーのテスト」（P.11-8）を参照してください。

ステップ 4　**LDAP サーバを使用するように外部認証をセットアップします。**この LDAP サーバをユーザ認証に使用するようにアプライアンスを設定し、ユーザ ロールを LDAP ディレクトリ内のグループに割り当てます。詳細についてはの「管理ユーザの外部認証のイネーブル化」（P.11-17）および電子メール セキュリティ アプライアンスのマニュアルまたはオンライン ヘルプの「Adding Users」を参照してください。

管理ユーザの認証のためのユーザ アカウント クエリー

外部ユーザを認証するために、AsyncOS はクエリーを使用してそのユーザのレコードを LDAP ディレクトリ内で検出し、ユーザのフル ネームが格納されている属性を見つけます。管理者が選択したサーバ タイプに応じて、AsyncOS によってデフォルトのクエリーとデフォルトの属性が入力されます。アカウントが失効しているユーザは拒否するようにアプライアンスを設定することもできます。それには、RFC 2307 で規定されている属性が LDAP ユーザ レコード内で定義されている必要があります（**shadowLastChange**、**shadowMax**、および **shadowExpire**）。ユーザのレコードがあるドメイン レベルのベース DN が必要です。

表 11-5 に、AsyncOS がユーザ アカウントを Active Directory サーバ上で検索するときに使用されるデフォルトのクエリー文字列とユーザのフル ネーム属性を示します。

表 11-5　Active Directory サーバのデフォルト クエリー文字列

サーバ タイプ	Active Directory
ベース DN	（ブランク）（ユーザ レコードを見つけるには具体的なベース DN を使用する必要があります）
クエリー文字列	`(&(objectClass=user)(sAMAccountName={u}))`
ユーザのフル ネームが格納されている属性	`displayName`

表 11-6 に、AsyncOS がユーザ アカウントを OpenLDAP サーバ上で検索するときに使用されるデフォルトのクエリー文字列とユーザのフル ネーム属性を示します。

表 11-6　Open LDAP サーバのデフォルト クエリー文字列

サーバ タイプ	OpenLDAP
ベース DN	（ブランク）（ユーザ レコードを見つけるには具体的なベース DN を使用する必要があります）
クエリー文字列	`(&(objectClass=posixAccount)(uid={u}))`
ユーザのフル ネームが格納されている属性	`gecos`

管理ユーザの認証のためのグループ メンバーシップ クエリー

LDAP グループをアプライアンスにアクセスするためのユーザ ロールと関連付けることができます。

AsyncOS は、あるユーザがディレクトリ グループのメンバーであるかどうかを判断するクエリーや、あるグループのすべてのメンバーを検索する別のクエリーを使用することもできます。ディレクトリ グループ メンバーシップ内のメンバーシップによって、そのユーザのシステム内のアクセス許可が決まります。GUI の [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザ（Users）] ページ（または CLI の `userconfig`）で外部認証をイネーブルにするときに、ユーザ ロールを LDAP ディレクトリ内のグループに割り当てます。ユーザ ロールによって、そのユーザがシステム内で持つアクセス許可が決まります。外部認証されたユーザの場合は、ロールは個々のユーザではなくディレクトリ グループに割り当てられます。たとえば、IT というディレクトリ グループ内のユーザに「Administrator」というロールを割り当て、「Support」というディレクトリ グループのユーザに「Help Desk User」というロールを割り当てます。

ユーザが異なるユーザ ロールを持つ複数の LDAP グループに属する場合は、AsyncOS がユーザに最も制限されたロールの権限を割り当てます。たとえば、ユーザが Operator 権限を持つグループと Help Desk User 権限を持つグループに属する場合、AsyncOS はユーザに Help Desk User ロールの権限を割り当てます。

グループ メンバーシップを問い合わせるための LDAP プロファイルを設定するときに、グループ レコードが格納されているディレクトリ レベルのベース DN を入力し、グループ メンバーのユーザ名が格納されている属性と、グループ名が格納されている属性を入力します。LDAP サーバ プロファイルに対して選択されたサーバ タイプに基づいて、ユーザ名とグループ名の属性のデフォルト値とデフォルト クエリー文字列が AsyncOS によって入力されます。

（注）　Active Directory サーバの場合は、ユーザが特定のグループのメンバーかどうかを判断するためのデフォルトのクエリー文字列は (&(objectClass=group)(member={u})) です。ただし、使用する LDAP スキーマにおいて、「memberof」のリストでユーザ名ではなく識別名が使用されている場合は、{dn} を {u} の代わりに使用できます。

表 11-7 に、AsyncOS が Active Directory サーバ上でグループ メンバーシップ情報を検索するときに使用されるデフォルトのクエリー文字列と属性を示します。

表 11-7　Active Directory サーバのデフォルト クエリー文字列および属性

クエリー文字列	Active Directory
ベース DN	（ブランク）（グループ レコードを見つけるには具体的なベース DN を使用する必要があります）
ユーザが特定のグループのメンバーかどうかを判断するためのクエリー文字列	`(&(objectClass=group)(member={u}))` **（注）** 使用する LDAP スキーマにおいてメンバーのリストの中でユーザ名ではなく識別名が使用されている場合は、`{u}` の代わりに `{dn}` を使用できます。
グループのすべてのメンバーを判別するクエリー文字列	`(&(objectClass=group)(cn={g}))`
各メンバーのユーザ名（またはそのユーザのレコードの DN）が格納されている属性	`member`
グループ名が格納されている属性	`cn`

表 11-8 に、AsyncOS が OpenLDAP サーバ上でグループ メンバーシップ情報を検索するときに使用されるデフォルトのクエリー文字列と属性を示します。

表 11-8　Open LDAP サーバのデフォルト クエリー文字列および属性

クエリー文字列	OpenLDAP
ベース DN	（ブランク）（グループ レコードを見つけるには具体的なベース DN を使用する必要があります）
ユーザが特定のグループのメンバーかどうかを判断するためのクエリー文字列	`(&(objectClass=posixGroup)(memberUid={u}))`
グループのすべてのメンバーを判別するクエリー文字列	`(&(objectClass=posixGroup)(cn={g}))`
各メンバーのユーザ名（またはそのユーザのレコードの DN）が格納されている属性	`memberUid`
グループ名が格納されている属性	`cn`

管理ユーザの外部認証のイネーブル化

LDAP サーバ プロファイルおよびクエリーを設定した後で、LDAP を使用する外部認証をイネーブルにすることができます。

手順

ステップ 1　セキュリティ管理アプライアンスで、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザ（Users）] ページを選択します。

ステップ 2　[有効（Enable）] をクリックします。

ステップ 3　[外部認証を有効にする（Enable External Authentication）] チェックボックスをオンにします。

ステップ 4　認証タイプとして [LDAP] を選択します。

ステップ 5　ユーザを認証する LDAP 外部認証クエリーを選択します。

ステップ 6　タイムアウトするまでアプライアンスがサーバからの応答を待つ時間を秒単位で入力します。

ステップ 7　アプライアンスで認証する LDAP ディレクトリからのグループ名を入力し、グループのユーザに対するロールを選択します。

ステップ 8　また、[行の追加（Add Row）] をクリックして別のディレクトリ グループを追加することもできます。アプライアンスが認証する各ディレクトリ グループに対して、ステップ 7 とステップ 8 を繰り返します。

ステップ 9　変更を送信し、保存します。