CHAPTER 18

l2tp tunnel hello コマンド～ log-adj-changes コマンド

l2tp tunnel hello

L2TP over IPSec 接続の hello メッセージ間の間隔を指定するには、グローバル コンフィギュレーション モードで **l2tp tunnel hello** コマンドを使用します。コマンドをコンフィギュレーションから削除してデフォルトを設定するには、このコマンドの no 形式を使用します。

l2tp tunnel hello *interval*

no l2tp tunnel hello *interval*

シンタックスの説明

interval	hello メッセージ間の間隔（秒）。デフォルトは 60 秒です。範囲は 10 ～ 300 秒です。

デフォルト

デフォルトは 60 秒です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

l2tp tunnel hello コマンドは、セキュリティ アプライアンスによる L2TP 接続の物理レイヤに関する問題の検出をイネーブルにします。デフォルトは 60 秒です。それをより低い値に設定すると、問題の発生した接続はより早く解除されます。

例

次の例では、hello メッセージ間の間隔を 30 秒に設定します。

```
hostname(config)# l2tp tunnel hello 30
```

関連コマンド

コマンド	説明
show vpn-sessiondbdetail remote filter protocol L2TPOverIPSec	L2TP 接続の詳細を表示します。
vpn-tunnel-protocol l2tp-ipsec	特定のトンネル グループのトンネリング プロトコルとして L2TP をイネーブルにします。

ldap-attribute-map（AAA サーバ ホスト モード）

既存のマッピング コンフィギュレーションを LDAP ホストにバインドするには、AAA サーバ ホスト モードで **ldap-attribute-map** コマンドを使用します。

バインディングを削除するには、このコマンドの **no** 形式を使用します。

ldap-attribute-map *map-name*

no ldap-attribute-map *map-name*

シンタックスの説明

map-name	LDAP アトリビュート マッピング コンフィギュレーションを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

シスコ定義の LDAP アトリビュート名が使い勝手が悪い、または他の要件に合致しない場合は、独自のアトリビュート名を作成し、Cisco アトリビュートにマッピングしてから、得られたアトリビュート コンフィギュレーションを LDAP サーバにバインドすることができます。通常の手順は、次のとおりです。

1. グローバル コンフィギュレーション モードで **ldap attribute-map** コマンドを使用して、何も入力されていないアトリビュート マップを作成します。このコマンドにより、ldap-attribute-map モードに入ります。このコマンドでは、「ldap」の後にハイフンがないことに注意してください。

2. ldap-attribute-map モードで **map-name** コマンドおよび **map-value** コマンドを使用して、アトリビュート マッピング コンフィギュレーションに情報を入力します。
3. AAA サーバ ホスト モードで **ldap-attribute-map** コマンドを使用して、アトリビュート マップ コンフィギュレーションを LDAP サーバにバインドします。

例

次のコマンド例では、AAA サーバ ホスト コンフィギュレーション モードに入り、myldapmap という名前の既存のアトリビュート マップを ldapsvr1 という名前の LDAP サーバにバインドします。

```
hostname(config)# aaa-server ldapsvr1 host 10.10.0.1
hostname(config-aaa-server-host)# ldap-attribute-map myldapmap
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
ldap attribute-map（グローバル コンフィギュレーション モード）	ユーザ定義のアトリビュート名を Cisco LDAP アトリビュート名にマッピングするために、LDAP アトリビュート マップを作成し、名前を付けます。
map-name	ユーザ定義の LDAP アトリビュート名を、Cisco LDAP アトリビュート名にマッピングします。
map-value	ユーザ定義のアトリビュート値を、Cisco　アトリビュートにマッピングします。
show running-config ldap attribute-map	特定の実行 ldap アトリビュート マッピング コンフィギュレーション、またはすべての実行アトリビュート マッピング コンフィギュレーションを表示します。
clear configure ldap attribute-map	すべての LDAP アトリビュート マップを削除します。

ldap attribute-map（グローバル コンフィギュレーション モード）

ユーザ定義のアトリビュート名を Cisco LDAP アトリビュート名にマッピングするために LDAP アトリビュート マップを作成して名前をつけるには、グローバル コンフィギュレーション モードで **ldap attribute-map** コマンドを使用します。

マップを削除するには、このコマンドの **no** 形式を使用します。

ldap attribute-map *map-name*

no ldap attribute-map *map-name*

シンタックスの説明

map-name	LDAP アトリビュート マップにユーザ定義の名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

ldap attribute-map コマンドを使用すると、独自のアトリビュート名と値を Cisco アトリビュート名にマッピングできます。作成されたアトリビュート マップは、LDAP サーバにバインドすることができます。通常の手順は、次のとおりです。

1. グローバル コンフィギュレーション モードで **ldap attribute-map** コマンドを使用して、何も入力されていないアトリビュート マップを作成します。このコマンドにより、LDAP アトリビュート マップ コンフィギュレーション モードに入ります。
2. LDAP アトリビュート マップ コンフィギュレーション モードで **map-name** コマンドおよび **map-value** コマンドを使用して、アトリビュート マップに情報を入力します。
3. AAA サーバ ホスト モードで **ldap-attribute-map** コマンドを使用して、LDAP サーバにアトリビュート マップをバインドします。このコマンドでは、「ldap」の後にハイフンを入力してください。

（注） アトリビュート マッピング機能を正しく使用するには、Cisco LDAP アトリビュートの名前と値、およびユーザ定義アトリビュートの名前と値を理解しておく必要があります。

例

次の例では、コマンドをグローバル コンフィギュレーション モードで入力し、myldapmap という名前の LDAP アトリビュート マップを作成してから、情報の入力、または LDAP サーバへのバインドを行います。

```
hostname(config)# ldap attribute-map myldapmap
hostname(config-ldap-attribute-map)#
```

関連コマンド

コマンド	説明
ldap-attribute-map（AAA サーバ ホスト モード）	LDAP アトリビュート マップを LDAP サーバにバインドします。
map-name	ユーザ定義の LDAP アトリビュート名を、Cisco LDAP アトリビュート名にマッピングします。
map-value	ユーザ定義のアトリビュート値を、Cisco　アトリビュート名にマッピングします。
show running-config ldap attribute-map	特定の実行 LDAP アトリビュート マップまたはすべての実行アトリビュート マップを表示します。
clear configure ldap attribute-map	すべての LDAP アトリビュート マップを削除します。

ldap-base-dn

認可要求を受信したときに、サーバが検索を開始する LDAP 階層内の位置を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **ldap-base-dn** コマンドを使用します。AAA サーバ ホスト コンフィギュレーション モードには、AAA サーバ プロトコル コンフィギュレーション モードからアクセスできます。この指定を削除して、検索の開始位置をリストの先頭にリセットするには、このコマンドの **no** 形式を使用します。

ldap-base-dn *string*

no ldap-base-dn

シンタックスの説明

string	認可要求を受信したときに、サーバが検索を開始する LDAP 階層内の位置を指定する最大 128 文字の文字列で、大文字と小文字が区別されます（たとえば、OU=Cisco）。文字列にスペースは使用できませんが、その他の特殊文字は使用できます。

デフォルト

検索はリストの先頭から開始されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	既存のコマンドです。このリリースで修正されました。

使用上のガイドライン

このコマンドは、LDAP サーバに対してのみ有効です。

例

次の例では、ホスト「1.2.3.4」上で「srvgrp1」という LDAP AAA サーバを設定し、タイムアウトを 9 秒に設定し、リトライ間隔を 7 秒に設定し、LDAP ベース DN を「starthere」として設定します。

```
hostname(config)# aaa-server svrgrp1 protocol ldap
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# ldap-base-dn starthere
hostname(config-aaa-server-host)# exit
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードに入って、ホスト固有の AAA サーバ パラメータを設定できるようにします。
ldap-scope	認可要求を受信したときに、サーバが実行する LDAP 階層内検索の範囲を指定します。
ldap-naming-attribute	LDAP サーバ上のエントリを一意に識別するための、相対認定者名アトリビュート（複数可）を指定します。
ldap-login-dn	ディレクトリ オブジェクトの名前を指定します。システムは、オブジェクトをこの名前でバインドします。
ldap-login-password	ログイン DN のパスワードを指定します。

ldap-defaults

LDAP のデフォルト値を定義するには、crl 設定コンフィギュレーション モードで **ldap-defaults** コマンドを使用します。crl 設定コンフィギュレーション モードには、暗号 CA トラストポイント コンフィギュレーション モードからアクセスできます。これらのデフォルト値は、LDAP サーバが必要とする場合にだけ使用されます。LDAP デフォルトを指定しない場合は、このコマンドの **no** 形式を使用します。

ldap-defaults *server* [*port*]

no ldap-defaults

シンタックスの説明

port	（オプション）LDAP サーバ ポートを指定します。このパラメータが指定されていない場合、セキュリティ アプライアンスは標準の LDAP ポート（389）を使用します。
server	LDAP サーバの IP アドレスまたはドメイン名を指定します。CRL 配布ポイント内にサーバが存在する場合、この値はそのサーバによって上書きされます。

デフォルト

デフォルト値は設定されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
crl 設定コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、デフォルト ポート（389）上で LDAP デフォルト値を定義します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# ldap-defaults ldapdomain4 8389
```

関連コマンド

コマンド	説明
crl configure	ca-crl コンフィギュレーション モードに入ります。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。
protocol ldap	LDAP を CRL 取得方法として指定します。

ldap-dn

CRL の取得時に認証を要求する LDAP サーバに X.500 認定者名とパスワードを渡すには、crl 設定コンフィギュレーション モードで **ldap-dn** コマンドを使用します。crl 設定コンフィギュレーション モードには、暗号 CA トラストポイント コンフィギュレーション モードからアクセスできます。これらのパラメータは、LDAP サーバが必要とする場合にだけ使用されます。

LDAP DN を指定しない場合は、このコマンドの **no** 形式を使用します。

ldap-dn *x.500-name password*

no ldap-dn

シンタックスの説明

password	この認定者名のパスワードを定義します。フィールドの最大長は 128 文字です。
x.500-name	この CRL データベースにアクセスするためのディレクトリ パスを定義します（たとえば、cn=crl,ou=certs,o=CAName,c=US）。フィールドの最大長は 128 文字です。

デフォルト

デフォルト値は設定されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
crl 設定コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、X.500 の名前に CN=admin,OU=devtest,O=engineering を指定し、central トラストポイントのパスワードに xxzzyy を指定します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# ldap-dn cn=admin,ou=devtest,o=engineering xxzzyy
```

関連コマンド

コマンド	説明
crl configure	crl 設定コンフィギュレーション モードに入ります。
crypto ca trustpoint	CA トラストポイント コンフィギュレーション モードに入ります。
protocol ldap	CRL の取得方法として LDAP を指定します。

ldap-login-dn

システムがバインドするディレクトリ オブジェクトの名前を指定するには、AAA サーバ ホスト モードで **ldap-login-dn** コマンドを使用します。AAA サーバ ホスト コンフィギュレーション モードには、AAA サーバ プロトコル コンフィギュレーション モードからアクセスできます。この指定を削除するには、このコマンドの **no** 形式を使用します。

ldap-login-dn *string*

no ldap-login-dn

シンタックスの説明

string	LDAP 階層内のディレクトリ オブジェクトの名前を指定する最大 128 文字の文字列で、大文字と小文字が区別されます。文字列にスペースは使用できませんが、その他の特殊文字は使用できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0 (1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、LDAP サーバに対してのみ有効です。サポートされる文字列の最大長は 128 文字です。

Microsoft Active Directory サーバなどの LDAP サーバでは、他のすべての LDAP 動作に関する要求を受け入れる前に、セキュリティ アプライアンスが認証済みバインディングを介してハンドシェイクを確立している必要があります。セキュリティ アプライアンスは、認証済みバインディングに対して識別情報を示すときに、ユーザ認証要求に Login DN フィールドを付加します。Login DN フィールドは、セキュリティ アプライアンスの認証特性を説明します。この特性は、管理者特権を持つユーザの特性に対応している必要があります。

string 変数には、VPN コンセントレータの認証済みバインディングに関するディレクトリ オブジェクトの名前を入力します（たとえば、cn=Administrator、cn=users、ou=people、dc=XYZ Corporation、dc=com）。匿名アクセスの場合、このフィールドはブランクのままにします。

例

次の例では、ホスト「1.2.3.4」上で「srvgrp1」という LDAP AAA サーバを設定し、タイムアウトを 9 秒に設定し、リトライ間隔を 7 秒に設定し、LDAP ログイン DN を「myobjectname」として設定します。

```
hostname(config)# aaa-server svrgrp1 protocol ldap
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# ldap-login-dn myobjectname
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードに入って、ホスト固有の AAA サーバ パラメータを設定できるようにします。
ldap-base-dn	認可要求を受信したときに、サーバが検索を開始する LDAP 階層内の位置を指定します。
ldap-login-password	ログイン DN のパスワードを指定します。このコマンドは、LDAP サーバに対してのみ有効です。
ldap-naming-attribute	LDAP サーバ上のエントリを一意に識別するための、相対認定者名アトリビュート（複数可）を指定します。
ldap-scope	認可要求を受信したときに、サーバが実行する LDAP 階層内検索の範囲を指定します。

ldap-login-password

LDAP サーバのログイン パスワードを指定するには、AAA サーバ ホスト モードで **ldap-login-password** コマンドを使用します。AAA サーバ ホスト コンフィギュレーション モードには、AAA サーバ プロトコル コンフィギュレーション モードからアクセスできます。このパスワード指定を削除するには、このコマンドの **no** 形式を使用します。

ldap-login-password *string*

no ldap-login-password

シンタックスの説明

string	大文字と小文字が区別される最大 64 文字の英数字のパスワード。パスワードにスペースは使用できません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、LDAP サーバに対してのみ有効です。パスワード文字列の最大長は 64 文字です。

例

次の例では、ホスト「1.2.3.4」上で「srvgrp1」という LDAP AAA サーバを設定し、タイムアウトを 9 秒に設定し、リトライ間隔を 7 秒に設定し、LDAP ログイン パスワードを「obscurepassword」として設定します。

```
hostname(config)# aaa-server svrgrp1 protocol ldap
hostname(config)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server)# timeout 9
hostname(config-aaa-server)# retry 7
hostname(config-aaa-server)# ldap-login-password obscurepassword
hostname(config-aaa-server)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードに入って、ホスト固有の AAA サーバ パラメータを設定できるようにします。
ldap-base-dn	認可要求を受信したときに、サーバが検索を開始する LDAP 階層内の位置を指定します。
ldap-login-dn	ディレクトリ オブジェクトの名前を指定します。システムは、オブジェクトをこの名前でバインドします。

ldap-naming-attribute	LDAP サーバ上のエントリを一意に識別するための、相対認定者名アトリビュート（複数可）を指定します。
ldap-scope	認可要求を受信したときに、サーバが実行する LDAP 階層内検索の範囲を指定します。

ldap-naming-attribute

相対認定者名アトリビュートを指定するには、AAA サーバ ホスト モードで **ldap-naming-attribute** コマンドを使用します。AAA サーバ ホスト コンフィギュレーション モードには、AAA サーバ プロトコル コンフィギュレーション モードからアクセスできます。この指定を削除するには、このコマンドの **no** 形式を使用します。

ldap-naming-attribute *string*

no ldap-naming-attribute

シンタックスの説明

string	LDAP サーバ上のエントリを一意に識別するための相対認定者名アトリビュートで、大文字と小文字が区別される最大 128 文字の英数字です。文字列にスペースは使用できませんが、その他の特殊文字は使用できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
aaa-server host	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

LDAP サーバ上のエントリを一意に識別するための、相対認定者名アトリビュートを入力します。共通の命名アトリビュートは、通常名（cn）とユーザ ID（uid）です。

このコマンドは、LDAP サーバに対してのみ有効です。サポートされる文字列の最大長は 128 文字です。

例

次の例では、ホスト「1.2.3.4」上で「srvgrp1」という LDAP AAA サーバを設定し、タイムアウトを 9 秒に設定し、リトライ間隔を 7 秒に設定し、LDAP 命名アトリビュートを「cn」として設定します。

```
hostname(config)# aaa-server svrgrp1 protocol ldap
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# ldap-naming-attribute cn
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードに入って、ホスト固有の AAA サーバ パラメータを設定できるようにします。
ldap-base-dn	認可要求を受信したときに、サーバが検索を開始する LDAP 階層内の位置を指定します。
ldap-login-dn	ディレクトリ オブジェクトの名前を指定します。システムは、オブジェクトをこの名前でバインドします。
ldap-login-password	ログイン DN のパスワードを指定します。このコマンドは、LDAP サーバに対してのみ有効です。
ldap-scope	認可要求を受信したときに、サーバが実行する LDAP 階層内検索の範囲を指定します。

ldap-over-ssl

セキュリティ アプライアンスと LDAP サーバの間にセキュアな SSL 接続を確立するには、AAA サーバ ホスト コンフィギュレーション モードで **ldap-over-ssl** コマンドを使用します。

接続に対して SSL をディセーブルにするには、このコマンドの **no** 形式を使用します。

ldap-over-ssl enable

no ldap-over-ssl enable

シンタックスの説明

enable	SSL により LDAP サーバへの接続が保護されることを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、セキュリティ アプライアンスと LDAP サーバ間の接続を SSL で保護することを指定するために使用します。

（注） 平文認証を使用している場合は、この機能をイネーブルにすることを推奨します。**sasl-mechanism** コマンドを参照してください。

例

次のコマンドを、AAA サーバ ホスト コンフィギュレーション モードで入力して、セキュリティ アプライアンスと、IP アドレスが 10.10.0.1 の ldapsvr1 という LDAP サーバとの間の接続に対して SSL をイネーブルにします。また、PLAIN SASL 認証メカニズムも設定します。

```
hostname(config)# aaa-server ldapsvr1 protocol ldap
hostname(config-aaa-server-host)# aaa-server ldapsvr1 host 10.10.0.1
hostname(config-aaa-server-host)# ldap-over-ssl enable
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
sasl-mechanism	LDAP クライアントとサーバの間に SASL 認証を指定します。
server-type	LDAP サーバのベンダーを Microsoft または Sun として指定します。
ldap attribute-map（グローバル コンフィギュレーション モード）	ユーザ定義のアトリビュート名を Cisco LDAP アトリビュート名にマッピングするために、LDAP アトリビュート マップを作成し、名前を付けます。

ldap-scope

認可要求を受信したときに、サーバが検索する LDAP 階層内の範囲を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **ldap-scope** コマンドを使用します。AAA サーバ ホスト コンフィギュレーション モードには、AAA サーバ プロトコル コンフィギュレーション モードからアクセスできます。この指定を削除するには、このコマンドの **no** 形式を使用します。

ldap-scope *scope*

no ldap-scope

シンタックスの説明

scope	認可要求を受信したときに、サーバが検索する LDAP 階層のレベル番号を指定します。有効値は、次のとおりです。 • ***onelevel***：ベース DN の 1 つ下のレベルのみを検索します。 • ***subtree***：ベース DN の下にあるすべてのレベルを検索します。

デフォルト

デフォルト値は、***onelevel*** です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	既存のコマンドです。このリリースで修正されました。

使用上のガイドライン

スコープを ***onelevel*** として指定すると、検索速度が向上します。これは、ベース DN の 1 つ下のレベルだけが検索されるためです。***subtree*** を指定すると速度が低下します。これは、ベース DN の下にあるすべてのレベルが検索されるためです。

このコマンドは、LDAP サーバに対してのみ有効です。

例

次の例では、ホスト「1.2.3.4」上で「srvgrp1」という LDAP AAA サーバを設定し、タイムアウトを 9 秒に設定し、リトライ間隔を 7 秒に設定し、LDAP スコープがサブツリー レベルを含むように設定します。

```
hostname(config)# aaa-server svrgrp1 protocol ldap
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# ldap-scope subtree
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードに入って、ホスト固有の AAA サーバ パラメータを設定できるようにします。
ldap-base-dn	認可要求を受信したときに、サーバが検索を開始する LDAP 階層内の位置を指定します。
ldap-login-dn	ディレクトリ オブジェクトの名前を指定します。システムは、オブジェクトをこの名前でバインドします。
ldap-login-password	ログイン DN のパスワードを指定します。このコマンドは、LDAP サーバに対してのみ有効です。
ldap-naming-attribute	LDAP サーバ上のエントリを一意に識別するための、相対認定者名アトリビュート（複数可）を指定します。

leap-bypass

LEAP Bypass をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで **leap-bypass enable** コマンドを使用します。LEAP Bypass をディセーブルにするには、**leap-bypass disable** コマンドを使用します。LEAP Bypass アトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、LEAP Bypass の値を別のグループ ポリシーから継承できます。

LEAP Bypass をイネーブルにすると、VPN ハードウェア クライアントの背後にある無線デバイスからの LEAP パケットが、ユーザ認証の前に VPN トンネルを通過できるようになります。これにより、シスコの無線アクセス ポイント デバイスを使用するワークステーションで LEAP 認証を確立できます。確立後、ワークステーションはユーザごとの認証をもう一度実行します。

leap-bypass {**enable | disable**}

no leap-bypass

シンタックスの説明

disable	LEAP Bypass をディセーブルにします。
enable	LEAP Bypass をイネーブルにします。

デフォルト

LEAP Bypass はディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

対話型のハードウェア クライアント認証がイネーブルになっていると、この機能は正常に動作しません。

詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

（注） 認証されていないトラフィックがトンネルを通過できるようにすると、セキュリティ リスクが生じる場合があります。

例

次の例は、「FirstGroup」というグループ ポリシーに LEAP Bypass を設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# leap-bypass enable
```

関連コマンド

コマンド	説明
secure-unit-authentication	VPN ハードウェア クライアントがトンネルを開始するたびに、クライアントにユーザ名とパスワードによる認証を要求します。
user-authentication	VPN ハードウェア クライアントの背後にいるユーザに対して、接続前にセキュリティ アプライアンスに識別情報を示すように要求します。

lifetime

IKE セキュリティ アソシエーションの期限が切れるまでのライフタイムを指定するには、暗号 isakmp ポリシー コンフィギュレーション モードで **lifetime** コマンドを使用します。ピアがライフタイムを提示していなければ、無限のライフタイムを指定できます。セキュリティ アソシエーションのライフタイムをデフォルト値の 86,400 秒（1 日）にリセットするには、このコマンドの **no** 形式を使用します。

lifetime *seconds*

no lifetime

シンタックスの説明

priority	Internet Key Exchange（IKE）ポリシーを一意に識別し、そのポリシーに優先順位を割り当てます。1 ～ 65534 の整数を使用します。1 は優先順位が最も高く、65534 が最も低くなります。
seconds	各セキュリティ アソシエーションが期限満了するまでの秒数を指定します。有限のライフタイムを提示するには、120 ～ 2,147,483,647 秒の整数を使用します。無限のライフタイムを提示するには、0 秒を使用します。

デフォルト

デフォルト値は 86,400 秒（1 日）です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 isakmp ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	**isakmp policy lifetime** コマンドは既存のものです。
7.2.(1)	**isakmp policy lifetime** コマンドが、**lifetime** コマンドに置き換えられました。

使用上のガイドライン

IKE は、ネゴシエーションを開始するとき、自身のセッション用のセキュリティ パラメータを合意しようとします。次に、各ピアのセキュリティ アソシエーションが、合意されたパラメータを参照します。ピアは、ライフタイムが期限満了するまで、セキュリティ アソシエーションを保持します。セキュリティ アソシエーションは、期限満了するまでその後の IKE ネゴシエーションで利用できるため、新しい IPSec セキュリティ アソシエーションを設定するときに時間を節約できます。ピアは、現在のセキュリティ アソシエーションが期限満了する前に、新しいセキュリティ アソシエーションをネゴシエートします。

ライフタイムを長くするほど、セキュリティ アプライアンスで以降の IPSec セキュリティ アソシエーションを設定する時間が節約されます。暗号化強度は十分なレベルにあるため、キーの再生成間隔を極端に短く（約 2 ～ 3 分ごとに）しなくてもセキュリティは保証されます。デフォルトをそのまま使用することをお勧めします。

（注） IKE セキュリティ アソシエーションが無限のライフタイムに設定されている場合、ピアが有限のライフタイムを提示したときは、ピアからのネゴシエートされた有限のライフタイムが使用されます。

例

この例では、グローバル コンフィギュレーション モードで、優先順位番号 40 の IKE ポリシー内に IKE セキュリティ アソシエーションのライフタイムを 50,400 秒（14 時間）に設定します。

```
hostname(config)# crypto isakmp policy 40
hostname(config-isakmp-policy)# lifetime 50400
```

次の例では、グローバル コンフィギュレーション モードで、IKE セキュリティ アソシエーションを無限のライフタイムに設定します。

```
hostname(config)# crypto isakmp policy 40
hostname(config-isakmp-policy)# lifetime 0
```

関連コマンド

clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure crypto isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear crypto isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

limit-resource

マルチ コンテキスト モードでクラスにリソース制限を指定するには、クラス コンフィギュレーション モードで **limit-resource** コマンドを使用します。制限をデフォルトに戻すには、このコマンドの **no** 形式を使用します。セキュリティ アプライアンスでは、コンテキストをリソース クラスに割り当てることでリソースを管理します。各コンテキストは、クラスによって設定されるリソース制限値を使用します。

limit-resource {**all 0** | [**rate**] *resource_name number*[**%**]}

no limit-resource {**all** | [**rate**] *resource_name*}

シンタックスの説明

all 0	すべてのリソースに対して制限を無制限として設定します。
number[**%**]	リソース制限を 1 以上の固定数として指定します。あるいは、パーセント記号（%）を使用して、1 ～ 100 までのシステム制限のパーセンテージとして指定します。無制限のリソースを示す場合は、制限を **0** に設定します。システム制限を持たないリソースの場合はパーセンテージ（%）を設定できません。絶対値のみ設定できます。
rate	リソースに対して秒単位でレートを設定することを指定します。秒単位でレートを設定可能なリソースについては、表 18-1 を参照してください。
resource_name	制限を設定するリソース名を指定します。この制限は、**all** に設定されている制限を上書きします。

デフォルト

すべてのリソースは、次に示す制限を除いて無制限に設定されています。これらの制限は、デフォルトではコンテキストごとに許可される最上限に設定されています。

- Telnet セッション：5 セッション。
- SSH セッション：5 セッション。
- IPSec セッション：5 セッション。
- MAC アドレス：65,535 エントリ。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

クラスに対してリソース制限を設定する場合、セキュリティ アプライアンスはクラスに割り当てられた各コンテキストにリソースの一部を確保するのではなく、セキュリティ アプライアンスはコンテキストに上限を設定します。リソースをオーバーサブスクライブした場合や、一部のリソースを無制限に許可した場合は、いくつかのコンテキストがそれらのリソースを使い果たして、他のコンテキストへのサービスに影響を及ぼす可能性があります。

表 18-1 には、リソースのタイプと制限がリストされています。**show resource types** コマンドも参照してください。

表 18-1　リソース名と制限

リソース名	レートまたは同時接続数	コンテキスト単位の最少数と最大数	システム制限[1]	説明
mac-addresses	同時接続数	該当なし	65,535	透過ファイアウォール モードで、MAC アドレス テーブルに含められる MAC アドレスの数。
conns	同時接続数またはレート	該当なし	同時接続数：プラットフォームの接続制限については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。 レート：該当なし	1 つのホストと複数の他のホストとの間の接続を含む、2 つのホスト間の TCP または UDP 接続。
inspects	比率	該当なし	該当なし	アプリケーション検査。
hosts	同時接続数	該当なし	該当なし	セキュリティ アプライアンスを通じて接続可能なホスト。
asdm	同時接続数	最小値：1 最大値：5	32	ASDM 管理セッション。 **（注）** ASDM セッションでは 2 つの HTTPS 接続が使用されます。1 つは常に必要な監視用、もう 1 つは変更を加えたときにのみ必要となる設定の変更用です。たとえば、ASDM セッションのシステム制限が 32 である場合は、HTTPS セッション数が 64 に制限されることを示します。
ssh	同時接続数	最小値：1 最大値：5	100	SSH セッション。
syslogs	比率	該当なし	該当なし	System ログ メッセージ。
telnet	同時接続数	最小値：1 最大値：5	100	Telnet セッション。
xlates	同時接続数	該当なし	該当なし	アドレス変換。

1.　このカラム値が該当なしの場合、リソースにハード システム制限がないため、リソースのパーセンテージを設定できません。

例

次の例では、conns に関するデフォルト クラスの制限値を、無制限から 10% に設定し直しています。

```
hostname(config)# class default
hostname(config-class)# limit-resource conns 10%
```

他のリソースは、すべて無制限のままです。

gold というクラスを追加するには、次のコマンドを入力します。

```
hostname(config)# class gold
hostname(config-class)# limit-resource mac-addresses 10000
hostname(config-class)# limit-resource conns 15%
hostname(config-class)# limit-resource rate conns 1000
hostname(config-class)# limit-resource rate inspects 500
hostname(config-class)# limit-resource hosts 9000
hostname(config-class)# limit-resource asdm 5
hostname(config-class)# limit-resource ssh 5
hostname(config-class)# limit-resource rate syslogs 5000
hostname(config-class)# limit-resource telnet 5
hostname(config-class)# limit-resource xlates 36000
```

関連コマンド

コマンド	説明
class	リソース クラスを作成します。
context	セキュリティ コンテキストを設定します。
member	リソース クラスにコンテキストを割り当てます。
show resource allocation	リソースを各クラスにどのように割り当てたかを表示します。
show resource types	制限を設定できるリソース タイプを表示します。

lmfactor

他のサーバによって設定された有効期限値ではなく、最後に変更されたタイムスタンプのみを持つオブジェクトをキャッシュするように再検証ポリシーを設定するには、キャッシュ モードで **lmfactor** コマンドを使用します。このようなオブジェクトを再検証するために新しいポリシーを設定するには、このコマンドを再度使用します。このアトリビュートをデフォルト値の 20 にリセットするには、このコマンドの **no** 形式を入力します。

lmfactor *value*

no lmfactor

シンタックスの説明

value	0 ～ 100 の範囲の整数。

デフォルト

デフォルト値は 20 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
キャッシュ モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスは、lmfactor の値を使用して、キャッシュされたオブジェクトに変化がないと見なす時間の長さを推定します。これが有効期限として認識されます。セキュリティ アプライアンスは有効期限を、最後の変更から経過した時間に lmfactor を乗算して推定します。

lmfactor をゼロに設定すると、再検証をただちに強制することになります。またこれを 100 に設定すると、再検証が強制されるまでの許容時間が最長になります。

例

次の例は、lmfactor を 30 に設定する方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# cache
hostname(config-webvpn-cache)# lmfactor 30
hostname(config-webvpn-cache)#
```

関連コマンド

コマンド	説明
cache	WebVPN キャッシュ モードに入ります。
cache-compressed	WebVPN キャッシュの圧縮を設定します。
disable	キャッシングをディセーブルにします。
expiry-time	オブジェクトを再検証せずにキャッシュする有効期限を設定します。
max-object-size	キャッシュするオブジェクトの最大サイズを定義します。
min-object-size	キャッシュするオブジェクトの最小サイズを定義します。

log

モジュラ ポリシー フレームワークを使用する場合は、一致またはクラス コンフィギュレーション モードで **log** コマンドを使用して **match** コマンドまたはクラス マップに一致するパケットをログに記録します。このログ アクションは、アプリケーション トラフィックの検査ポリシー マップで使用できます（**policy-map type inspect** コマンド）。このアクションをディセーブルにするには、このコマンドの **no** 形式を使用します。

log

no log

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
一致コンフィギュレーションおよびクラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

検査ポリシー マップは、1 つ以上の **match** コマンドと **class** コマンドで構成されます。検査ポリシー マップで使用できるコマンド自体は、アプリケーションによって異なります。**match** または **class** コマンドを入力してアプリケーション トラフィックを識別してから（**class** コマンドは、**match** コマンドを含む既存の **class-map type inspect** コマンドを指す）、**log** コマンドを入力し、**match** コマンドまたは **class** コマンドに一致するパケットをすべてログに記録します。

レイヤ 3/4 ポリシー マップ（**policy-map** コマンド）で **inspect** コマンドを使用してアプリケーション検査をイネーブルにするときは、このアクションを含んでいる検査ポリシー マップをイネーブルにします。たとえば、**inspect http http_policy_map** コマンドを入力します。http_policy_map は検査ポリシー マップの名前です。

例

次の例では、パケットが http-traffic クラス マップに一致する場合にログを送信します。

```
hostname(config-cmap)# policy-map type inspect http http-map1
hostname(config-pmap)# class http-traffic
hostname(config-pmap-c)# log
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
policy-map type inspect	アプリケーション検査のための特別なアクションを定義します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

log-adj-changes

OSPF 隣接ルータがアップ状態またはダウン状態になると syslog メッセージを送信するようにルータを設定するには、ルータ コンフィギュレーション モードで **log-adj-changes** コマンドを使用します。この機能をオフにするには、このコマンドの **no** 形式を使用します。

log-adj-changes [*detail*]

no log-adj-changes [*detail*]

シンタックスの説明

detail	（オプション）隣接ルータがアップ状態またはダウン状態になるときだけでなく、状態が変化するたびに syslog メッセージを送信します。

デフォルト

このコマンドは、デフォルトではイネーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

log-adj-changes コマンドは、デフォルトでイネーブルになっており、コマンドの **no** 形式を使用して削除しない限り、実行コンフィギュレーションに表示されます。

例

次の例では、OSPF 隣接ルータがアップ状態またはダウン状態になったときに syslog メッセージを送信しないようにします。

```
hostname(config)# router ospf 5
hostname(config-router)# no log-adj-changes
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードに入ります。
show ospf	OSPF ルーティング プロセスに関する一般情報を表示します。