CHAPTER 7

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

l2tp tunnel hello

L2TP over IPsec 接続における 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。この間隔をデフォルト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。

l2tp tunnel hello *interval*

no l2tp tunnel hello *interval*

構文の説明

間隔	hello メッセージ間の間隔（秒）。デフォルトは 60 秒です。指定できる範囲は 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

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

l2tp tunnel hello コマンドは、ASA による L2TP 接続の物理層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。デフォルト設定を使用すると、L2TP トンネルが 180 秒後に切断されることが予想されます。60 秒未満の値に設定すると、問題が発生している接続はより早く切断されます。L2TP の最大再試行回数は 3 回です。

例

次に、hello メッセージ間の間隔を 30 秒に設定する例を示します。

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

関連コマンド

コマンド	説明
show vpn-sessiondb detail remote filter protocol L2TPOverIPsec	L2TP 接続の詳細を表示します。
vpn-tunnel-protocol l2tp-ipsec	L2TP を特定のトンネル グループのトンネリング プロトコルとしてイネーブルにします。

lacp max-bundle

EtherChannel チャネル グループで許可されるアクティブ インターフェイスの最大数を指定するには、インターフェイス コンフィギュレーション モードで **lacp max-bundle** コマンドを使用します。この値をデフォルトに設定するには、このコマンドの **no** 形式を使用します。

lacp max-bundle *number*

no lacp max-bundle

構文の説明

number	このチャネル グループで許可されるアクティブ インターフェイスの最大数を 1 ～ 8 の範囲内で指定します。9.2(1) 以降では、最大数が 16 に引き上げられています。スイッチが 16 個のアクティブ インターフェイスをサポートしていない場合、このコマンドは必ず 8 以下に設定する必要があります。

コマンド デフォルト

(9.1 以前)デフォルトは 8 です。

(9.2(1) 以降)デフォルトは 16 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.2(1)	アクティブ インターフェイスの数が 8 から 16 に増加しました。

使用上のガイドライン

このコマンドは、ポートチャネル インターフェイスに対して入力します。チャネル グループあたりのアクティブ インターフェイスの最大数は 8 です。このコマンドは、最大数を減らす場合に使用します。

例

次に、EtherChannel のインターフェイスの最大数を 4 に設定する例を示します。

```
ciscoasa(config)# interface port-channel 1
ciscoasa(config-if)# lacp max-bundle 4
```

関連コマンド

コマンド	説明
channel-group	EtherChannel にインターフェイスを追加します。
interface port-channel	EtherChannel を設定します。
lacp port-priority	チャネル グループの物理インターフェイスのプライオリティを設定します。
lacp system-priority	LACP システム プライオリティを設定します。
port-channel load-balance	ロード バランシング アルゴリズムを設定します。
port-channel min-bundle	ポートチャネル インターフェイスがアクティブになるために必要な、アクティブ インターフェイスの最小数を指定します。
show lacp	LACP 情報（トラフィック統計情報、システム ID、ネイバーの詳細など）が表示されます。
show port-channel	EtherChannel 情報が、詳細に 1 行のサマリー形式で表示されます。このコマンドは、ポートとポートチャネルの情報も表示します。
show port-channel load-balance	ポートチャネル負荷分散情報が、指定のパラメータ セットに対するハッシュ結果および選択されたメンバー インターフェイスとともに表示されます。

lacp port-priority

EtherChannel における物理インターフェイスのプライオリティを設定するには、インターフェイス コンフィギュレーション モードで **lacp port-priority** コマンドを使用します。プライオリティをデフォルトに設定するには、このコマンドの **no** 形式を使用します。

lacp port-priority *number*

no lacp port-priority

構文の説明

number	プライオリティ（1 ～ 65535）を設定します。数字が大きいほど、プライオリティは低くなります。

コマンド デフォルト

デフォルトは 32768 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、物理インターフェイスに対して入力します。使用可能な数よりも多くのインターフェイスを割り当てた場合、ASA ではこの設定を使用して、アクティブ インターフェイスとスタンバイ インターフェイスを決定します。ポート プライオリティ設定がすべてのインターフェイスで同じ場合、プライオリティはインターフェイス ID（スロット/ポート）で決まります。最も小さいインターフェイス ID が、最も高いプライオリティになります。たとえば、GigabitEthernet 0/0 のプライオリティは GigabitEthernet 0/1 よりも高くなります。

あるインターフェイスについて、インターフェイス ID は大きいが、そのインターフェイスがアクティブになるように優先順位を付ける場合は、より小さい値を持つようにこのコマンドを設定します。たとえば、GigabitEthernet 1/3 を GigabitEthernet 0/7 よりも前にアクティブにするには、**lacp port-priority** の値を、1/3 インターフェイスでは 12345 とし、0/7 インターフェイスではデフォルトの 32768 とします。

EtherChannel の反対の端にあるデバイスのポート プライオリティが衝突している場合、システム プライオリティを使用して使用するポート プライオリティが決定されます。**lacp system-priority** コマンドを参照してください。

リンク集約制御プロトコル（LACP）では、2 つのネットワーク デバイス間でリンク集約制御プロトコル データ ユニット（LACPDU）を交換することによって、インターフェイスが集約されます。LACP では、ユーザが介入しなくても、EtherChannel へのリンクの自動追加および削除が調整されます。また、コンフィギュレーションの誤りが処理され、メンバ インターフェイスの両端が正しいチャネル グループに接続されていることがチェックされます。

例

次に、GigabitEthernet 0/2 のポート プライオリティの値を小さくして、EtherChannel で GigabitEthernet 0/0 および 0/1 よりも先に使用されるように設定する例を示します。

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# interface GigabitEthernet0/1
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# lacp port-priority 1234
ciscoasa(config-if)# channel-group 1 mode active
```

関連コマンド

コマンド	説明
channel-group	EtherChannel にインターフェイスを追加します。
interface port-channel	EtherChannel を設定します。
lacp max-bundle	チャネル グループで許可されるアクティブ インターフェイスの最大数を指定します。
lacp system-priority	LACP システム プライオリティを設定します。
port-channel load-balance	ロード バランシング アルゴリズムを設定します。
port-channel min-bundle	ポートチャネル インターフェイスがアクティブになるために必要な、アクティブ インターフェイスの最小数を指定します。
show lacp	LACP 情報（トラフィック統計情報、システム ID、ネイバーの詳細など）が表示されます。
show port-channel	EtherChannel 情報が、詳細に 1 行のサマリー形式で表示されます。このコマンドは、ポートとポートチャネルの情報も表示します。
show port-channel load-balance	ポートチャネル負荷分散情報が、指定のパラメータ セットに対するハッシュ結果および選択されたメンバー インターフェイスとともに表示されます。

lacp system-priority

EtherChannel における ASA 全体での LACP システムのプライオリティを設定するには、グローバル コンフィギュレーション モードで **lacp system-priority** コマンドを使用します。この値をデフォルトに設定するには、このコマンドの **no** 形式を使用します。

lacp system-priority *number*

no lacp system-priority

構文の説明

number	LACP システム プライオリティを 1 ～ 65535 の範囲で設定します。デフォルトは 32768 です。数字が大きいほど、プライオリティは低くなります。このコマンドは、ASA に対してグローバルです。

コマンド デフォルト

デフォルトは 32768 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。

使用上のガイドライン

EtherChannel の反対の端にあるデバイスのポート プライオリティが衝突している場合、システム プライオリティを使用して使用するポート プライオリティが決定されます。EtherChannel 内でのインターフェイス プライオリティについては、**lacp port-priority** コマンドを参照してください。

例

次に、システムのプライオリティをデフォルトよりも高くする（小さい数値を設定する）例を示します。

```
ciscoasa(config)# lacp system-priority 12345
```

関連コマンド

コマンド	説明
channel-group	EtherChannel にインターフェイスを追加します。
interface port-channel	EtherChannel を設定します。
lacp max-bundle	チャネル グループで許可されるアクティブ インターフェイスの最大数を指定します。
lacp port-priority	チャネル グループの物理インターフェイスのプライオリティを設定します。
port-channel load-balance	ロード バランシング アルゴリズムを設定します。
port-channel min-bundle	ポートチャネル インターフェイスがアクティブになるために必要な、アクティブ インターフェイスの最小数を指定します。
show lacp	LACP 情報（トラフィック統計情報、システム ID、ネイバーの詳細など）が表示されます。
show port-channel	EtherChannel 情報が、詳細に 1 行のサマリー形式で表示されます。このコマンドは、ポートとポートチャネルの情報も表示します。
show port-channel load-balance	ポートチャネル負荷分散情報が、指定のパラメータ セットに対するハッシュ結果および選択されたメンバー インターフェイスとともに表示されます。

ldap attribute-map

ユーザ定義の属性名を Cisco LDAP 属性名にマッピングするために LDAP 属性マップを作成し、名前を付けるには、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*

構文の説明

map-name	LDAP 属性マップのユーザ定義名を指定します。

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

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

ldap attribute-map コマンドを使用すると、ユーザ独自の属性名と値を Cisco 属性名にマッピングできます。その後、作成された属性マップを LDAP サーバにバインドできます。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、何も入力されていない属性マップを作成します。このコマンドにより、LDAP 属性マップ コンフィギュレーション モードが開始されます。
2. LDAP 属性マップ コンフィギュレーション モードで **map-name** コマンドと **map-value** コマンドを使用し、属性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、属性マップを LDAP サーバにバインドします。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) 属性マッピング機能を正しく使用するには、Cisco LDAP 属性名と値の両方を理解し、さらにユーザ定義属性名と値を理解しておく必要があります。

例

次に、グローバル コンフィギュレーション モードで、情報を入力したり LDAP サーバにバインドする前に myldapmap という名前の LDAP 属性マップを作成するコマンドの例を示します。

```
ciscoasa(config)# ldap attribute-map myldapmap
ciscoasa(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 属性マップを LDAP サーバにバインドします。
map-name	ユーザ定義の LDAP 属性名を Cisco LDAP 属性名にマッピングします。
map-value	ユーザ定義の属性値を Cisco 属性名にマッピングします。
show running-config ldap attribute-map	実行中の特定の LDAP 属性マップまたは実行中のすべての属性マップを表示します。
clear configure ldap attribute-map	すべての LDAP 属性マップを削除します。

ldap-attribute-map

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 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。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*

構文の説明

map-name	LDAP 属性マッピング 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

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

シスコ定義の LDAP 属性名が使いやすさやその他の要件を満たしていない場合は、独自の属性名を作成し、それをシスコの属性にマッピングして、作成された属性コンフィギュレーションを LDAP サーバにバインドできます。一般的な手順には次のものが含まれます。

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、何も入力されていない属性マップを作成します。このコマンドにより、LDAP 属性マップ コンフィギュレーション モードが開始されます。このコマンドでは、「ldap」の後にハイフンを入力しないでください。
2. LDAP 属性マップ コンフィギュレーション モードで **map-name** コマンドと **map-value** コマンドを使用して、属性マッピング 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、LDAP サーバに属性マップ コンフィギュレーションをバインドします。

例

次に、AAA サーバ ホスト コンフィギュレーション モードで、myldapmap という名前の既存の属性マップを ldapsvr1 という名前の LDAP サーバにバインドするコマンドの例を示します。

```
ciscoasa(config)# aaa-server ldapsvr1 host 10.10.0.1
ciscoasa(config-aaa-server-host)# ldap-attribute-map myldapmap
ciscoasa(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）	ユーザ定義の属性名を Cisco LDAP 属性名にマッピングするために、LDAP 属性マップを作成して名前を付けます。
map-name	ユーザ定義の LDAP 属性名を、Cisco LDAP 属性名にマッピングします。
map-value	ユーザ定義の属性値をシスコ属性にマッピングします。
show running-config ldap attribute-map	特定の実行 LDAP 属性マッピング コンフィギュレーションまたはすべての実行属性マッピング 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 属性マップを削除します。

ldap-base-dn

サーバが認可要求を受信したときに検索を開始する、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

構文の説明

string	サーバが認可要求を受信したときに検索を開始する LDAP 階層内の位置を指定する、最大 128 文字のストリング（たとえば、OU=Cisco）。大文字と小文字は区別されます。

デフォルト

リストの先頭から検索を開始します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは LDAP サーバでのみ有効です。

例

次に、ホスト 1.2.3.4 に srvgrp1 という名前の LDAP AAA サーバを設定し、タイムアウトを 9 秒、再試行間隔を 7 秒、LDAP ベース DN を starthere に設定する例を示します。

```
ciscoasa(config)# aaa-server svrgrp1 protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa(config-aaa-server-host)# timeout 9
ciscoasa(config-aaa-server-host)# retry 7
ciscoasa(config-aaa-server-host)# ldap-base-dn starthere
ciscoasa(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 モードを開始し、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	サーバが認可要求を受信した場合に検索する LDAP 階層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、1 つ以上の相対識別名属性を指定します。
ldap-login-dn	システムがバインドするディレクトリ オブジェクト名を指定します。
ldap-login-password	ログイン DN のパスワードを指定します。

ldap-defaults

LDAP 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のみ使用されます。LDAP デフォルト値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

構文の説明

port	（任意）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、ASA は標準の LDAP ポート（389）を使用します。
サーバ	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

デフォルト設定は設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、デフォルト ポート（389）に LDAP デフォルト値を定義する例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(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 モードを開始します。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
protocol ldap	CRL の取得方法として LDAP を指定します。

ldap-dn

CRL 取得のために認証を要求する 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 サーバで必要な場合のみ使用されます。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

構文の説明

password	この認定者名のパスワードを定義します。最大のフィールドの長さは 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）。最大のフィールドの長さは 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

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、トラストポイント central の X.500 名として CN=admin,OU=devtest,O=engineering、パスワードとして xxzzyy を指定する例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(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 モードを開始します。
crypto ca trustpoint	CA トラストポイント コンフィギュレーション モードを開始します。
protocol ldap	CRL の取得方法として LDAP を指定します。

ldap-group-base-dn

ダイナミック アクセス ポリシーによってグループ検索に使用される Active Directory 階層の基本グループを指定するには、AAA サーバ ホスト コンフィギュレーション モードで **ldap-group-base-dn** コマンドを使用します。このコマンド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。

ldap-group-base-dn [*string*]

no ldap-group-base-dn [*string*]

構文の説明

string	サーバが検索を開始する Active Directory 階層内の位置を指定する、最大 128 文字のストリング。大文字と小文字は区別されます。たとえば、ou=Employees を指定します。文字列でスペースは使用できませんが、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。グループ検索 DN を指定しない場合、ベース DN から検索が開始されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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 モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

使用上のガイドライン

ldap-group-base-dn コマンドは、LDAP を使用する Active Directory サーバにのみ適用され、**show ad-groups** コマンドがグループ検索を開始するときに使用する Active Directory 階層レベルを指定します。検索で取得されたグループは、ダイナミック グループ ポリシーによって特定のポリシーの選択基準として使用されます。

例

次に、組織の部門（ou）レベルの Employees から検索を開始するようにグループ ベース DN を設定する例を示します。

```
ciscoasa(config-aaa-server-host)# ldap-group-base-dn ou=Employees
```

関連コマンド

コマンド	説明
group-search-timeout	グループのリストについて Active Directory サーバからの応答を ASA が待機する時間を調整します。
show ad-groups	Active Directory サーバ上でリストされるグループを表示します。

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 コンフィギュレーション 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

構文の説明

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 文字のストリング。大文字と小文字は区別されます。文字列でスペースは使用できませんが、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

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは LDAP サーバでのみ有効です。サポートされるストリングの最大長は 128 文字です。

Microsoft Active Directory サーバなどの一部の LDAP サーバでは、他の LDAP 動作の要求を受け入れる前に、ASA 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。ASA は、ログイン DN フィールドをユーザ認証要求にアタッチして、認証済みバインディングに対して識別情報を示します。ログイン DN フィールドには、ASA の認証特性が記述されます。これらの特性は、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のディレクトリ オブジェクト名を入力します（たとえば、cn=Administrator, cn=users, ou=people, dc=XYZ Corporation, dc=com）。匿名アクセスの場合は、このフィールドをブランクのままにします。

例

次に、ホスト 1.2.3.4 に svrgrp1 という名前の LDAP AAA サーバを設定し、タイムアウトを 9 秒、再試行間隔を 7 秒、LDAP ログイン DN を myobjectname に設定する例を示します。

```
ciscoasa(config)# aaa-server svrgrp1 protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa(config-aaa-server-host)# timeout 9
ciscoasa(config-aaa-server-host)# retry 7
ciscoasa(config-aaa-server-host)# ldap-login-dn myobjectname
ciscoasa(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 モードを開始し、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	サーバが認可要求を受信した場合に検索を開始する LDAP 階層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 サーバでのみ有効です。
ldap-naming-attribute	LDAP サーバ上のエントリを一意に識別する、1 つ以上の相対識別名属性を指定します。
ldap-scope	サーバが認可要求を受信した場合に検索する LDAP 階層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 コンフィギュレーション 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-password *string*

no ldap-login-password

構文の説明

string	最大 64 文字の英数字のパスワード。大文字と小文字は区別されます。パスワードにスペース文字を含めることはできません。

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

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは LDAP サーバでのみ有効です。パスワードの最大長は 64 文字です。

例

次に、ホスト 1.2.3.4 に srvgrp1 という名前の LDAP AAA サーバを設定し、タイムアウトを 9 秒、再試行間隔を 7 秒、LDAP ログイン パスワードを obscurepassword に設定する例を示します。

```
ciscoasa(config)# aaa-server svrgrp1 protocol ldap
ciscoasa(config)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa(config-aaa-server)# timeout 9
ciscoasa(config-aaa-server)# retry 7
ciscoasa(config-aaa-server)# ldap-login-password obscurepassword
ciscoasa(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 モードを開始し、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	サーバが認可要求を受信した場合に検索を開始する LDAP 階層の位置を指定します。
ldap-login-dn	システムがバインドするディレクトリ オブジェクト名を指定します。
ldap-naming-attribute	LDAP サーバ上のエントリを一意に識別する、1 つ以上の相対識別名属性を指定します。
ldap-scope	サーバが認可要求を受信した場合に検索する LDAP 階層の範囲を指定します。

ldap-naming-attribute

相対認定者名属性を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **ldap-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

構文の説明

string	LDAP サーバ上のエントリを一意に識別する、最大 128 文字の英数字の相対認定者名属性を指定します。大文字と小文字は区別されます。文字列でスペースは使用できませんが、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

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

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、相対認定者名属性を指定します。共通の命名属性は、一般名（cn）とユーザ ID（uid）です。

このコマンドは LDAP サーバでのみ有効です。サポートされるストリングの最大長は 128 文字です。

例

次に、ホスト 1.2.3.4 に srvgrp1 という名前の LDAP AAA サーバを設定し、タイムアウトを 9 秒、再試行間隔を 7 秒、LDAP 命名属性を cn に設定する例を示します。

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

```
ciscoasa(config-aaa-server-host)# ldap-naming-attribute cn
ciscoasa(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 モードを開始し、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	サーバが認可要求を受信した場合に検索を開始する LDAP 階層の位置を指定します。
ldap-login-dn	システムがバインドするディレクトリ オブジェクト名を指定します。
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 サーバでのみ有効です。
ldap-scope	サーバが認可要求を受信した場合に検索する LDAP 階層の範囲を指定します。

ldap-over-ssl

セキュアな SSL 接続を ASA と LDAP サーバの間で確立するには、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。接続の 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

構文の説明

enable	SSL で LDAP サーバへの接続を保護す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

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用して、SSL で ASA と LDAP サーバの間の接続を保護することを指定します。

(注) プレーン テキスト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

次に、AAA サーバ ホスト コンフィギュレーション モードで、ASA と LDAP サーバ ldapsvr1（IP アドレスは 10.10.0.1）の間の接続に対して SSL をイネーブルにするコマンドの例を示します。PLAIN SASL 認証メカニズムも設定します。

```
ciscoasa(config)# aaa-server ldapsvr1 protocol ldap
ciscoasa(config-aaa-server-host)# aaa-server ldapsvr1 host 10.10.0.1
ciscoasa(config-aaa-server-host)# ldap-over-ssl enable
ciscoasa(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 ベンダーに Microsoft または Sun のいずれかを指定します。
ldap attribute-map（グローバル コンフィギュレーション モード）	ユーザ定義の属性名を Cisco LDAP 属性名にマッピングするために、LDAP 属性マップを作成して名前を付けます。

ldap-scope

サーバが認可要求を受信したときに検索する 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

構文の説明

scope	サーバが認可要求を受信したときに検索する LDAP 階層内のレベルの数を指定します。有効な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 の下のレベルをすべて検索します。

デフォルト

デフォルト値は **onelevel** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

scope を **onelevel** と指定すると、ベース DN の 1 つ下のレベルのみが検索されるため、検索速度が向上します。**subtree** を指定すると、ベース DN の下のレベルがすべて検索されるため、検索速度が低下します。

このコマンドは LDAP サーバでのみ有効です。

例

次に、ホスト 1.2.3.4 に svrgrp1 という名前の LDAP AAA サーバを設定し、タイムアウトを 9 秒、再試行間隔を 7 秒、LDAP 範囲を subtree に設定する例を示します。

```
ciscoasa(config)# aaa-server svrgrp1 protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa(config-aaa-server-host)# timeout 9
```

```
ciscoasa(config-aaa-server-host)# retry 7
ciscoasa(config-aaa-server-host)# ldap-scope subtree
ciscoasa(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 モードを開始し、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	サーバが認可要求を受信した場合に検索を開始する LDAP 階層の位置を指定します。
ldap-login-dn	システムがバインドするディレクトリ オブジェクト名を指定します。
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 サーバでのみ有効です。
ldap-naming-attribute	LDAP サーバ上のエントリを一意に識別する、1 つ以上の相対識別名属性を指定します。

leap-bypass

LEAP バイパス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 バイパス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。実行コンフィギュレーションから LEAP バイパス属性を削除するには、このコマンドの **no** 形式を使用します。このオプションにより、別のグループ ポリシーから LEAP バイパスの値を継承できます。

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

no leap-bypass

構文の説明

disable	LEAP バイパスをディセーブルにします。
enable	LEAP バイパスをイネーブルにします。

デフォルト

LEAP バイパスはディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

LEAP バイパス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 パケットは、ユーザ認証の前に VPN トンネルを通過できます。これにより、シスコ ワイヤレス 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 認証を確立できるようになります。デバイスは、ユーザ認証ごとに認証を再実行できます。

インタラクティブ ハードウェア クライアント認証をイネーブルにした場合、この機能は正常に動作しません。

詳細については、CLI 設定ガイド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 リスクが発生する可能性があります。

例

次の例は、「FirstGroup」という名前のグループ ポリシーに対して LEAP バイパスを設定する方法を示しています。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(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 クライアントに、トンネルを開始するたび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 ASA に識別情報を示すように要求します。

license

要求の送信元の組織を示すために ASA からクラウド Web セキュリティ プロキシ サーバに送信する認証キーを設定するには、scansafe 汎用オプション コンフィギュレーション モードで **license** コマンドを使用します。ライセンスを削除するには、このコマンドの **no** 形式を使用します。

license *hex_key*

no license [*hex_key*]

構文の説明

hex_key	16 バイトの 16 進数の形式で認証キーを指定します。

コマンド 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

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

各 ASA は、クラウド Web セキュリティから取得した認証キーを使用する必要があります。認証キーを使用して、クラウド Web セキュリティは、Web 要求に関連付けられた会社を識別し、ASA が有効なカスタマーに関連付けられていることを確認できます。

ASA では、2 つの認証キー（企業キーおよびグループ キー）のいずれかを使用できます。

企業認証キー

企業認証キーは、企業内の複数の ASA で使用できます。このキーは、単に ASA のクラウド Web セキュリティ サービスをイネーブルにします。管理者は ScanCenter（https://scancenter.scansafe.com/portal/admin/login.jsp）でこのキーを生成します。後で使用するためにこのキーを電子メールで送信できます。ScanCenter では、後でこのキーを検索できません。ScanCenter には、最後の 4 桁だけが表示されます。詳細については、クラウド Web セキュリティのマニュアルを参照してください。マニュアルは、http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html から入手できます。

グループ認証キー

グループ認証キーは 2 つの機能を実行する各 ASA に固有の特別なキーです。

- 1 つの ASA のクラウド Web セキュリティ サービスをイネーブルにします。
- ASA からのすべてのトラフィックが識別されるため、ASA ごとに ScanCenter ポリシーを作成できます。

管理者は ScanCenter（https://scancenter.scansafe.com/portal/admin/login.jsp）でこのキーを生成します。後で使用するためにこのキーを電子メールで送信できます。ScanCenter では、後でこのキーを検索できません。ScanCenter には、最後の 4 桁だけが表示されます。詳細については、クラウド Web セキュリティのマニュアルを参照してください。マニュアルは、http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html から入手できます。

例

次に、プライマリ サーバのみを設定する例を示します。

```
scansafe general-options
 server primary ip 180.24.0.62 port 8080
 retry-count 5
 license 366C1D3F5CE67D33D3E9ACEC265261E5
```

関連コマンド

コマンド	説明
class-map type inspect scansafe	ホワイトリストに記載されたユーザとグループのインスペクション クラス マップを作成します。
default user group	ASA に入ってくるユーザのアイデンティティを ASA が判別できない場合のデフォルトのユーザ名やグループを指定します。
http[s]（パラメータ）	インスペクション ポリシー マップのサービス タイプ（HTTP または HTTPS）を指定します。
inspect scansafe	このクラスのトラフィックに対するクラウド Web セキュリティ インスペクションをイネーブルにします。
match user group	ユーザまたはグループをホワイトリストと照合します。
policy-map type inspect scansafe	インスペクション ポリシー マップを作成すると、ルールのために必要なパラメータを設定し、任意でホワイトリストを識別できます。
retry-count	再試行回数値を入力します。この値は、可用性をチェックするために、クラウド Web セキュリティ プロキシ サーバをポーリングする前に ASA が待機する時間です。
scansafe	マルチ コンテキスト モードでは、コンテキストごとにクラウド Web セキュリティを許可します。
scansafe general-options	汎用クラウド Web セキュリティ サーバ オプションを設定します。
server {primary | backup}	プライマリまたはバックアップのクラウド Web セキュリティ プロキシ サーバの完全修飾ドメイン名または IP アドレスを設定します。
show conn scansafe	大文字の Z フラグに示されたようにすべてのクラウド Web セキュリティ接続を表示します。
show scansafe server	サーバが現在のアクティブ サーバ、バックアップ サーバ、または到達不能のいずれであるか、サーバのステータスを表示します。

コマンド	説明
show scansafe statistics	合計と現在の http 接続を表示します。
user-identity monitor	AD エージェントから指定したユーザまたはグループ情報をダウンロードします。
ホワイトリスト	トラフィックのクラスでホワイトリスト アクションを実行します。

license-server address

参加ユニットが使用する共有ライセンス サーバの IP アドレスと共有秘密を指定するには、グローバル コンフィギュレーション モードで **license-server address** コマンドを使用します。共有ライセンスへの参加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。共有ライセンスを使用すると、多数の SSL VPN セッションの購入および ASA のグループ間で必要に応じてセッションを共有できます。共有には、ASA のうち 1 台を共有ライセンス サーバに、また残りを共有ライセンス参加者として設定します。

license-server address *address* **secret** *secret* [**port** *port*]

no license-server address [*address* **secret** *secret* [**port** *port*]]

構文の説明

address	共有ライセンス サーバの IP アドレスを指定します。
port *port*	(任意)**license-server port** コマンドを使用してサーバ コンフィギュレーションのデフォルト ポートを変更した場合は、それに合わせてバックアップ サーバのポートを設定します(1 ～ 65535)。デフォルトのポートは 50554 です。
secret *secret*	共有秘密を指定します。共有秘密は、**license-server secret** コマンドを使用してサーバに設定された秘密と一致する必要があります。

コマンド デフォルト

デフォルトのポートは 50554 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

共有ライセンス参加ユニットには、共有ライセンス参加キーが必要です。インストールされているライセンスを確認するには、**show activation-key** コマンドを使用します。

参加ユニットごとに共有ライセンス サーバを 1 つのみ指定できます。

次に、共有ライセンスの動作手順を示します。

1. いずれの ASA を共有ライセンス サーバとするかを決定し、デバイス シリアル番号を使用する共有ライセンス サーバのライセンスを購入します。
2. いずれの ASA を共有ライセンス バックアップ サーバを含む共有ライセンス参加者とするかを決定し、各デバイス シリアル番号を使用して各デバイスに対して共有ライセンス参加ライセンスを取得します。
3. （任意）別の ASA を共有ライセンス バックアップ サーバとして指定します。バックアップ サーバには 1 台のみ指定できます。

   （注） 共有ライセンス バックアップ サーバに必要なのは参加ライセンスのみです。

4. 共有ライセンス サーバ上に共有秘密を設定します。共有秘密を保持する参加者であればいずれも共有ライセンスを使用できます。
5. ASA を参加者として設定する場合、ローカル ライセンスおよびモデル情報を含む自身の情報を送信することで共有ライセンス サーバに登録します。

   （注） 参加者は IP ネットワークを経由してサーバと通信できる必要がありますが、同じサブネット上にある必要はありません。

6. 共有ライセンス サーバは、参加者がサーバにポーリングするべき頻度の情報で応答します。
7. 参加者がローカル ライセンスのセッションを使い果たした場合、参加者は共有ライセンス サーバに 50 セッション単位で追加セッションの要求を送信します。
8. 共有ライセンス サーバは、共有ライセンスで応答します。1 台の参加者が使用する合計セッション数は、プラットフォーム モデルの最大セッション数を超えられません。

   （注） 共有ライセンスサーバは、ローカル セッションを使い果たした場合に共有ライセンス プールに参加もできます。参加には参加ライセンスもサーバ ライセンスも必要ありません。

   a. 参加者に対して共有ライセンス プールに十分なセッションがない場合、サーバは使用可能な限りのセッション数で応答します。
   b. 参加者はさらなるセッションを要求するリフレッシュ メッセージの送信をサーバが要求に適切に対応できるまで続けます。
9. 参加者の負荷が減少した場合、参加者はサーバに共有セッションを解放するようにメッセージを送信します。

（注） ASA は、サーバと参加者間のすべての通信の暗号化に SSL を使用します。

参加システムとサーバの間の通信に関する問題

参加者とサーバ間の通信問題については、次のガイドラインを参照してください。

- 参加者が更新の送信に失敗して更新間隔 3 倍の時間が経過した後で、サーバはセッションを解放して共有ライセンス プールに戻します。
- 参加者が更新を送信するためにライセンス サーバに到達できない場合、参加者はサーバから受信した共有ライセンスを最大 24 時間使用し続けられます。

- 24 時間を経過しても参加者がまだライセンス サーバと通信できない場合、参加者はセッションがまだ必要であっても共有ライセンスを解放します。参加者は既存の確立している接続を維持しますが、ライセンス制限を超えて新しい接続を受け入れられません。
- 参加者が 24 時間経過前にサーバに再接続したが、サーバが参加セッションを期限切れにした後である場合、参加者はセッションに対する新しい要求を送信する必要があります。サーバは、参加者に再割り当てできる限りのセッション数で応答します。

例

次に、ライセンス サーバの IP アドレスおよび共有秘密、ならびにバックアップ ライセンス サーバの IP アドレスの設定例を示します。

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup address 10.1.1.2
```

関連コマンド

コマンド	説明
activation-key	ライセンス アクティベーション キーを入力します。
clear configure license-server	共有ライセンス サーバ コンフィギュレーションをクリアします。
clear shared license	共有ライセンス統計情報をクリアします。
license-server backup address	参加者の共有ライセンス バックアップ サーバを指定します。
license-server backup backup-id	メインの共有ライセンス サーバのバックアップ サーバの IP アドレスおよびシリアル番号を指定します。
license-server backup enable	共有ライセンス バックアップ サーバになるユニットをイネーブルにします。
license-server enable	共有ライセンス サーバになるユニットをイネーブルにします。
license-server port	サーバが参加者からの SSL 接続をリッスンするポートを設定します。
license-server refresh-interval	サーバと通信する頻度を設定するために参加者に提供される更新間隔を設定します。
license-server secret	共有秘密を共有ライセンス サーバに設定します。
show activation-key	インストールされている現在のライセンスを表示します。
show running-config license-server	共有ライセンス サーバ コンフィギュレーションを表示します。
show shared license	共有ライセンス統計情報を表示します。
show vpn-sessiondb	VPN セッションのライセンス情報を表示します。

license-server backup address

参加ユニットが使用する共有ライセンス バックアップ サーバの IP アドレスを指定するには、グローバル コンフィギュレーション モードで **license-server backup address** コマンドを使用します。バックアップ サーバの使用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。

license-server backup address *address*

no license-server address [*address*]

構文の説明

address	共有ライセンス バックアップ サーバの IP アドレスを指定します。

コマンド 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

次の表に、コマンドを入力できるモードを示します。

コマンド モード	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	
	ルーテッド	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

共有ライセンス バックアップ サーバには、**license-server backup enable** コマンドが設定されている必要があります。

例

次に、ライセンス サーバの IP アドレスおよび共有秘密、ならびにバックアップ ライセンス サーバの IP アドレスの設定例を示します。

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup address 10.1.1.2
```

関連コマンド

コマンド	説明
activation-key	ライセンス アクティベーション キーを入力します。
clear configure license-server	共有ライセンス サーバ コンフィギュレーションをクリアします。
clear shared license	共有ライセンス統計情報をクリアします。
license-server address	共有ライセンス サーバの IP アドレスと参加者の共有秘密を指定します。
license-server backup backup-id	メインの共有ライセンス サーバのバックアップ サーバの IP アドレスおよびシリアル番号を指定します。
license-server backup enable	共有ライセンス バックアップ サーバになるユニットをイネーブルにします。
license-server enable	共有ライセンス サーバになるユニットをイネーブルにします。
license-server port	サーバが参加者からの SSL 接続をリッスンするポートを設定します。
license-server refresh-interval	サーバと通信する頻度を設定するために参加者に提供される更新間隔を設定します。
license-server secret	共有秘密を共有ライセンス サーバに設定します。
show activation-key	インストールされている現在のライセンスを表示します。
show running-config license-server	共有ライセンス サーバ コンフィギュレーションを表示します。
show shared license	共有ライセンス統計情報を表示します。
show vpn-sessiondb	VPN セッションのライセンス情報を表示します。

license-server backup backup-id

メイン共有ライセンス サーバ コンフィギュレーションで共有ライセンス バックアップ サーバを指定するには、グローバル コンフィギュレーション モードで **license-server backup backup-id** コマンドを使用します。バックアップ サーバ コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

license-server backup *address* **backup-id** *serial_number* [**ha-backup-id** *ha_serial_number*]

no license-server backup *address* [**backup-id** *serial_number* [**ha-backup-id** *ha_serial_number*]]

構文の説明

address	共有ライセンス バックアップ サーバの IP アドレスを指定します。
backup-id *serial_number*	共有ライセンス バックアップ サーバのシリアル番号を指定します。
ha-backup-id *ha_serial_number*	バックアップ サーバでフェールオーバーを使用する場合は、セカンダリ共有ライセンス バックアップ サーバのシリアル番号を指定します。

コマンド 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

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

1 つのバックアップ サーバとそのオプションのスタンバイ ユニットのみを指定できます。

バックアップ サーバのシリアル番号を表示するには、**show activation-key** コマンドを入力します。

参加ユニットをバックアップ サーバとしてイネーブルにするには、**license-server backup enable** コマンドを使用します。

共有ライセンス バックアップ サーバは、バックアップの役割を実行する前にメインの共有ライセンス サーバへの登録に成功している必要があります。登録時には、メインの共有ライセンス サーバは共有ライセンス情報に加えてサーバ設定もバックアップと同期します。情報には、登録済み参加者の一覧および現在のライセンス使用状況が含まれます。メイン サーバとバックアップ サーバは、10 秒間隔でデータを同期します。初回同期の後で、バックアップ サーバはリロード後でもバックアップの役割を実行できます。

メイン サーバがダウンすると、バックアップ サーバがサーバ動作を引き継ぎます。バックアップ サーバは継続して最大 30 日間動作できます。30 日を超えると、バックアップ サーバは参加者へのセッション発行を中止し、既存のセッションはタイムアウトします。メイン サーバをこの 30 日間中に確実に復旧するようにします。クリティカル レベルの syslog メッセージが 15 日めに送信され、30 日めに再送信されます。

メイン サーバが復旧した場合、メイン サーバはバックアップ サーバと同期してから、サーバ動作を引き継ぎます。

バックアップ サーバがアクティブでないときは、メインの共有ライセンス サーバの通常の参加者として動作します。

（注） メインの共有ライセンス サーバの初回起動時には、バックアップ サーバは独立して 5 日間のみ動作できます。動作制限は 30 日に到達するまで日ごとに増加します。また、メイン サーバがその後短時間でもダウンした場合、バックアップ サーバの動作制限は日ごとに減少します。メイン サーバが復旧した場合、バックアップ サーバは再び日ごとに増加を開始します。たとえば、メイン サーバが 20 日間ダウンしていて、その期間中バックアップ サーバがアクティブであった場合、バックアップ サーバには、10 日間の制限のみが残っています。バックアップ サーバは、非アクティブなバックアップとしてさらに 20 日間が経過した後で、最大の 30 日間まで「充電」されます。この充電機能は共有ライセンスの誤使用を防ぐために実装されています。

例

次に、共有秘密を設定し、更新間隔とポートを変更し、バックアップ サーバを設定し、このユニットを inside インターフェイスおよび dmz インターフェイスで共有ライセンス サーバとしてイネーブルにする例を示します。

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

関連コマンド

コマンド	説明
activation-key	ライセンス アクティベーション キーを入力します。
clear configure license-server	共有ライセンス サーバ コンフィギュレーションをクリアします。
clear shared license	共有ライセンス統計情報をクリアします。
license-server address	共有ライセンス サーバの IP アドレスと参加者の共有秘密を指定します。
license-server backup address	参加者の共有ライセンス バックアップ サーバを指定します。
license-server backup enable	共有ライセンス バックアップ サーバになるユニットをイネーブルにします。

コマンド	説明
license-server enable	共有ライセンス サーバになるユニットをイネーブルにします。
license-server port	サーバが参加者からの SSL 接続をリッスンするポートを設定します。
license-server refresh-interval	サーバと通信する頻度を設定するために参加者に提供される更新間隔を設定します。
license-server secret	共有秘密を共有ライセンス サーバに設定します。
show activation-key	インストールされている現在のライセンスを表示します。
show running-config license-server	共有ライセンス サーバ コンフィギュレーションを表示します。
show shared license	共有ライセンス統計情報を表示します。
show vpn-sessiondb	VPN セッションのライセンス情報を表示します。

license-server backup enable

このユニットを共有ライセンス バックアップ サーバとしてイネーブルにするには、グローバル コンフィギュレーション モードで **license-server backup enable** コマンドを使用します。バックアップ サーバ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。

license-server backup enable *interface_name*

no license-server enable *interface_name*

構文の説明

interface_name	参加ユニットがバックアップ サーバとの通信に使用するインターフェイスを指定します。このコマンドは必要なインターフェイスの数だけ繰り返せます。

コマンド 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

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

バックアップ サーバには、共有ライセンス参加キーが必要です。

共有ライセンス バックアップ サーバは、バックアップの役割を実行する前にメインの共有ライセンス サーバへの登録に成功している必要があります。登録時には、メインの共有ライセンス サーバは共有ライセンス情報に加えてサーバ設定もバックアップと同期します。情報には、登録済み参加者の一覧および現在のライセンス使用状況が含まれます。メイン サーバとバックアップ サーバは、10 秒間隔でデータを同期します。初回同期の後で、バックアップ サーバはリロード後でもバックアップの役割を実行できます。

メイン サーバがダウンすると、バックアップ サーバがサーバ動作を引き継ぎます。バックアップ サーバは継続して最大 30 日間動作できます。30 日を超えると、バックアップ サーバは参加者へのセッション発行を中止し、既存のセッションはタイムアウトします。メイン サーバをこの 30 日間中に確実に復旧するようにします。クリティカル レベルの syslog メッセージが 15 日めに送信され、30 日めに再送信されます。

メイン サーバが復旧した場合、メイン サーバはバックアップ サーバと同期してから、サーバ動作を引き継ぎます。

バックアップ サーバがアクティブでないときは、メインの共有ライセンス サーバの通常の参加者として動作します。

(注) メインの共有ライセンス サーバの初回起動時には、バックアップ サーバは独立して 5 日間のみ動作できます。動作制限は 30 日に到達するまで日ごとに増加します。また、メイン サーバがその後短時間でもダウンした場合、バックアップ サーバの動作制限は日ごとに減少します。メイン サーバが復旧した場合、バックアップ サーバは再び日ごとに増加を開始します。たとえば、メイン サーバが 20 日間ダウンしていて、その期間中バックアップ サーバがアクティブであった場合、バックアップ サーバには、10 日間の制限のみが残っています。バックアップ サーバは、非アクティブなバックアップとしてさらに 20 日間が経過した後で、最大の 30 日間まで「充電」されます。この充電機能は共有ライセンスの誤使用を防ぐために実装されています。

例

次に、ライセンス サーバと共有秘密を指定し、このユニットを内部インターフェイスと dmz インターフェイス上のバックアップ共有ライセンス サーバとしてイネーブルにする例を示します。

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup enable inside
ciscoasa(config)# license-server backup enable dmz
```

関連コマンド

コマンド	説明
activation-key	ライセンス アクティベーション キーを入力します。
clear configure license-server	共有ライセンス サーバ コンフィギュレーションをクリアします。
clear shared license	共有ライセンス統計情報をクリアします。
license-server address	共有ライセンス サーバの IP アドレスと参加者の共有秘密を指定します。
license-server backup address	参加者の共有ライセンス バックアップ サーバを指定します。
license-server backup backup-id	メインの共有ライセンス サーバのバックアップ サーバの IP アドレスおよびシリアル番号を指定します。
license-server enable	共有ライセンス サーバになるユニットをイネーブルにします。
license-server port	サーバが参加者からの SSL 接続をリッスンするポートを設定します。
license-server refresh-interval	サーバと通信する頻度を設定するために参加者に提供される更新間隔を設定します。
license-server secret	共有秘密を共有ライセンス サーバに設定します。
show activation-key	インストールされている現在のライセンスを表示します。
show running-config license-server	共有ライセンス サーバ コンフィギュレーションを表示します。
show shared license	共有ライセンス統計情報を表示します。
show vpn-sessiondb	VPN セッションのライセンス情報を表示します。

license-server enable

このユニットを共有ライセンス サーバとして指定するには、グローバル コンフィギュレーション モードで **license-server enable** コマンドを使用します。共有ライセンス サーバ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。共有ライセンスを使用すると、多数の SSL VPN セッションの購入および ASA のグループ間で必要に応じてセッションを共有できます。共有には、ASA のうち 1 台を共有ライセンス サーバに、また残りを共有ライセンス参加者として設定します。

license-server enable *interface_name*

no license-server enable *interface_name*

構文の説明

interface_name	参加ユニットがサーバとの通信に使用するインターフェイスを指定します。このコマンドは必要なインターフェイスの数だけ繰り返せます。

コマンド 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

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

共有ライセンス サーバには、共有ライセンス サーバ キーが必要です。インストールされているライセンスを確認するには、**show activation-key** コマンドを使用します。

次に、共有ライセンスの動作手順を示します。

1. いずれの ASA を共有ライセンス サーバとするかを決定し、デバイス シリアル番号を使用する共有ライセンス サーバのライセンスを購入します。
2. いずれの ASA を共有ライセンス バックアップ サーバを含む共有ライセンス参加者とするかを決定し、各デバイス シリアル番号を使用して各デバイスに対して共有ライセンス参加ライセンスを取得します。

3. (任意)別の ASA を共有ライセンス バックアップ サーバとして指定します。バックアップ サーバには 1 台のみ指定できます。

(注) 共有ライセンス バックアップ サーバに必要なのは参加ライセンスのみです。

4. 共有ライセンス サーバ上に共有秘密を設定します。共有秘密を保持する参加者であればいずれも共有ライセンスを使用できます。
5. ASA を参加者として設定する場合、ローカル ライセンスおよびモデル情報を含む自身の情報を送信することで共有ライセンス サーバに登録します。

(注) 参加者は IP ネットワークを経由してサーバと通信できる必要がありますが、同じサブネット上にある必要はありません。

6. 共有ライセンス サーバは、参加者がサーバにポーリングするべき頻度の情報で応答します。
7. 参加者がローカル ライセンスのセッションを使い果たした場合、参加者は共有ライセンス サーバに 50 セッション単位で追加セッションの要求を送信します。
8. 共有ライセンス サーバは、共有ライセンスで応答します。1 台の参加者が使用する合計セッション数は、プラットフォーム モデルの最大セッション数を超えられません。

(注) 共有ライセンスサーバは、ローカル セッションを使い果たした場合に共有ライセンス プールに参加もできます。参加には参加ライセンスもサーバ ライセンスも必要ありません。

   a. 参加者に対して共有ライセンス プールに十分なセッションがない場合、サーバは使用可能な限りのセッション数で応答します。
   b. 参加者はさらなるセッションを要求するリフレッシュ メッセージの送信をサーバが要求に適切に対応できるまで続けます。
9. 参加者の負荷が減少した場合、参加者はサーバに共有セッションを解放するようにメッセージを送信します。

(注) ASA は、サーバと参加者間のすべての通信の暗号化に SSL を使用します。

参加システムとサーバの間の通信に関する問題

参加者とサーバ間の通信問題については、次のガイドラインを参照してください。

- 参加者が更新の送信に失敗して更新間隔 3 倍の時間が経過した後で、サーバはセッションを解放して共有ライセンス プールに戻します。
- 参加者が更新を送信するためにライセンス サーバに到達できない場合、参加者はサーバから受信した共有ライセンスを最大 24 時間使用し続けられます。
- 24 時間を経過しても参加者がまだライセンス サーバと通信できない場合、参加者はセッションがまだ必要であっても共有ライセンスを解放します。参加者は既存の確立している接続を維持しますが、ライセンス制限を超えて新しい接続を受け入れられません。
- 参加者が 24 時間経過前にサーバに再接続したが、サーバが参加セッションを期限切れにした後である場合、参加者はセッションに対する新しい要求を送信する必要があります。サーバは、参加者に再割り当てできる限りのセッション数で応答します。

例

次に、共有秘密を設定し、更新間隔とポートを変更し、バックアップ サーバを設定し、このユニットを inside インターフェイスおよび DMZ インターフェイスで共有ライセンス サーバとしてイネーブルにする例を示します。

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

関連コマンド

コマンド	説明
activation-key	ライセンス アクティベーション キーを入力します。
clear configure license-server	共有ライセンス サーバ コンフィギュレーションをクリアします。
clear shared license	共有ライセンス統計情報をクリアします。
license-server address	共有ライセンス サーバの IP アドレスと参加者の共有秘密を指定します。
license-server backup address	参加者の共有ライセンス バックアップ サーバを指定します。
license-server backup backup-id	メインの共有ライセンス サーバのバックアップ サーバの IP アドレスおよびシリアル番号を指定します。
license-server backup enable	共有ライセンス バックアップ サーバになるユニットをイネーブルにします。
license-server port	サーバが参加者からの SSL 接続をリッスンするポートを設定します。
license-server refresh-interval	サーバと通信する頻度を設定するために参加者に提供される更新間隔を設定します。
license-server secret	共有秘密を共有ライセンス サーバに設定します。
show activation-key	インストールされている現在のライセンスを表示します。
show running-config license-server	共有ライセンス サーバ コンフィギュレーションを表示します。
show shared license	共有ライセンス統計情報を表示します。
show vpn-sessiondb	VPN セッションのライセンス情報を表示します。

license-server port

共有ライセンス サーバが参加ユニットからの SSL 接続をリッスンするポートを設定するには、グローバル コンフィギュレーション モードで **license-server port** コマンドを使用します。デフォルト ポートに戻すには、このコマンドの **no** 形式を使用します。

license-server port *port*

no license-server port [*port*]

構文の説明

seconds	参加ユニットからの SSL 接続をサーバがリッスンするポート（1 ～ 65535）を設定します。デフォルトは、TCP ポート 50554 です。

コマンド デフォルト

デフォルトのポートは 50554 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

デフォルト ポートを変更する場合は、**license-server address** コマンドを使用して、各参加ユニットに同じポートを設定してください。

例

次に、共有秘密を設定し、更新間隔とポートを変更し、バックアップ サーバを設定し、このユニットを inside インターフェイスおよび DMZ インターフェイスで共有ライセンス サーバとしてイネーブルにする例を示します。

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

関連コマンド

コマンド	説明
activation-key	ライセンス アクティベーション キーを入力します。
clear configure license-server	共有ライセンス サーバ コンフィギュレーションをクリアします。
clear shared license	共有ライセンス統計情報をクリアします。
license-server address	共有ライセンス サーバの IP アドレスと参加者の共有秘密を指定します。
license-server backup address	参加者の共有ライセンス バックアップ サーバを指定します。
license-server backup backup-id	メインの共有ライセンス サーバのバックアップ サーバの IP アドレスおよびシリアル番号を指定します。
license-server backup enable	共有ライセンス バックアップ サーバになるユニットをイネーブルにします。
license-server enable	共有ライセンス サーバになるユニットをイネーブルにします。
license-server refresh-interval	サーバと通信する頻度を設定するために参加者に提供される更新間隔を設定します。
license-server secret	共有秘密を共有ライセンス サーバに設定します。
show activation-key	インストールされている現在のライセンスを表示します。
show running-config license-server	共有ライセンス サーバ コンフィギュレーションを表示します。
show shared license	共有ライセンス統計情報を表示します。
show vpn-sessiondb	VPN セッションのライセンス情報を表示します。

license-server refresh-interval

参加ユニットが共有ライセンス サーバと通信する頻度を設定するために参加ユニットに提供されるリフレッシュ間隔を設定するには、グローバル コンフィギュレーション モードで **license-server refresh-interval** コマンドを使用します。デフォルトのリフレッシュ間隔に戻すには、このコマンドの **no** 形式を使用します。

license-server refresh-interval *seconds*

no license-server refresh-interval [*seconds*]

構文の説明

seconds	リフレッシュ間隔（10 ～ 300 秒）を設定します。デフォルトは 30 秒です。

コマンド デフォルト

デフォルトは 30 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	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	
	ルーテッド	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

各参加ユニットは、SSL を使用して定期的に共有ライセンス サーバと通信します。そのため、共有ライセンス サーバは現在のライセンス使用状況を把握し、ライセンス要求を受信したりライセンス要求に応答できます。

例

次に、共有秘密を設定し、更新間隔とポートを変更し、バックアップ サーバを設定し、このユニットを inside インターフェイスおよび dmz インターフェイスで共有ライセンス サーバとしてイネーブルにする例を示します。

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

関連コマンド

コマンド	説明
activation-key	ライセンス アクティベーション キーを入力します。
clear configure license-server	共有ライセンス サーバ コンフィギュレーションをクリアします。
clear shared license	共有ライセンス統計情報をクリアします。
license-server address	共有ライセンス サーバの IP アドレスと参加者の共有秘密を指定します。
license-server backup address	参加者の共有ライセンス バックアップ サーバを指定します。
license-server backup backup-id	メインの共有ライセンス サーバのバックアップ サーバの IP アドレスおよびシリアル番号を指定します。
license-server backup enable	共有ライセンス バックアップ サーバになるユニットをイネーブルにします。
license-server enable	共有ライセンス サーバになるユニットをイネーブルにします。
license-server port	サーバが参加者からの SSL 接続をリッスンするポートを設定します。
license-server secret	共有秘密を共有ライセンス サーバに設定します。
show activation-key	インストールされている現在のライセンスを表示します。
show running-config license-server	共有ライセンス サーバ コンフィギュレーションを表示します。
show shared license	共有ライセンス統計情報を表示します。
show vpn-sessiondb	VPN セッションのライセンス情報を表示します。

license-server secret

共有ライセンス サーバに共有秘密を設定するには、グローバル コンフィギュレーション モードで **license-server secret** コマンドを使用します。共有秘密を削除するには、このコマンドの **no** 形式を使用します。

license-server secret *secret*

no license-server secret *secret*

構文の説明

secret	共有秘密を 4 ～ 128 文字の ASCII 文字のストリングで設定します。

コマンド 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

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

この共有秘密を持つ、**license-server address** コマンドで指定された参加ユニットは、ライセンス サーバを使用できます。

例

次に、共有秘密を設定し、更新間隔とポートを変更し、バックアップ サーバを設定し、このユニットを inside インターフェイスおよび dmz インターフェイスで共有ライセンス サーバとしてイネーブルにする例を示します。

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

関連コマンド

コマンド	説明
activation-key	ライセンス アクティベーション キーを入力します。
clear configure license-server	共有ライセンス サーバ コンフィギュレーションをクリアします。
clear shared license	共有ライセンス統計情報をクリアします。
license-server address	共有ライセンス サーバの IP アドレスと参加者の共有秘密を指定します。
license-server backup address	参加者の共有ライセンス バックアップ サーバを指定します。
license-server backup backup-id	メインの共有ライセンス サーバのバックアップ サーバの IP アドレスおよびシリアル番号を指定します。
license-server backup enable	共有ライセンス バックアップ サーバになるユニットをイネーブルにします。
license-server enable	共有ライセンス サーバになるユニットをイネーブルにします。
license-server port	サーバが参加者からの SSL 接続をリッスンするポートを設定します。
license-server refresh-interval	サーバと通信する頻度を設定するために参加者に提供される更新間隔を設定します。
show activation-key	インストールされている現在のライセンスを表示します。
show running-config license-server	共有ライセンス サーバ コンフィギュレーションを表示します。
show shared license	共有ライセンス統計情報を表示します。
show vpn-sessiondb	VPN セッションのライセンス情報を表示します。

license smart

スマート ライセンス資格要求を設定するには、グローバル コンフィギュレーション モードで **license smart** コマンドを使用します。資格を削除してデバイスのライセンスを解除するには、このコマンドの **no** 形式を使用します。

(注) この機能は、ASAv および Firepower シャーシのみでサポートされています。

license smart

no license smart

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド 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

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドは、ASAv のサポートのために追加されました。
9.4(1.152)	Firepower 9300 のサポートが追加されました。
9.6(1)	Firepower 4100 シリーズのサポートが追加されました。
9.8(2)	Firepower 2100 シリーズのサポートが追加されました。

使用上のガイドライン

このコマンドを使用すると、ライセンス スマート コンフィギュレーション モードになり、機能層やその他のライセンス資格を設定できます。ASAv の場合、初めて権限付与を要求したときは、変更を有効にするためにライセンス スマート コンフィギュレーション モードを終了する必要があります。

例

次に、機能層を標準に設定し、スループット レベルを 2G に設定する例を示します。

```
ciscoasa# license smart
ciscoasa(config-smart-lic)# feature tier standard
ciscoasa(config-smart-lic)# throughput level 2G
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

関連コマンド

コマンド	説明
call-home	Smart Call Home を設定します。スマート ライセンスでは、Smart Call Home インフラストラクチャが使用されます。
clear configure license	スマート ライセンス設定をクリアします。
feature tier	スマート ライセンスの機能層を設定します。
http-proxy	スマート ライセンスおよび Smart Call Home の HTTP(S) プロキシを設定します。
license smart deregister	ライセンス認証局からデバイスを登録解除します。
license smart register	デバイスをライセンス認証局に登録します。
license smart renew	登録またはライセンス権限を更新します。
service call-home	Smart Call Home をイネーブルにします。
show license	スマート ライセンスのステータスを表示します。
show running-config license	スマート ライセンスの設定を表示します。
throughput level	スマート ライセンスのスループット レベルを設定します。

license smart deregister

Cisco License Authority に対するデバイスのスマート ライセンス登録を解除するには、特権 EXEC モードで **license smart deregister** コマンドを使用します。

(注) この機能は、ASAv および Firepower 2100 だけでサポートされています。

license smart deregister

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド 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

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドは、ASAv のサポートのために追加されました。
9.8(2)	Firepower 2100 シリーズのサポートが追加されました。

使用上のガイドライン

ASA の登録を解除すると、アカウントから ASA が削除されます。ASA のすべてのライセンス権限付与と証明書が削除されます。登録を解除することで、ライセンスを新しい ASA に利用することもできます。このコマンドを実行すると、ASA がリロードします。

例

次に、デバイスの登録を解除する例を示します。

```
ciscoasa# license smart deregister
```

関連コマンド

コマンド	説明
call-home	Smart Call Home を設定します。スマート ライセンスでは、Smart Call Home インフラストラクチャが使用されます。
clear configure license	スマート ライセンス設定をクリアします。
feature tier	スマート ライセンスの機能層を設定します。
http-proxy	スマート ライセンスおよび Smart Call Home の HTTP(S) プロキシを設定します。
license smart	スマート ライセンスのライセンス権限付与を要求できます。
license smart register	デバイスをライセンス認証局に登録します。
license smart renew	登録またはライセンス権限を更新します。
service call-home	Smart Call Home をイネーブルにします。
show license	スマート ライセンスのステータスを表示します。
show running-config license	スマート ライセンスの設定を表示します。
throughput level	スマート ライセンスのスループット レベルを設定します。

license smart register

Cisco License Authority に対するデバイスのスマート ライセンス登録を行うには、特権 EXEC モードで **license smart register** コマンドを使用します。

(注) この機能は、ASAv および Firepower 2100 だけでサポートされています。

license smart register idtoken *id_token* [**force**]

構文の説明

idtoken *id_token*	Smart Software Manager で、この ASA を追加するバーチャル アカウントの登録トークンを要求してコピーします。
force	License Authority と同期されていない可能性がある登録済みの ASA を登録します。

コマンド 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

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドは、ASAv のサポートのために追加されました。
9.8(2)	Firepower 2100 シリーズのサポートが追加されました。

使用上のガイドライン

License Authority に ASA を登録すると、ASA と License Authority の間の通信に使用する ID 証明書が発行されます。また、該当するバーチャル アカウントに ASA が割り当てられます。通常、この手順は 1 回で済みます。ただし、通信の問題などが原因でアイデンティティ証明書の期限が切れた場合は、ASA の再登録が必要になります。

例

次に、登録トークンを使用して登録を行う例を示します。

```
ciscoasa# license smart register idtoken
YjE3Njc5MzYtMGQzMi00OTA4LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQkd
YRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

関連コマンド

コマンド	説明
call-home	Smart Call Home を設定します。スマート ライセンスでは、Smart Call Home インフラストラクチャが使用されます。
clear configure license	スマート ライセンス設定をクリアします。
feature tier	スマート ライセンスの機能層を設定します。
http-proxy	スマート ライセンスおよび Smart Call Home の HTTP(S) プロキシを設定します。
license smart	スマート ライセンスのライセンス権限付与を要求できます。
license smart deregister	ライセンス認証局からデバイスを登録解除します。
license smart renew	登録またはライセンス権限を更新します。
service call-home	Smart Call Home をイネーブルにします。
show license	スマート ライセンスのステータスを表示します。
show running-config license	スマート ライセンスの設定を表示します。
throughput level	スマート ライセンスのスループット レベルを設定します。

license smart renew

スマート ライセンスの登録またはライセンス資格の認証を更新するには、特権 EXEC モードで **license smart renew** コマンドを使用します。

(注) この機能は、ASAv および Firepower 2100 だけでサポートされています。

license smart renew {id | auth}

構文の説明

id	デバイスの登録を更新します。
auth	ライセンス資格を更新します。

コマンド 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

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドは、ASAv のサポートのために追加されました。
9.8(2)	Firepower 2100 シリーズのサポートが追加されました。

使用上のガイドライン

デフォルトでは、アイデンティティ証明書は 6 ヵ月ごと、ライセンス資格は 30 日ごとに自動的に更新されます。インターネット アクセスの期間が限られている場合や、Smart Software Manager でライセンスを変更した場合などは、これらの登録を手動で更新することもできます。

例

次に、登録とライセンスの両方の認証を更新する例を示します。

```
ciscoasa# license smart renew id
ciscoasa# license smart renew auth
```

関連コマンド

コマンド	説明
call-home	Smart Call Home を設定します。スマート ライセンスでは、Smart Call Home インフラストラクチャが使用されます。
clear configure license	スマート ライセンス設定をクリアします。
feature tier	スマート ライセンスの機能層を設定します。
http-proxy	スマート ライセンスおよび Smart Call Home の HTTP(S) プロキシを設定します。
license smart	スマート ライセンスのライセンス権限付与を要求できます。
license smart deregister	ライセンス認証局からデバイスを登録解除します。
license smart register	デバイスをライセンス認証局に登録します。
service call-home	Smart Call Home をイネーブルにします。
show license	スマート ライセンスのステータスを表示します。
show running-config license	スマート ライセンスの設定を表示します。
throughput level	スマート ライセンスのスループット レベルを設定します。

license smart reservation

パーマネント ライセンスの予約をイネーブルにするには、グローバル コンフィギュレーション モードで **license smart reservation** コマンドを使用します。パーマネント ライセンスの予約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。

license smart reservation

no license smart reservation

(注) この機能は、ASAv と Firepower 2100 にのみ適用されます。

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

この機能はデフォルトで無効に設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.5(2.200)	このコマンドは、ASAv のサポート用に導入されました。
9.8(2)	Firepower 2100 シリーズのサポートが追加されました。

使用上のガイドライン

インターネット アクセスを持たない ASA の場合は、Smart Software Manager からパーマネント ライセンスを要求できます（https://software.cisco.com/#SmartLicensing-Inventory）。パーマネント ライセンスでは、すべての機能を最大限に使用できます。

ASAv の場合、**license smart reservation** コマンドを入力すると、次のコマンドが削除されます。

```
license smart
    feature tier standard
        throughput level {100M | 1G | 2G}
```

通常のスマート ライセンスを使用するには、このコマンドの **no** 形式を使用し、上記のコマンドを再入力します。その他の Smart Call Home 設定はそのまま維持されますが、使用されないため、それらのコマンドを再入力する必要はありません。

Firepower シャーシの場合、コンテキスト ライセンスなどのデフォルト以外のライセンスに対しては、**license smart/feature** コマンドを入力する必要があります。これらのコマンドは、ASA に機能の設定を許可するよう指定するために必要です。

(注) 永続ライセンスの予約については、ASA を廃棄する前にライセンスを戻す必要があります。ライセンスを正式に戻さないと、ライセンスが使用中の状態のままになり、新しい ASA に再使用できません。**license smart reservation return** コマンドを参照してください。

例

次に、パーマネント ライセンスの予約をイネーブルにして、Smart Software Manager に入力するライセンス コードを要求し、Smart Software Manager から受け取った承認コードをインストールする例を示します。

```
ciscoasa(config)# license smart reservation
ciscoasa(config)# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
...
ciscoasa(config)# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
```

関連コマンド

コマンド	説明
license smart reservation cancel	Smart Software Manager でコードを入力していない場合に、パーマネント ライセンスの要求をキャンセルします。
license smart reservation install	承認コードを入力します。
license smart reservation request universal	Smart Software Manager に入力するライセンス コードを要求します。
license smart reservation return	Smart Software Manager にライセンスを戻します。

license smart reservation cancel

まだ Smart Software Manager でコードを入力していない場合にパーマネント ライセンスの予約の要求をキャンセルするには、特権 EXEC モードで **license smart reservation cancel** コマンドを使用します。

license smart reservation cancel

(注) この機能は、ASAv と Firepower 2100 にのみ適用されます。

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド 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

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.5(2.200)	このコマンドは、ASAv のサポート用に導入されました。
9.8(2)	Firepower 2100 シリーズのサポートが追加されました。

使用上のガイドライン

license smart reservation request universal コマンドを使用して Smart Software Manager に入力するライセンス コードを要求した場合、そのコードをまだ Smart Software Manager に入力していなければ、**license smart reservation cancel** コマンドを使用して要求をキャンセルできます。

パーマネント ライセンスの予約をディセーブルにする（**no license smart reservation**）と、保留中のすべての要求がキャンセルされます。

すでに Smart Software Manager にコードを入力している場合は、ASA へのライセンスの適用を完了する必要があります。その時点から、**license smart reservation return** コマンドによってライセンスを戻すことが可能になります。

例

次に、パーマネント ライセンスの予約をイネーブルにして、Smart Software Manager に入力するライセンス コードを要求した後に、要求をキャンセルする例を示します。

```
ciscoasa(config)# license smart reservation
ciscoasa(config)# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
ciscoasa(config)# license smart reservation cancel
```

関連コマンド

コマンド	説明
license smart reservation	パーマネント ライセンスの予約をイネーブルにします。
license smart reservation install	承認コードを入力します。
license smart reservation request universal	Smart Software Manager に入力するライセンス コードを要求します。
license smart reservation return	Smart Software Manager にライセンスを戻します。

license smart reservation install

Smart Software Manager から受け取ったパーマネント ライセンスの予約の承認コードを入力するには、特権 EXEC モードで **license smart reservation install** コマンドを使用します。

license smart reservation install *code*

(注) この機能は、ASAv と Firepower 2100 にのみ適用されます。

構文の説明

code	Smart Software Manager から受け取ったパーマネント ライセンスの予約の承認コード。

コマンド 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

次の表に、コマンドを入力できるモードを示します。

コマンド モード	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	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.5(2.200)	このコマンドは、ASAv のサポート用に導入されました。
9.8(2)	Firepower 2100 シリーズのサポートが追加されました。

使用上のガイドライン

インターネット アクセスを持たない ASA の場合は、Smart Software Manager からパーマネント ライセンスを要求できます（https://software.cisco.com/#SmartLicensing-Inventory）。**license smart reservation request universal** コマンドを使用して Smart Software Manager に入力するコードを要求します。Smart Software Manager にコードを入力するときは、受け取った承認コードをコピーして、**license smart reservation install** コマンドを使用して ASA に入力します。

例

次に、パーマネント ライセンスの予約をイネーブルにして、Smart Software Manager に入力するライセンス コードを要求し、Smart Software Manager から受け取った承認コードをインストールする例を示します。

```
ciscoasa(config)# license smart reservation
ciscoasa(config)# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
```

```
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
...
ciscoasa(config)# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
```

関連コマンド

コマンド	説明
license smart reservation	パーマネント ライセンスの予約をイネーブルにします。
license smart reservation cancel	Smart Software Manager でコードを入力していない場合に、パーマネント ライセンスの要求をキャンセルします。
license smart reservation request universal	Smart Software Manager に入力するライセンス コードを要求します。
license smart reservation return	Smart Software Manager にライセンスを戻します。

license smart reservation universal

Smart Software Manager に入力するライセンス コードを要求するには、特権 EXEC モードで **license smart reservation universal** コマンドを使用します。

license smart reservation universal

(注) この機能は、ASAv と Firepower 2100 にのみ適用されます。

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド 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

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.5(2.200)	このコマンドは、ASAv のサポート用に導入されました。
9.8(2)	Firepower 2100 シリーズのサポートが追加されました。

使用上のガイドライン

インターネット アクセスを持たない ASA の場合は、Smart Software Manager から永続ライセンスを要求できます。**license smart reservation request universal** コマンドを使用して Smart Software Manager に入力するコードを要求します。

ASAv の導入により、どのライセンス（ASAv5/ASAv10/ASAv30）を要求するかが決定されます。

このコマンドを再入力すると、リロード後にも同じコードが表示されます。このコードをまだ Smart Software Manager に入力していない場合、要求をキャンセルするときは、**license smart reservation cancel** コマンドを入力します。

パーマネント ライセンスの予約をディセーブルにすると、保留中のすべての要求がキャンセルされます。すでに Smart Software Manager にコードを入力している場合は、その手順を完了して ASA にライセンスを適用する必要があります。その時点から、必要に応じてライセンスを戻すことが可能になります。**license smart reservation return** コマンドを参照してください。

承認コードを要求するには、Smart Software Manager のインベントリ画面に移動して（https://software.cisco.com/#SmartLicensing-Inventory）、[Licenses] タブをクリックします。[Licenses] タブにアカウントに関連するすべての既存のライセンスが、標準およびパーマネントの両方とも表示されます。[License Reservation] をクリックして、ASA のコードをボックスに入力します。[Reserve License] をクリックします。Smart Software Manager が承認コードを生成します。コードをダウンロードまたはクリップボードにコピーできます。この時点で、ライセンスは、Smart Software Manager に従って使用中です。

[License Reservation] ボタンが表示されない場合、お使いのアカウントはパーマネント ライセンスの予約について承認されていません。この場合、パーマネント ライセンスの予約を無効にして標準のスマート ライセンス コマンドを再入力する必要があります。

license smart reservation install コマンドを使用して ASA に承認コードを入力します。

例

次に、パーマネント ライセンスの予約をイネーブルにして、Smart Software Manager に入力するライセンス コードを要求し、Smart Software Manager から受け取った承認コードをインストールする例を示します。

```
ciscoasa(config)# license smart reservation
ciscoasa(config)# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
...
ciscoasa(config)# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
```

関連コマンド

コマンド	説明
license smart reservation	パーマネント ライセンスの予約をイネーブルにします。
license smart reservation cancel	Smart Software Manager でコードを入力していない場合に、パーマネント ライセンスの要求をキャンセルします。
license smart reservation install	承認コードを入力します。
license smart reservation return	Smart Software Manager にライセンスを戻します。

license smart reservation return

Smart Software Manager にライセンスを戻すための戻りコードを生成するには、特権 EXEC モードで **license smart reservation return** コマンドを使用します。

license smart reservation return

(注) この機能は、ASAv と Firepower 2100 にのみ適用されます。

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド 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

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.5(2.200)	このコマンドは、ASAv のサポート用に導入されました。
9.8(2)	Firepower 2100 シリーズのサポートが追加されました。

使用上のガイドライン

インターネット アクセスを持たない ASA の場合は、Smart Software Manager から永続ライセンスを要求できます。パーマネント ライセンスが不要になった場合（ASA を廃棄する場合や ASAv のモデル レベルの変更によって新しいライセンスが必要になった場合など）、ライセンスを正式に Smart Software Manager に戻す必要があります。ライセンスを正式に戻さないと、ライセンスが使用中の状態のままになり、他の場所で使用するために容易に解除できません。

license smart reservation return コマンドを入力すると、ASA が即座にライセンス未適用状態になり、試用状態に移行します。このコードを再度表示する必要がある場合は、このコマンドを再入力します。新しいパーマネント ライセンスを要求する（**license smart reservation request universal**）か、ASAv のモデル レベルを変更する（電源を切り、vCPU/RAM を変更する）と、このコードを再表示できなくなることに注意してください。必ず、コードをキャプチャして、戻す作業を完了してください。

Smart Software Manager にコードを入力する前に、**show license udi** コマンドを使用して ASA のユニバーサル デバイス識別子（UDI）を表示します。これにより、この ASA インスタンスを Smart Software Manager で識別できるようになります。Smart Software Manager インベントリ画面に移動して（https://software.cisco.com/#SmartLicensing-Inventory）、[Product Instances] タブをクリックします。[Product Instances] タブに、ライセンスが付与されているすべての製品が UDI によって表示されます。ライセンスを解除する ASAv を確認し、[Actions] > [Remove] を選択して、ASA の戻りコードをボックスに入力します。[Remove Product Instance] をクリックします。パーマネントライセンスが使用可能なライセンスのプールに戻されます。

例

次に、ASAv で戻りコードを生成し、ASAv UDI を表示する例を示します。

```
ciscoasa# license smart reservation return
Enter this return code in the Cisco Smart Software Manager portal:
Au3431rGRS00Ig5HQl2vpcg{uXiTRfVrp7M/zDpirLwYCaq8oSv60yZJuFDVBS2QliQ=
ciscoasa# show license udi
UDI: PID:ASAv,SN:9AHV3KJBEKE
```

関連コマンド

コマンド	説明
license smart reservation	パーマネント ライセンスの予約をイネーブルにします。
license smart reservation cancel	Smart Software Manager でコードを入力していない場合に、パーマネント ライセンスの要求をキャンセルします。
license smart reservation install	承認コードを入力します。
license smart reservation request universal	Smart Software Manager に入力するライセンス コードを要求します。

lifetime（CA サーバ モード）

ローカル認証局（CA）証明書、各発行済み証明書、または証明書失効リスト（CRL）の有効期間を指定するには、CA サーバ 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。パラメータをデフォルト設定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 {**ca-certificate** | **certificate** | **crl**} *time*

no lifetime {**ca-certificate** | **certificate** | **crl**}

構文の説明

ca-certificate	ローカル CA サーバ証明書のライフタイムを指定します。
certificate	CA サーバが発行するすべてのユーザ証明書のライフタイムを指定します。
crl	CRL のライフタイムを指定します。
time	CA 証明書およびすべての発行済み証明書の場合、*time* はその証明書の有効日数を指定します。有効範囲は 5 ～ 30 年です。デフォルトのライフタイム値は 15 年です。 発行されたすべてのユーザ証明書の有効範囲は 1 日 ～ 4 年です。デフォルトのライフタイム値は 2 年です。 CRL の場合、*time* は CRL の有効時間数を指定します。CRL の有効な範囲は、1 ～ 720 時間です。

デフォルト

デフォルトのライフタイムは次のとおりです。

- CA 証明書：15 年
- 発行済み証明書：2 年
- CRL：6 時間

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.12(1)	**lifetime ca-certificate** で使用可能な値は、5 ～ 30 年に変更されており、デフォルトは 15 年です。 **lifetime certificate** で使用可能な値は、1 日 ～ 4 年に変更されており、デフォルトは 2 年です。

使用上のガイドライン

証明書または CRL が有効である日数または時間数を指定すると、このコマンドは、証明書または CRL に含める有効期限を決定します。

lifetime ca-certificate コマンドは、ローカル CA サーバ証明書の初回生成時（初めてローカル CA サーバを設定し、**no shutdown** コマンドを発行するとき）に有効になります。CA 証明書の期限が切れると、設定されたライフタイム値を使用して新しい CA 証明書が生成されます。既存の CA 証明書のライフタイム値は変更できません。

例

次に、3 か月間有効な証明書を発行するように CA を設定する例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# lifetime certificate 90
ciscoasa(config-ca-server))#
```

次に、2 日間有効な CRL を発行するように CA を設定する例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# lifetime crl 48
ciscoasa(config-ca-server)#
```

関連コマンド

コマンド	説明
cdp-url	CA が発行する証明書に含める証明書失効リストの配布ポイント（CDP）を指定します。
crypto ca server	CA サーバ コンフィギュレーション モードのコマンド セットにアクセスできるようにします。これらのコマンド セットを使用することで、ローカル CA を設定および管理できます。
crypto ca server crl issue	CRL を強制的に発行します。
show crypto ca server	ローカル CA コンフィギュレーションの詳細を ASCII テキストで表示します。
show crypto ca server cert-db	ローカル CA サーバ証明書を表示します。
show crypto ca server crl	ローカル CA の現在の CRL を表示します。

lifetime（IKEv2 ポリシー モード）

AnyConnect IPsec 接続に使用する IKEv2 セキュリティ アソシエーション（SA）の暗号化アルゴリズムを指定するには、IKEv2 ポリシー コンフィギュレーション モードで **encryption** コマンドを使用します。コマンドを削除してデフォルト設定を使用するには、このコマンドの **no** 形式を使用します。

lifetime {{**seconds** *seconds*} | **none**}

構文の説明

seconds	ライフタイムの秒数（120 ～ 2,147,483,647 秒）。デフォルトは 86,400 秒（24 時間）です。

デフォルト

デフォルトは 86,400 秒（24 時間）です。

使用上のガイドライン

IKEv2 SA は、IKEv2 ピアがフェーズ 2 で安全に通信できるようにするためにフェーズ 1 で使用されるキーです。**crypto ikev2 policy** コマンドを入力した後、**lifetime** コマンドを使用して SA のライフタイムを設定します。

このコマンドでは、IKEv2 SA のキーを再生成する間隔を設定します。none キーワードを使用すると、SA のキー再生成がディセーブルになります。ただし、引き続き AnyConnect クライアントで SA のキー再生成を実行できます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。

例

次に、IKEv2 ポリシー コンフィギュレーション モードを開始し、ライフタイムを 43,200 秒（12 時間）に設定する例を示します。

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# lifetime 43200
```

関連コマンド

コマンド	説明
encryption	AnyConnect IPsec 接続に対して IKEv2 SA の暗号化アルゴリズムを指定します。
group	AnyConnect IPsec 接続に対して IKEv2 SA の Diffie-Hellman グループを指定します。
整合性	AnyConnect IPsec 接続に対して IKEv2 SA の ESP 整合性アルゴリズムを指定します。
prf	AnyConnect IPsec 接続に対して IKEv2 SA の疑似乱数関数を指定します。

limit-resource

マルチ コンテキスト モードでクラスの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。ASA では、リソース クラスにコンテキストを割り当てることによって、リソースを管理します。各コンテキストでは、クラスによって設定されたリソース制限が使用されます。

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

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

構文の説明

all	すべてのリソースの制限を設定します。
number[**%**]	リソース制限を 1 以上の固定数、またはパーセント記号(%)付きのシステム制限のパーセンテージ(1 ～ 100)として指定します。リソースに制限がない場合、または VPN リソース タイプについて制限をなしに設定する場合は、この値を **0** に設定します。システム制限が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。絶対値のみを設定できます。
rate	リソースの 1 秒あたりのレートを設定することを指定します。1 秒あたりのレートを設定できるリソースについては、表 7-1 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

すべてのコンテキストは、別のクラスに割り当てられていない場合はデフォルト クラスに属します。コンテキストをデフォルト クラスに積極的に割り当てる必要はありません。

ほとんどのリソースについては、デフォルト クラスではすべてのコンテキストがリソースに無制限でアクセスできます。ただし、次の制限を除きます。

- Telnet セッション:5 セッション。(コンテキストあたりの最大値)。
- SSH セッション:5 セッション。(コンテキストあたりの最大値)。
- IPsec セッション:5 セッション。(コンテキストあたりの最大値)。
- MAC アドレス:65,535 エントリ。(コンテキストあたりの最大値)。
- AnyConnect ピア:0 セッション(AnyConnect ピアを許可するようにクラスを手動で設定する必要があります)。
- VPN サイトツーサイト トンネル:0 セッション(VPN セッションを許可するようにクラスを手動で設定する必要があります)。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	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	
	ルーテッド	トランスペアレント	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	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
9.0(1)	新規リソース タイプ routes が作成されました。これは、各コンテキストでのルーティング テーブル エントリの最大数を設定するためです。 新しいリソース タイプ vpn other と vpn burst other が作成されました。これは、各コンテキストでのサイトツーサイト VPN トンネルの最大数を設定するためです。
9.5(2)	新しいリソース タイプ vpn anyconnect と vpn burst anyconnect が作成されました。これは、各コンテキストでの AnyConnect VPN ピアの最大数を設定するためです。
9.6(2)	最大ストレージを設定するための新しいリソース タイプ **storage** が作成されました。

使用上のガイドライン

デフォルトでは、すべてのセキュリティ コンテキストは ASA のリソースに無制限でアクセスできますが、コンテキストあたりの上限が定められている場合を除きます。唯一の例外は、VPN のリソース(デフォルトでディセーブルになっています)です。特定のコンテキストが使用しているリソースが多すぎることが原因で、他のコンテキストが接続を拒否されるといった現象が発生した場合は、コンテキストあたりのリソースの使用量を制限するようにリソース管理を設定できます。VPN のリソースについては、VPN トンネルを許可するようにリソース管理を設定する必要があります。

表 7-1 に、リソース タイプと制限を示します。**show resource types** コマンドも参照してください。

表 7-1　リソース名と制限

リソース名	レートまたは同時	コンテキストあたりの最小数と最大数	システム制限[1]	説明
asdm	同時接続数	最小 1 最大 20	32	ASDM 管理セッション。 (注)　ASDM セッションでは、2 つの HTTPS 接続を使用します。1 つは常に存在するモニタリング用の接続、もう 1 つは変更時にのみ存在するコンフィギュレーション変更用の接続です。たとえば、ASDM セッションのシステム制限が 32 の場合、HTTPS セッション数は 64 に制限されます。
conns	同時またはレート	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、CLI 設定ガイドを参照してください。 レート:該当なし	任意の 2 つのホスト間の TCP または UDP 接続(1 つのホストと他の複数のホストとの間の接続を含む)。
ホスト	同時接続数	該当なし	該当なし	ASA 経由で接続可能なホスト。
inspects	レート	該当なし	該当なし	アプリケーション インスペクション。
mac-addresses	同時接続数	該当なし	65,535	トランスペアレント ファイアウォール モードでは、MAC アドレス テーブルで許可される MAC アドレス数。
routes	同時接続数	該当なし	該当なし	ダイナミック ルート。
ssh	同時接続数	最小 1 最大 5	100	SSH セッション
storage	MB	最大値は、指定するフラッシュ メモリのドライブによって異なります。	最大値は、指定するフラッシュ メモリのドライブによって異なります。	コンテキストでのディレクトリのストレージ制限(MB 単位)。ドライブを指定するには、**storage-url** コマンドを使用します。
syslogs	レート	該当なし	該当なし	システム ログ メッセージ。
telnet	同時接続数	最小 1 最大 5	100	Telnet セッション。

表 7-1　リソース名と制限(続き)

リソース名	レートまたは同時	コンテキストあたりの最小数と最大数	システム制限[1]	説明
vpn burst anyconnect	同時接続数	該当なし	モデルに応じた AnyConnect Premium ピア数から、vpn anyconnect 用にすべてのコンテキストに割り当てられたセッション数の合計を差し引いた値。	**vpn anyconnect** でコンテキストに割り当てられた数を超えて許可される AnyConnect セッションの数。たとえば、使用するモデルで 5000 のピアがサポートされており、**vpn anyconnect** で割り当てたピア数の合計が全コンテキストで 4000 の場合は、残りの 1000 セッションが **vpn burst anyconnect** に使用可能です。**vpn anyconnect** ではセッション数がコンテキストに対して保証されますが、対照的に **vpn burst anyconnect** ではオーバーサブスクライブが可能です。バースト プールをすべてのコンテキストが、先着順に使用できます。
vpn anyconnect	同時接続数	該当なし	モデルごとの使用可能な AnyConnect VPN ピア数については、CLI 設定ガイドの「モデルごとにサポートされている機能のライセンス」を参照してください。	AnyConnect ピア。このリソースはオーバーサブスクライブできません。すべてのコンテキストへの割り当て合計がモデルの制限を超えてはなりません。このリソースに割り当てたピアは、そのコンテキストに対して保証されます。
vpn burst other	同時接続数	該当なし	モデルに応じた Other VPN セッション数から、**vpn other** 用にすべてのコンテキストに割り当てられたセッション数の合計を差し引いた値。	**vpn other** でコンテキストに割り当てられた数を超えて許可されるサイトツーサイト VPN セッションの数。たとえば、使用するモデルで 5000 セッションがサポートされており、**vpn other** で割り当てたセッション数の合計が全コンテキストで 4000 の場合は、残りの 1000 セッションが **vpn burst other** に使用可能です。**vpn other** ではセッション数がコンテキストに対して保証されますが、対照的に **vpn burst other** ではオーバーサブスクライブが可能です。バースト プールをすべてのコンテキストが、先着順に使用できます。
vpn other	同時接続数	該当なし	モデルごとの使用可能な Other VPN セッション数については、CLI 設定ガイドの「モデルごとにサポートされている機能のライセンス」を参照してください。	サイトツーサイト VPN セッション。このリソースはオーバーサブスクライブできません。すべてのコンテキストへの割り当て合計がモデルの制限を超えてはなりません。このリソースに割り当てたセッションは、そのコンテキストに対して保証されます。
xlates	同時接続数	該当なし	該当なし	アドレス変換。

1. このカラムに「該当なし」と記述されている場合、そのリソースにはハード 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

次に、接続のデフォルト クラスの制限に、無制限ではなく 10 % を設定する例を示します。

```
ciscoasa(config)# class default
ciscoasa(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。

```
ciscoasa(config)# class gold
ciscoasa(config-class)# limit-resource mac-addresses 10000
ciscoasa(config-class)# limit-resource conns 15%
ciscoasa(config-class)# limit-resource rate conns 1000
ciscoasa(config-class)# limit-resource rate inspects 500
ciscoasa(config-class)# limit-resource hosts 9000
ciscoasa(config-class)# limit-resource asdm 5
ciscoasa(config-class)# limit-resource ssh 5
ciscoasa(config-class)# limit-resource rate syslogs 5000
ciscoasa(config-class)# limit-resource telnet 5
ciscoasa(config-class)# limit-resource xlates 36000
ciscoasa(config-class)# limit-resource routes 700
```

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。
コンテキスト	セキュリティ コンテキストを設定します。
member	コンテキストをリソース クラスに割り当てます。
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

最終変更時刻のタイムスタンプだけを持つオブジェクトのキャッシングに関する再検証ポリシーを設定するには、キャッシュ コンフィギュレーション 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の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。属性をデフォルト値 20 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。

lmfactor *value*

no lmfactor

構文の説明

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す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	トランスペアレント	シングル	コンテキスト	システム
キャッシュ コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

ASA は、lmfactor の値を使用して、キャッシュされたオブジェクトを変更なしと見なす時間の長さを推定します。これは有効期限と呼ばれます。ASA は、最終変更後の経過時間に lmfactor をかけることによって有効期限を推定します。

lmfactor を 0 に設定すると、ただちに再検証が強制されます。100 に設定すると、再検証までの時間は可能な限り長くなります。

例

次に、lmfactor を 30 に設定する例を示します。

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

関連コマンド

コマンド	説明
cache	WebVPN キャッシュ モードを開始します。
cache-compressed	WebVPN キャッシュの圧縮を設定します。
disable	キャッシュ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。

load-monitor

クラスタ トラフィック ロード モニタリングを設定するには、クラスタ コンフィギュレーション モードで **load-monitor** コマンドを使用します。この機能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。

load-monitor [**frequency** *seconds*] [**intervals** *intervals*]

no load monitor [**frequency** *seconds*] [**interval** *interval*]

構文の説明

frequency *seconds*	（オプション）モニタリング メッセージの間隔を 10 ～ 360 秒の範囲で設定します。デフォルトは 20 秒です。
intervals *intervals*	（オプション）ASA がデータを保持する間隔の数を 1 ～ 60 の範囲で設定します。デフォルトは 30 です。

コマンド デフォルト

このコマンドは、デフォルトでイネーブルになっています。デフォルトの頻度は、20 秒です。デフォルトの間隔は、30 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	シングル	コンテキスト	システム
クラスタ構成	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.13(1)	コマンドが追加されました。

使用上のガイドライン

クラスタ メンバのトラフィック負荷をモニタできます。対象には、合計接続数、CPU とメモリの使用率、バッファ ドロップなどが含まれます。負荷が高すぎる場合、残りのユニットが負荷を処理できる場合は、ユニットのクラスタリングを手動で無効にするか、外部スイッチのロードバランシングを調整するかを選択できます。この機能は、デフォルトでイネーブルにされています。たとえば、各シャーシに 3 つのセキュリティ モジュールが搭載された Firepower 9300 のシャーシ間クラスタリングの場合、シャーシ内の 2 つのセキュリティ モジュールがクラスタを離れると、そのシャーシに対する同じ量のトラフィックが残りのモジュールに送信され、過負荷になる可能性があります。トラフィックの負荷は定期的にモニタできます。負荷が高すぎる場合は、ユニットのクラスタリングを手動で無効にすることを選択できます。

トラフィック負荷を表示するには、**show cluster info load-monitor** コマンドを使用します。

例

次に、周波数を 50 秒に、間隔を 25 に設定する例を示します。

```
ciscoasa(cfg-cluster)# load-monitor frequency 50 intervals 25
```

関連コマンド

コマンド	説明
クラスタ	クラスタ コンフィギュレーション モードを開始します

local-domain-bypass

DNS 要求が Cisco Umbrella をバイパスする必要があるローカル ドメインを設定するには、Umbrella コンフィギュレーション モードで **local-domain-bypass** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

local-domain-bypass {*regular_expression* | **regex class** *regex_classmap*}

no local-domain-bypass {*regular_expression* | **regex class** *regex_classmap*}

構文の説明

regular_expression	バイパスするローカル ドメインを識別する正規表現。この正規表現は、ローカル ドメインのように単純にすることができます（たとえば、example.com）。最大 100 文字の正規表現を入力できます。 このオプションを使用する場合は、**local-domain-bypass** コマンドを複数回入力して、複数のローカル ドメインを定義できます。
regex class *regex_classmap*	バイパスするローカル ドメイン名を定義する正規表現クラスの名前。クラス内の正規表現に一致する完全修飾ドメイン名に対するすべての DNS 要求は、Umbrella サーバではなく、設定された DNS サーバに直接送信されます。

デフォルト

デフォルトでは、すべてのドメインに対する DNS 要求が Cisco Umbrella に送信されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	シングル	コンテキスト	システム
Umbrella の設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.12(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用する場合のガイドラインを次に示します。

- このコマンドを複数回入力して、ドメイン名の正規表現を直接定義することができます。
- 正規表現クラスを使用するときは、このコマンドを 1 回だけ入力できます。ただし、正規表現を直接使用する場合は、コマンドの単一の正規表現クラス バージョンと複数のインスタンスを組み合わせることができます。

例

次の例では、バイパスするローカルドメインとして example.com を定義しています。

```
ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)# local-domain-bypass example.com
```

次の例では、example.com と一致する正規表現を作成しています。これは、*example.com 上の完全修飾ドメイン名と一致します。次に、この例では、必要な正規表現クラス マップを作成して、Umbrella のローカル ドメイン バイパスとして使用しています。

```
ciscoasa(config)# regex example-com example.com
ciscoasa(config)# class-map type regex match-any umbrella-bypass
ciscoasa(config-cmap)# match regex example-com

ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)# local-domain-bypass regex class umbrella-bypass
```

関連コマンド

コマンド	説明
umbrella-global	Cisco Umbrella グローバルパラメータを設定します。

local-unit

このクラスタ メンバの名前を指定するには、クラスタ グループ コンフィギュレーション モードで **local-unit** コマンドを使用します。名前を削除するには、このコマンドの **no** 形式を使用します。

local-unit *unit_name*

no local-unit [*unit_name*]

構文の説明

unit_name	このクラスタ メンバの固有の名前を、1 ～ 38 文字の ASCII 文字列で指定します。

コマンド 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

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	シングル	コンテキスト	システム
クラスタ グループ コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

各ユニットに固有の名前が必要です。クラスタ内の他のユニットと同じ名前を付けることはできません。

例

次に、このユニットに unit1 という名前を付ける例を示します。

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# local-unit unit1
```

関連コマンド

コマンド	説明
clacp system-mac	スパンド EtherChannel を使用するときは、ASA は cLACP を使用してネイバー スイッチとの間で EtherChannel のネゴシエーションを行います。
cluster group	クラスタに名前を付け、クラスタ コンフィギュレーション モードを開始します。
cluster-interface	クラスタ制御リンク インターフェイスを指定します。
cluster interface-mode	クラスタ インターフェイス モードを設定します。
conn-rebalance	接続の再分散をイネーブルにします。
console-replicate	スレーブ ユニットからマスター ユニットへのコンソール複製をイネーブルにします。
enable(クラスタ グループ)	クラスタリングをイネーブルにします。
health-check	クラスタのヘルス チェック機能(ユニットのヘルス モニタリングおよびインターフェイスのヘルス モニタリングを含む)をイネーブルにします。
key	クラスタ制御リンクの制御トラフィックの認証キーを設定します。
mtu cluster-interface	クラスタ制御リンク インターフェイスの最大伝送ユニットを指定します。
priority(クラスタ グループ)	マスター ユニット選定のこのユニットのプライオリティを設定します。

location-logging

GTP インスペクションで、モバイル ステーションの場所と場所の変更をログに記録するには、GTP インスペクションのポリシー マップ パラメータ コンフィギュレーション モードで **location-logging** コマンドを使用します。場所のロギングを無効にするには、このコマンドの **no** 形式を使用します。

location-logging [**cell-id**]

no location-logging [**cell-id**]

構文の説明

cell-id	ユーザが現在登録されているセル ID を含めるかどうかを指定します。セル ID は、セル グローバル識別（CGI）または E-UTRAN セル グローバル識別子（ECGI）から抽出されます。

デフォルト

デフォルトでは、場所のロギングは無効になっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション モード	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.13(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

GTP インスペクションを使用すると、モバイル端末の場所の変更を追跡できます。場所の変更を追跡すると、不正なローミング請求を特定するのに役立つ場合があります。たとえば、モバイル端末が、米国のセルから欧州のセルに 30 分以内に移動するなど、ある場所から別の場所にありえない時間で移動した場合などです。

場所のロギングを有効にすると、システムは International Mobile Subscriber Identity（IMSI）ごとに新しい場所または変更された場所の syslog メッセージを生成します。

- 324010 は新しい PDP コンテキストの作成を示し、携帯電話の国コード（MCC）、モバイル ネットワーク コード（MNC）、情報要素、および必要に応じてユーザが現在登録されているセル ID が含まれます。セル ID は、セル グローバル識別（CGI）または E-UTRAN セル グローバル識別子（ECGI）から抽出されます。

- 324011 は、IMSI が PDP コンテキストの作成中に保存されたものから移動したことを示します。メッセージには、以前および現在の MCC/MNC および必要に応じてセル ID が表示されます。

デフォルトでは、syslog メッセージにタイムスタンプ情報は含まれません。これらのメッセージを分析してありえないローミングを識別する場合は、タイムスタンプも有効にする必要があります。タイムスタンプ ロギングは GTP インスペクション マップに含まれません。**logging timestamp** コマンドを使用します。

例

次の例では、タイムスタンプを syslog メッセージに追加してから、セル ID を使用して場所のロギングを有効にしています。

```
ciscoasa(config)# logging timestamp
ciscoasa(config)# policy-map type inspect gtp gtp-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# location-logging cell-id
```

関連コマンド

コマンド	説明
inspect gtp	GTP アプリケーション インスペクションをイネーブルにします。
policy-map type inspect gtp	GTP インスペクション ポリシー マップを作成または編集します。
show service-policy inspect gtp	GTP 設定および統計情報を表示します。

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 トラフィックのインスペクション ポリシー マップ（**policy-map type inspect** コマンド）で使用できます。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

構文の説明

このコマンドには引数またはキーワードはありません。

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

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

インスペクション 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。インスペクション ポリシー マップで使用できる実際のコマンドは、アプリケーションによって異なります。**match** コマンドまたは **class** コマンドを入力してアプリケーション トラフィックを特定した後（**class** コマンドは、**match** コマンドを含む既存の **class-map type inspect** コマンドを参照する）、**log** コマンドを入力して、**match** コマンドまたは **class** コマンドに一致するすべてのパケットをログに記録できます。

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 インスペクションをイネーブルにする場合、このアクションを含むインスペクション ポリシー マップをイネーブルにできます。たとえば、**inspect http http_policy_map** コマンドを入力します。http_policy_map は、インスペクション ポリシー マップの名前です。

例

次に、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する例を示します。

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

関連コマンド

コマンド	説明
class	ポリシー マップのクラス 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インスペクション 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 インスペクションの特別なアクションを定義します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

log-adjacency-changes

NLSP IS-IS 隣接がステートを変更(アップまたはダウン)する際に IS-IS が syslog メッセージを送信することを可能にするには、ルータ ISIS コンフィギュレーション モードで **log-adjacency-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-adjacency-changes [all]

no log-adjacency-changes [**all**]

構文の説明

all	(オプション)non_IIH イベントによって生成される変更を含みます。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドにより、IS-IS 隣接のステート変更のモニタリングが可能になります。これは、大規模なネットワークをモニタリングする場合に非常に役立つことがあります。メッセージは、システム エラー メッセージ機能を使用してロギングされます。メッセージは次の形式になります。

```
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Up, new adjacency
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Down, hold time expired
```

例

次に、隣接の変更をログに記録するように ルータ に指示する例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# log-adjacency-changes
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
認証キー	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。

コマンド	説明
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト（TLV）を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

log-adj-changes

OSPF ネイバーが起動または停止したときに 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**]

構文の説明

detail	（任意）ネイバーが起動または停止した場合だけでなく、状態が変わるたびに syslog メッセージを送信します。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

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います。このコマンドの **no** 形式で削除しない限り、実行コンフィギュレーションに表示されます。

例

次に、OSPF ネイバーが起動または停止したときに syslog メッセージを送信しないようにする例を示します。

```
ciscoasa(config)# router ospf 5
ciscoasa(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 モードを開始します。
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。

log-adjacency-changes

OSPFv3 ネイバーが起動または停止したときに 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-adjacency-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-adjacency-changes [**detail**]

no log-adjacency-changes [**detail**]

構文の説明

detail	（任意）ネイバーが起動または停止した場合だけでなく、状態が変わるたびに syslog メッセージを送信します。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	シングル	コンテキスト	システム
IPv6 ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

log-adjacency-changes コマンドはデフォルトでイネーブルになっています。このコマンドの **no** 形式で削除しない限り、実行コンフィギュレーションに表示されます。

例

次に、OSPFv3 ネイバーが起動または停止したときに syslog メッセージを送信しないようにする例を示します。

```
ciscoasa(config)# ipv6 router ospf 5
ciscoasa(config-router)# no log-adjacency-changes
```

関連コマンド

コマンド	説明
ipv6 router ospf	ルータ コンフィギュレーション モードを開始します。
show ipv6 ospf	OSPFv3 ルーティング プロセスに関する一般情報を表示します。