CHAPTER 2

acl-netmask-convert コマンド～ application-access hide-details コマンド

acl-netmask-convert

aaa-server host コマンドを使用してアクセスする RADIUS サーバからダウンロード可能な ACL に受信したネットマスクを ASA でどのように処理するかを指定するには、AAA サーバ ホスト コンフィギュレーション モードで **acl-netmask-convert** コマンドを使用します。ASA の指定した動作を解除するには、このコマンドの **no** 形式を使用します。

acl-netmask-convert {**auto-detect** | **standard** | **wildcard**}

no acl-netmask-convert

構文の説明

auto-detect	ASA は、使用されているネットマスク表現のタイプを判断しようとします。ASA は、ワイルドカード ネットマスク表現を検出した場合、標準ネットマスク表現に変換します。このキーワードの詳細については、「使用上のガイドライン」を参照してください。
standard	ASA は、RADIUS サーバから受信したダウンロード可能な ACL に標準ネットマスク表現のみが含まれていると見なします。ワイルドカード ネットマスク表現からの変換は実行されません。
wildcard	ASA は、RADIUS サーバから受信したダウンロード可能な ACL にワイルドカード ネットマスク表現のみが含まれていると見なし、ACL のダウンロード時にそれらのすべてを標準ネットマスク表現に変換します。

デフォルト

デフォルトでは、ワイルドカード ネットマスク表現からの変換は実行されません。

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
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(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

RADIUS サーバから提供されるダウンロード可能な ACL にワイルドカード形式のネットマスクが含まれている場合は、wildcard または auto-detect キーワードを指定して **acl-netmask-convert** コマンドを使用します。ASA は、ダウンロード可能な ACL に標準ネットマスク表現が含まれていると想定します。一方、Cisco VPN 3000 シリーズ コンセントレータは、ダウンロード可能な ACL に、標準ネットマスク表現とは逆のワイルドカード ネットマスク表現が含まれていると想定します。ワイルドカード マスクでは、無視するビット位置に 1、照合するビット位置に 0 が配置されます。**acl-netmask-convert** コマンドを使用すると、このような相違が RADIUS サーバ上のダウンロード可能な ACL の設定方法に与える影響を最小限に抑えることができます。

RADIUS サーバの設定方法が不明な場合は、**auto-detect** キーワードが役立ちます。ただし、「穴」があるワイルドカード ネットマスク表現は、正しく検出および変換できません。たとえば、ワイルドカード ネットマスク 0.0.255.0 は、第 3 オクテットに任意の値を許可し、Cisco VPN 3000 シリーズ コンセントレータでは有効に使用できます。ただし、ASA では、この表現をワイルドカード ネットマスクとして検出できません。

例

次に、ホスト「192.168.3.4」に「srvgrp1」という名前の RADIUS AAA サーバを設定し、ダウンロード可能な ACL のネットマスクの変換をイネーブルにして、タイムアウトを 9 秒、再試行間隔を 7 秒、認証ポートを 1650 に設定する例を示します。

```
ciscoasa(config)# aaa-server svrgrp1 protocol radius
ciscoasa(config-aaa-server-group)# aaa-server svrgrp1 host 192.168.3.4
ciscoasa(config-aaa-server-host)# acl-netmask-convert wildcard
ciscoasa(config-aaa-server-host)# timeout 9
ciscoasa(config-aaa-server-host)# retry-interval 7
ciscoasa(config-aaa-server-host)# authentication-port 1650
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

関連コマンド

コマンド	説明
aaa authentication	**aaa-server** コマンドまたは ASDM ユーザ認証により指定されたサーバ上の LOCAL、TACACS+、または RADIUS ユーザ認証をイネーブルまたはディセーブルにします。
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードを開始します。このモードでは、ホストに固有の AAA サーバパラメータを設定できます。
clear configure aaa-server	すべての AAA コマンド ステートメントをコンフィギュレーションから削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

アクション

アクセス ポリシーをセッションに適用するか、またはセッションを終了するには、ダイナミック アクセス ポリシー レコード コンフィギュレーション モードで **action** コマンドを使用します。セッションをリセットしてアクセス ポリシーをセッションに適用するには、このコマンドの **no** 形式を使用します。

action {continue | terminate}

no action {continue | terminate}

構文の説明

continue	アクセス ポリシーをセッションに適用します。
terminate	接続を切断します。

デフォルト

デフォルト値は continue 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
ダイナミック アクセス ポリシー レコード 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
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

選択したすべての DAP レコードでセッションにアクセス ポリシーを適用するには、**continue** キーワードを使用します。選択した DAP レコードのいずれかで接続を切断するには、**terminate** キーワードを使用します。

例

次に、Finance という DAP ポリシーのセッションを切断する例を示します。

```
ciscoasa (config)# config-dynamic-access-policy-record Finance
ciscoasa(config-dynamic-access-policy-record)# action terminate
ciscoasa(config-dynamic-access-policy-record)#
```

関連コマンド

コマンド	説明
dynamic-access-policy-record	DAP レコードを作成します。
show running-config dynamic-access-policy-record	すべての DAP レコードまたは指定した DAP レコードの実行コンフィギュレーションを表示します。

action cli command

イベント マネージャ アプレットでアクションを設定するには、イベント マネージャ アプレット コンフィギュレーション モードで **action cli command** コマンドを使用します。設定したアクションを削除するには、**no action** *n* コマンドを入力します。

action *n* **cli command** "*command*"

no action *n*

構文の説明

"*command*"	コマンド名を指定します。*command* オプションの値は、引用符で囲む必要があります。引用符で囲んでいない場合、コマンドが 2 つ以上の単語で構成されているとエラーが発生します。このコマンドは、特権レベル 15（最高）を持つユーザとして、グローバル コンフィギュレーション モードで実行されます。ディセーブルになっているため、このコマンドは入力を受け付けない場合があります。**noconfirm** オプションは、コマンドで使用できる場合に使用します。
n	アクション ID を指定します。有効な ID の範囲は 0 ～ 42947295 です。

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
イベント マネージャ アプレット 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
9.2(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

イベント マネージャ アプレットでアクションを設定するには、このコマンドを使用します。

例

次に、イベント マネージャ アプレットでアクションを設定する例を示します。

```
hostname (config-applet)# action 1 cli command "show version"
```

関連コマンド

コマンド	説明
description	アプレットについて説明します。
event manager run	イベント マネージャ アプレットを実行します。
show event manager	設定された各イベント マネージャ アプレットの統計情報を表示します。
debug event manager	イベント マネージャのデバッグ トレースを管理します。

action-uri

Web サーバの URI を指定して、シングル サインオン（SSO）認証用のユーザ名とパスワードを受信するには、AAA サーバ ホスト コンフィギュレーション モードで **action-uri** コマンドを使用します。URI パラメータ値をリセットするには、このコマンドの **no** 形式を使用します。

action-uri *string*

no action-uri

（注） HTTP プロトコルを使用して SSO を正しく設定するには、認証と HTTP プロトコル交換についての詳しい実務知識が必要です。

構文の説明

string	認証プログラムの URI。複数行に入力できます。各行の最大文字数は 255 です。URI 全体の最大文字数は、2048 文字です。

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	—	—

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

これは HTTP フォームのコマンドを使用した SSO です。URI（ユニフォーム リソース識別子）は、インターネット上のコンテンツの位置を特定するコンパクトな文字列です。これらのコンテンツには、テキスト ページ、ビデオ クリップ、サウンド クリップ、静止画、動画、ソフトウェア プログラムなどがあります。URI の最も一般的な形式は、Web ページ アドレスです。Web ページ アドレスは、URI の特定の形式またはサブセットで、URL と呼ばれます。

ASA の WebVPN サーバでは、POST 要求を使用して、認証 Web サーバに SSO 認証要求を送信できます。これを行うには、HTTP POST 要求を使用して、認証 Web サーバ上のアクション URI にユーザ名とパスワードを渡すように ASA を設定します。**action-uri** コマンドでは、ASA が POST 要求を送信する Web サーバ上の認証プログラムの場所と名前を指定します。

認証 Web サーバ上のアクション URI を見つけるには、ブラウザで直接 Web サーバのログイン ページに接続します。ブラウザに表示されるログイン Web ページの URL が、認証 Web サーバの アクション URI です。

入力しやすいように、URI は連続する複数の行に入力できるようになっています。各行は入力と同時に ASA によって連結され、URI が構成されます。action-uri 行の 1 行あたりの最大文字数は 255 文字ですが、それよりも少ない文字を各行に入力できます。

(注) ストリングに疑問符を含める場合は、疑問符の前に Ctrl+V のエスケープ シーケンスを使用する必要があります。

例

次に、www.example.com の URI を指定する例を示します。

http://www.example.com/auth/index.html/appdir/authc/forms/MCOlogin.fcc?TYPE=33554433&REALMOID=06-000a1311-a828-1185-ab41-8333b16a0008&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=SM5FZmjnk3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6rB1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F%2Fauth.example.com

```
ciscoasa(config)# aaa-server testgrp1 host www.example.com
ciscoasa(config-aaa-server-host)# action-uri http://www.example.com/auth/index.htm
ciscoasa(config-aaa-server-host)# action-uri l/appdir/authc/forms/MCOlogin.fcc?TYP
ciscoasa(config-aaa-server-host)# action-uri 554433&REALMOID=06-000a1311-a828-1185
ciscoasa(config-aaa-server-host)# action-uri -ab41-8333b16a0008&GUID=&SMAUTHREASON
ciscoasa(config-aaa-server-host)# action-uri =0&METHOD=GET&SMAGENTNAME=$SM$5FZmjnk
ciscoasa(config-aaa-server-host)# action-uri 3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6r
ciscoasa(config-aaa-server-host)# action-uri B1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F
ciscoasa(config-aaa-server-host)# action-uri %2Fauth.example.com
ciscoasa(config-aaa-server-host)#
```

(注) アクション URI にホスト名とプロトコルを含める必要があります。上記の例では、これらは URI の最初にある http://www.example.com に含まれています。

関連コマンド

コマンド	説明
auth-cookie-name	認証クッキーの名前を指定します。
hidden-parameter	SSO サーバとの交換に使用する非表示パラメータを作成します。
password-parameter	SSO 認証用にユーザ パスワードを送信する必要がある HTTP POST 要求パラメータの名前を指定します。
start-url	プリログイン クッキーを取得する URL を指定します。
user-parameter	SSO 認証用にユーザ名を送信する必要がある HTTP POST 要求のパラメータの名前を指定します。

activate-tunnel-group-script

このコマンドは、tunnel-group sub-mode で username-from-certificate が設定されている場合に、ASDM によって生成されたスクリプト ファイルをリロードするために内部で使用されます。

(注) このコマンドは、ASA CLI では使用しないでください。

activation-key

ASA にライセンス アクティベーション キーを入力するには、特権 EXEC モードで **activation-key** コマンドを使用します。

activation-key [**noconfirm**] *activation_key* [**activate** | **deactivate**]

構文の説明

activate	時間ベースのアクティベーション キーをアクティブ化します。**activate** がデフォルト値です。特定の機能に対して最後にアクティブ化した時間ベース キーがアクティブになります。
activation_key	アクティベーション キーを ASA に適用します。*activation_key* は、各要素の間にスペースを 1 つ入れた 5 つの要素から構成される 16 進数のストリングです。先頭の 0x 指定子は任意です。すべての値が 16 進数と見なされます。 1 つの永続キーおよび複数の時間ベース キーをインストールできます。新しい永続キーを入力した場合、すでにインストール済みのキーが上書きされます。
deactivate	時間ベースのアクティベーション キーを非アクティブ化します。非アクティブ化した場合でも、アクティベーション キーは ASA にインストールされたままです。後で **activate** キーワードを使用してアクティブ化できます。キーの初回入力時で、**deactivate** を指定した場合、キーは ASA に非アクティブ ステートでインストールされます。
noconfirm	(オプション)確認を求めるプロンプトを表示せずにアクティベーション キーを入力します。

デフォルト

デフォルトでは、ASA は、ライセンスがすでにインストールされた状態で出荷されます。このライセンスは、注文した内容およびベンダーがインストールした内容に応じて、ライセンスを追加できる基本ライセンスの場合と、すべてのライセンスがすでにインストールされている場合があります。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。

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	—	•

コマンド履歴

リリース	変更内容
7.0(5)	次の制限値が増加されました。 • ASA5510 Base ライセンス接続は 32000 から 5000 に、VLAN は 0 から 10 に増加。 • ASA5510 Security Plus ライセンス接続は 64000 から 130000 に、VLAN は 10 から 25 に増加。 • ASA5520 接続は 130000 から 280000 に、VLAN は 25 から 100 に増加。 • ASA5540 接続は 280000 から 400000 に、VLAN は 100 から 200 に増加。
7.1(1)	SSL VPN ライセンスが追加されました。
7.2(1)	5000 ユーザの SSL VPN ライセンスが ASA 5550 以降に対して追加されました。
7.2(2)	• ASA 5505 ASA上の Security Plus ライセンスに対する VLAN 最大数が、5(3 つのフル機能インターフェイス、1 つのフェールオーバー インターフェイス、1 つのバックアップ インターフェイスに制限されるインターフェイス)から 20 のフル機能インターフェイスに増加されました。また、トランク ポート数も 1 から 8 に増加されました。 • VLAN の制限値が変更されました。ASA 5510 の基本ライセンスでは 10 から 50 に、Security Plus ライセンスでは 25 から 100 に、ASA 5520 では 100 から 150 に、ASA 5550 では 200 から 250 に増えています。
7.2(3)	ASA 5510 は、GE(ギガビット イーサネット)を Security Plus ライセンスのあるポート 0 および 1 でサポートします。ライセンスを Base から Security Plus にアップグレードした場合、外部 Ethernet 0/0 および Ethernet 0/1 ポートの容量は、元の FE(ファスト イーサネット)の 100 Mbps から GE の 1000 Mbps に増加します。インターフェイス名は Ethernet 0/0 および Ethernet 0/1 のままです。**speed** コマンドを使用してインターフェイスの速度を変更します。また、**show interface** コマンドを使用して各インターフェイスの現在の設定速度を確認します。
8.0(2)	• Advanced Endpoint Assessment ライセンスが追加されました。 • VPN ロードバランシングが ASA 5510 Security Plus ライセンスでサポートされます。
8.0(3)	AnyConnect for Mobile ライセンスが追加されました。
8.0(4)/8.1(2)	時間ベース ライセンスが追加されました。
8.1(2)	ASA 5580 上でサポートされる VLAN 数が 100 から 250 に増加されました。
8.0(4)	UC Proxy セッション ライセンスが追加されました。
8.2(1)	• ボットネット トラフィック フィルタ ライセンスが追加されました。 • AnyConnect Essentials ライセンスが追加されました。デフォルトで、ASA は AnyConnect Essentials ライセンスを使用します。これをディセーブルにして他のライセンスを使用するには、**no anyconnect-essentials** コマンドを使用します。 • SSL VPN の共有ライセンスが追加されました。
8.2(2)	モビリティ プロキシに UC Proxy ライセンスが必要なくなりました。

リリース	変更内容
8.3(1)	• フェールオーバー ライセンスが各ユニット上で同一である必要がなくなりました。両方のユニットで使用するライセンスは、プライマリ ユニットおよびセカンダリ ユニットからの結合されたライセンスです。 • 時間ベース ライセンスがスタッカブルになりました。 • IME ライセンスが追加されました。 • 時間ベース ライセンスを複数インストールできるようになり、同時に機能ごとに 1 つのアクティブなライセンスを保持できます。 • **activate** キーワードまたは **deactivate** キーワードを使用して、時間ベース ライセンスをアクティブ化または非アクティブ化できます。
8.4(1)	• ASA 5550 および ASA 5585-X（SSP-10）では、コンテキストの最大数が 50 から 100 に引き上げられました。ASA 5580 および 5585-X（SSP-20）以降では、コンテキストの最大数が 50 から 250 に引き上げられました。 • ASA 5580 および ASA 5585-X では、VLAN の最大数が 250 から 1024 に引き上げられました。 • ファイアウォール接続の最大数が次のように引き上げられました。 – ASA 5580-20：1,000 K から 2,000 K へ – ASA 5580-40：2,000 K から 4,000 K へ – ASA 5585-X（SSP-10 搭載）：750 K から 1,000 K へ – ASA 5585-X（SSP-20 搭載）：1,000 K から 2,000 K へ – ASA 5585-X（SSP-40 搭載）：2,000 K から 4,000 K へ – ASA 5585-X（SSP-60 搭載）：2,000 K から 10,000 K へ • ASA 5580 の場合、AnyConnect VPN セッションの制限が 5,000 から 10,000 に引き上げられました。 • ASA 5580 の場合、その他の VPN セッションの制限が 5,000 から 10,000 に引き上げられました。 • AnyConnect Essentials ライセンスおよび AnyConnect Premium ライセンスに IKEv2 を使用した IPsec リモート アクセス VPN が追加されました。 • Other VPN ライセンス（以前の IPsec VPN）にはサイトツーサイト セッションが追加されました。 • ペイロード暗号化機能のないモデルでは（ASA 5585-X など）、ASA ソフトウェアは ASA で特定の国にエクスポートできるようにして、Unified Communications と VPN 機能をディセーブルにします。

使用上のガイドライン

アクティベーション キーの取得

アクティベーション キーを取得するには、シスコの代理店から購入できる Product Authorization Key が必要になります。機能ライセンスごとに個別の製品アクティベーション キーを購入する必要があります。たとえば、基本ライセンスがある場合は、Advanced Endpoint Assessment 用と追加の SSL VPN セッション用に別々のキーを購入する必要があります。

製品認証キーを取得した後、次のいずれかの URL の Cisco.com でキーを登録する必要があります。

- Cisco.com の登録済みユーザの場合は、次の Web サイトを使用します。

  http://www.cisco.com/go/license

- Cisco.com の登録済みユーザではない場合は、次の Web サイトを使用します。

  http://www.cisco.com/go/license/public

コンテキスト モードのガイドライン

- マルチ コンテキスト モードでシステム実行スペース内にアクティベーション キーを適用します。
- 共有ライセンスは、マルチ コンテキスト モードではサポートされていません。

フェールオーバーのガイドライン

- 共有ライセンスは、アクティブ/アクティブ モードではサポートされていません。
- フェールオーバー ユニットは、各ユニット上で同一のライセンスを必要としません。

  旧バージョンの ASA ソフトウェアは、各ユニット上のライセンスが一致する必要がありました。バージョン 8.3(1) から、同一のライセンスをインストールする必要がなくなりました。通常、ライセンスをプライマリ ユニット専用に購入します。アクティブ/スタンバイ フェールオーバーでは、セカンダリ ユニットがアクティブになるとプライマリ ライセンスを継承します。両方のユニット上にライセンスがある場合、これらのライセンスは単一の実行フェールオーバー クラスタ ライセンスに結合されます。

- ASA 5505 および 5510 では、両方の装置に Security Plus ライセンスが必要です。基本ライセンスはフェールオーバーをサポートしないため、基本ライセンスのみを保持するスタンバイ装置ではフェールオーバーをイネーブルにできません。

アップグレードとダウングレードのガイドライン

任意の旧バージョンから最新バージョンにアップグレードした場合、アクティベーション キーの互換性は存続します。ただし、ダウングレード機能の維持には問題が生じる場合があります。

- バージョン 8.1 以前にダウングレードする場合:アップグレード後に、*8.2 より前*に追加された機能のライセンスを追加でアクティブ化すると、ダウングレードした場合でも旧バージョンに対するアクティベーション キーの互換性は存続します。ただし、*8.2 以降*に追加された機能ライセンスをアクティブ化した場合は、アクティベーション キーの下位互換性がなくなります。互換性のないライセンス キーがある場合は、次のガイドラインを参照してください。
  - 旧バージョンでアクティベーション キーを入力した場合は、そのキーが ASA で使用されます(バージョン 8.2 以降でアクティブ化した新しいライセンスがない場合)。
  - 新しいシステムで、以前のアクティベーション キーがない場合は、旧バージョンと互換性のある新しいアクティベーション キーを要求する必要があります。

- バージョン 8.2 以前にダウングレードする場合：バージョン 8.3 では、より堅牢な時間ベース キーの使用およびフェールオーバー ライセンスの変更が次のとおり追加されました。
  - 複数の時間ベースのアクティベーション キーがアクティブな場合、ダウングレード時には一番最近アクティブ化された時間ベース キーのみがアクティブになれます。他のキーはすべて非アクティブ化されます。
  - フェールオーバー ペアに不一致のライセンスがある場合、ダウングレードによりフェールオーバーはディセーブルになります。キーが一致した場合でも、使用するライセンスは、結合されたライセンスではなくなります。

その他のガイドラインと制限事項

- アクティベーション キーは、コンフィギュレーション ファイルには保存されません。隠しファイルとしてフラッシュ メモリに保存されます。
- アクティベーション キーは、デバイスのシリアル番号に関連付けられます。機能ライセンスは、デバイス間で転送できません（ハードウェア障害の発生時を除く）。ハードウェア障害が発生したためにデバイスを交換する必要がある場合は、シスコのライセンス チームに連絡して、既存のライセンスを新しいシリアル番号に転送するよう依頼してください。シスコのライセンス チームから、製品認証キーの参照番号と既存のシリアル番号を求められます。
- 購入後に、返金またはアップグレードしたライセンスのためにライセンスを返却できません。
- すべてのライセンス タイプをアクティブ化できますが、たとえば、マルチ コンテキスト モードおよび VPN など一部の機能には相互互換性がありません。AnyConnect Essentials ライセンスの場合、次のライセンスとは互換性がありません。SSL VPN フル ライセンス、SSL VPN 共有ライセンス、および Advanced Endpoint Assessment ライセンス。デフォルトでは、AnyConnect Essentials ライセンスがこれらのライセンスの代わりに使用されます。設定の AnyConnect Essentials ライセンスをディセーブルにして他のライセンスを使用するように復元するには、**no anyconnect-essentials** コマンドを使用します。
- 一部の永続ライセンスでは、アクティブ化後に ASA をリロードする必要があります。表 2-1 に、リロードが必要なライセンスを示します。

表 2-1　永続ライセンスのリロード要件

モデル	リロードが必要なライセンス アクション
ASA 5505 および ASA 5510	基本ライセンスと Security Plus ライセンスの切り替え
すべてのモデル	暗号化ライセンスの変更
すべてのモデル	永続ライセンスのダウングレード（たとえば、10 個のコンテキストから 2 個のコンテキストへ）。

例

次に、ASA のアクティベーション キーを変更する例を示します。

```
ciscoasa# activation-key 0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490
```

次に、**activation-key** コマンドの出力例を示します。ここでは、新しいアクティベーション キーが古いアクティベーション キーと異なる場合のフェールオーバーに対する出力が示されています。

```
ciscoasa# activation-key 0xyadayada 0xyadayada 0xyadayada 0xyadayada 0xyadayada

Validating activation key. This may take a few minutes...
The following features available in the running permanent activation key are NOT available
in the new activation key:
```

```
Failover is different.
   running permanent activation key: Restricted (R)
   new activation key: Unrestricted (UR)
WARNING: The running activation key was not updated with the requested key.
Proceed with updating flash activation key? [y]
Flash permanent activation key was updated with the requested key.
```

次に、ライセンス ファイルの出力例を示します。

```
Serial Number Entered: 123456789ja
Number of Virtual Firewalls Selected: 10
Formula One device: ASA 5520

Failover                        : Enabled
VPN-DES                         : Enabled
VPN-3DES-AES                    : Enabled
Security Contexts               : 10
GTP/GPRS                        : Disabled
SSL VPN Peers                   : Default
Total VPN Peers                 : 750
Advanced Endpoint Assessment    : Disabled
AnyConnect for Mobile           : Enabled
AnyConnect for Cisco VPN Phone  : Disabled
Shared License                  : Disabled
UC Phone Proxy Sessions         : Default
Total UC Proxy Sessions         : Default
AnyConnect Essentials           : Disabled
Botnet Traffic Filter           : Disabled
Intercompany Media Engine       : Enabled

----------------------------------------
THE FOLLOWING ACTIVATION KEY IS VALID FOR:
ASA SOFTWARE RELEASE 8.2+ ONLY.

Platform = asa

123456789JA:yadayda1 yadayda1 yadayda1 yadayda1 yadayda1
----------------------------------------
THE FOLLOWING ACTIVATION KEY IS VALID FOR:
ALL ASA SOFTWARE RELEASES, BUT EXCLUDES ANY
8.2+ FEATURES FOR BACKWARDS COMPATIBILITY.

Platform = asa

123456789JA:yadayda2 yadayda2 yadayda2 yadayda2 yadayda2
```

関連コマンド

コマンド	説明
anyconnect-essentials	AnyConnect Essentials ライセンスをイネーブルまたはディセーブルにします。
show activation-key	アクティベーション キーを表示します。
show version	ソフトウェア バージョンおよびアクティベーション キーを表示します。

activex-relay

クライアントレス ポータルに ActiveX を必要とするアプリケーションを埋め込むには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで **activex-relay** コマンドを使用します。デフォルトのグループ ポリシーから **activex-relay** コマンドを継承するには、このコマンドの **no** 形式を使用します。

activex-relay {**enable** | **disable**}

no activex-relay

構文の説明

enable	WebVPN セッションの ActiveX をイネーブルにします。
disable	WebVPN セッションの ActiveX をディセーブルにします。

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
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザ名 webvpn 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。

使用上のガイドライン

オブジェクト タグがある HTML コンテンツ（画像、オーディオ、ビデオ、Java アプレット、ActiveX、PDF、またはフラッシュなど）に対する ActiveX をユーザが WebVPN ブラウザから起動できるようにするには、**activex-relay enable** コマンドを使用します。これらのアプリケーションでは、WebVPN セッションを使用して ActiveX コントロールをダウンロードおよびアップロードします。ActiveX リレーは、WebVPN セッションが閉じるまで有効です。Microsoft OWA 2007 などを使用する場合は、ActiveX をディセーブルにする必要があります。

（注） これらには同じ機能があるため、スマート トンネルをディセーブルにしても、**activex-relay enable** コマンドによってスマート トンネルのログが生成されます。

次に、特定のグループ ポリシーに関連付けられている WebVPN セッションの ActiveX コントロールをイネーブルにする例を示します。

```
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# activex-relay enable
```

次に、特定のユーザ名に関連付けられている WebVPN セッションの ActiveX コントロールをディセーブルにする例を示します。

```
ciscoasa(config-username-policy)# webvpn
ciscoasa(config-username-webvpn)# activex-relay disable
```

ad-agent-mode

Cisco アイデンティティ ファイアウォール インスタンスの Active Directory エージェントを設定できるように AD エージェント モード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 **ad-agent-mode** コマンドを使用します。

ad-agent-mode

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
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(2)	このコマンドが追加されました。

使用上のガイドライン

アイデンティティ ファイアウォールに対して Active Directory エージェントを設定するには、**aaa-server** コマンドのサブモードである **ad-agent-mode** コマンドを入力します。**ad-agent-mode** コマンドを入力すると、AAA サーバ グループ コンフィギュレーション モードが開始されます。

AD エージェントは、定期的に、または要求に応じて、WMI を介して Active Directory サーバのセキュリティ イベント ログ ファイルをモニタし、ユーザのログインおよびログオフ イベントを調べます。AD エージェントは、ユーザ ID および IP アドレス マッピングのキャッシュを保持し、ASA に変更を通知します。

AD エージェント サーバ グループのプライマリ AD エージェントとセカンダリ AD エージェントを設定します。プライマリ AD エージェントが応答していないことを ASA が検出し、セカンダリ AD エージェントが指定されている場合、ASA はセカンダリ AD エージェントに切り替えます。AD エージェントの Active Directory サーバは、通信プロトコルとして RADIUS を使用します。そのため、ASA と AD エージェントとの共有秘密のキー属性を指定する必要があります。

例

次に、アイデンティティ ファイアウォールの Active Directory エージェントを設定するときに、**ad-agent-mode** をイネーブルにする例を示します。

```
ciscoasa(config)# aaa-server adagent protocol radius
ciscoasa(config)# ad-agent-mode
ciscoasa(config-aaa-server-group)# aaa-server adagent (inside) host 192.168.1.101
ciscoasa(config-aaa-server-host)# key mysecret
ciscoasa(config-aaa-server-hostkey)# user-identity ad-agent aaa-server adagent
ciscoasa(config-aaa-server-host)# test aaa-server ad-agent
```

関連コマンド

コマンド	説明
aaa-server	AAA サーバ グループを作成し、グループ固有の AAA サーバ パラメータとすべてのグループ ホストに共通の AAA サーバ パラメータを設定します。
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

address（ダイナミック フィルタ ブラックリスト、ホワイトリスト）

IP アドレスをボットネット トラフィック フィルタのブラックリストまたはホワイトリストに追加するには、ダイナミック フィルタ ブラックリストまたはホワイトリスト コンフィギュレーション モードで **address** コマンドを使用します。アドレスを削除するには、このコマンドの **no** 形式を使用します。

address *ip_address mask*

no address *ip_address mask*

構文の説明

ip_address	ブラックリストに IP アドレスを追加します。
mask	IP アドレスのサブネット マスクを定義します。*mask* には、単一ホストまたはサブネットのマスクを指定できます。

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
ダイナミック フィルタ ブラックリストまたはホワイトリスト 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
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

スタティック データベースを使用すると、ホワイトリストまたはブラックリストに追加するドメイン名または IP アドレスでダイナミック データベースを増強できます。ダイナミック フィルタ ホワイトリストまたはブラックリスト コンフィギュレーション モードを開始した後、**address** コマンドおよび **name** コマンドを使用して、適切な名前としてホワイトリストに、または不適切な名前としてブラックリストにタグ付けするドメイン名または IP アドレス（ホストまたはサブネット）を手動で入力できます。

このコマンドを複数回入力して、複数のエントリを追加できます。最大 1000 個のブラックリスト エントリと、最大 1000 個のホワイトリスト エントリを追加できます。

例

次に、ブラックリストおよびホワイトリストのエントリを作成する例を示します。

```
ciscoasa(config)# dynamic-filter blacklist
ciscoasa(config-llist)# name bad1.example.com
ciscoasa(config-llist)# name bad2.example.com
ciscoasa(config-llist)# address 10.1.1.1 255.255.255.0
ciscoasa(config-llist)# dynamic-filter whitelist
ciscoasa(config-llist)# name good.example.com
ciscoasa(config-llist)# name great.example.com
ciscoasa(config-llist)# name awesome.example.com
ciscoasa(config-llist)# address 10.1.1.2 255.255.255.255
```

関連コマンド

コマンド	説明
clear configure dynamic-filter	実行ボットネット トラフィック フィルタ コンフィギュレーションをクリアします。
clear dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピング データをクリアします。
clear dynamic-filter reports	ボットネット トラフィック フィルタのレポート データをクリアします。
clear dynamic-filter statistics	ボットネット トラフィック フィルタの統計情報をクリアします。
dns domain-lookup	サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにします。
dns server-group	ASA の DNS サーバを指定します。
dynamic-filter blacklist	ボットネット トラフィック フィルタのブラックリストを編集します。
dynamic-filter database fetch	ボットネット トラフィック フィルタのダイナミック データベースを手動で取得します。
dynamic-filter database find	ドメイン名または IP アドレスをダイナミック データベースから検索します。
dynamic-filter database purge	ボットネット トラフィック フィルタのダイナミック データベースを手動で削除します。
dynamic-filter enable	アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネット トラフィック フィルタをイネーブルにします。
dynamic-filter updater-client enable	ダイナミック データベースのダウンロードをイネーブルにします。
dynamic-filter use-database	ダイナミック データベースの使用をイネーブルにします。
dynamic-filter whitelist	ボットネット トラフィック フィルタのホワイトリストを編集します。
inspect dns dynamic-filter-snoop	DNS インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。
name	ブラックリストまたはホワイトリストに名前を追加します。
show asp table dynamic-filter	高速セキュリティ パスにインストールされているボットネット トラフィック フィルタ ルールを表示します。

コマンド	説明
show dynamic-filter data	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプル エントリなど、ダイナミック データベースに関する情報を表示します。
show dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。**detail** キーワードを指定した場合は、実際の IP アドレスおよび名前を表示します。
show dynamic-filter reports	上位 10 個のボットネット サイト、ポート、および感染したホストに関するレポートを生成します。
show dynamic-filter statistics	ボットネット トラフィック フィルタでモニタされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。
show dynamic-filter updater-client	サーバの IP アドレス、ASA が次にサーバに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデート サーバに関する情報を表示します。
show running-config dynamic-filter	ボットネット トラフィック フィルタの実行コンフィギュレーションを表示します。

address（media-termination）（廃止）

電話プロキシ機能へのメディア接続に使用するメディア ターミネーション インスタンスのアドレスを指定するには、メディア ターミネーション コンフィギュレーション モードで **address** コマンドを使用します。メディア ターミネーション コンフィギュレーションからアドレスを削除するには、このコマンドの **no** 形式を使用します。

address *ip_address* [**interface** *intf_name*]

no address *ip_address* [**interface** *intf_name*]

構文の説明

interface *intf_name*	メディア ターミネーション アドレスを使用するインターフェイスの名前を指定します。1 つのインターフェイスに設定できるメディア ターミネーション アドレスは 1 つだけです。
ip_address	メディア ターミネーション インスタンスに使用する IP アドレスを指定します。

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
メディア ターミネーション 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。
9.4(1)	このコマンドは、すべての **phone-proxy** および **uc-ime** コマンドとともに廃止されました。

使用上のガイドライン

ASA では、次の基準を満たすメディア ターミネーションの IP アドレスが設定されている必要があります。

- メディア ターミネーション インスタンスでは、すべてのインターフェイスに対してグローバルなメディア ターミネーション アドレスを設定することも、インターフェイスごとにメディア ターミネーション アドレスを設定することもできます。しかし、グローバルなメディア ターミネーション アドレスと、インターフェイスごとに設定するメディア ターミネーション アドレスは同時に使用できません。
- 複数のインターフェイスに対してメディア ターミネーション アドレスを設定する場合、IP 電話との通信時に ASA で使用するアドレスを、インターフェイスごとに設定する必要があります。
- IP アドレスは、そのインターフェイスのアドレス範囲内で使用されていない、パブリックにルーティング可能な IP アドレスです。

例

次に、media-termination address コマンドを使用して、メディア接続に使用する IP アドレスを指定する例を示します。

```
ciscoasa(config)# media-termination mediaterm1
ciscoasa(config-media-termination)# address 192.0.2.25 interface inside
ciscoasa(config-media-termination)# address 10.10.0.25 interface outside
```

関連コマンド

コマンド	説明
phone-proxy	Phone Proxy インスタンスを設定します。
media-termination	電話プロキシ インスタンスに適用するメディア ターミネーション インスタンスを設定します。

address-family ipv4

標準 IP Version 4（IPv4）アドレス プレフィックスを使用してルーティング セッションを設定するためのアドレス ファミリを入力するには、ルータ コンフィギュレーション モードで **address-family ipv4** コマンドを使用します。アドレス ファミリ コンフィギュレーション モードを終了し、実行コンフィギュレーションから IPv4 アドレス ファミリ 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。

address-family ipv4

no address-family ipv4

デフォルト

IPv4 アドレス プレフィックスはイネーブルではありません。

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		
	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
ルータ モード 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
9.2(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

address-family ipv4 コマンドは、コンテキスト ルータをアドレス ファミリ コンフィギュレーション モードにします。このルータから、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定できます。アドレス ファミリ コンフィギュレーション モードを終了し、ルータ コンフィギュレーション モードに戻るには、**exit** と入力します。

（注） アドレス ファミリ IPv4 のルーティング情報が、**neighbor remote-as** コマンドを使用して設定した各 BGP ルーティング セッションにデフォルトでアドバタイズされます。ただし、**neighbor remote-as** コマンドを設定する前に **no bgp default ipv4-unicast** コマンドを入力している場合は除きます。

例

次に、ルータを IPv4 アドレス ファミリのアドレス ファミリ コンフィギュレーション モードにする例を示します。

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)#
```

関連コマンド

コマンド	説明
bgp default ipv4-unicast	BGP ピアリング セッションのデフォルトとして IP Version 4（IPv4）ユニキャスト アドレス ファミリを設定します。
neighbor remote-as	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。

address-family ipv6

標準 IP Version 6（IPv6）アドレス プレフィックスを使用してルーティング セッション（BGP など）を設定するためのアドレス ファミリを入力するには、ルータ コンフィギュレーション モードで **address-family ipv6** コマンドを使用します。アドレス ファミリ コンフィギュレーション モードを終了し、実行コンフィギュレーションから IPv6 アドレス ファミリ 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。

address-family ipv6 [unicast]

no address-family ipv6

構文の説明

unicast	（オプション）IPv6 ユニキャスト アドレス プレフィックスを指定します。

デフォルト

IPv6 アドレス プレフィックスはイネーブルではありません。IPv6 アドレス プレフィックスが設定されている場合は、ユニキャスト アドレス プレフィックスがデフォルトです。

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
ルータ モード 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
9.3(2)	このコマンドが追加されました。

使用上のガイドライン

address-family ipv6 コマンドは、コンテキスト ルータをアドレス ファミリ コンフィギュレーション モードにします。このルータから、標準 IPv6 アドレス プレフィックスを使用するルーティング セッションを設定できます。アドレス ファミリ コンフィギュレーション モードを終了し、ルータ コンフィギュレーション モードに戻るには、**exit** と入力します。

例

次に、ルータを IPv4 アドレス ファミリのアドレス ファミリ コンフィギュレーション モードにする例を示します。

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv6
ciscoasa(config-router-af)#
```

関連コマンド

コマンド	説明
neighbor ipv6-address activate	BGP ネイバーとの情報交換をイネーブルにします。

address-pool

アドレスをリモート クライアントに割り当てるためのアドレス プールのリストを指定するには、トンネル グループ一般属性コンフィギュレーション モードで **address-pool** コマンドを使用します。アドレス プールを削除するには、このコマンドの **no** 形式を使用します。

address-pool [(*interface name*)] *address_pool1* [*...address_pool6*]

no address-pool [(*interface name*)] *address_pool1* [*...address_pool6*]

構文の説明

address_pool	**ip local pool** コマンドで設定したアドレス プールの名前を指定します。最大 6 個のローカル アドレス プールを指定できます。
interface name	（任意）アドレス プールに使用するインターフェイスを指定します。

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
トンネル グループ一般属性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

これらのコマンドは、インターフェイスごとに 1 つずつ、複数入力できます。インターフェイスが指定されていない場合、コマンドは明示的に参照されていないインターフェイスすべてに対してデフォルトを指定します。

グループ ポリシーの **address-pools** コマンドによるアドレス プール設定は、トンネル グループの **address-pool** コマンドによるローカル プール設定を上書きします。

プールの指定順序は重要です。ASA では、このコマンドでプールを指定した順序に従って、それらのプールからアドレスが割り当てられます。

例

次に、設定トンネル一般コンフィギュレーション モードで、IPsec リモート アクセス トンネル グループ テスト用にアドレスをリモート クライアントに割り当てるためのアドレス プールのリストを指定する例を示します。

```
ciscoasa(config)# tunnel-group test type remote-access
ciscoasa(config)# tunnel-group test general
ciscoasa(config-tunnel-general)# address-pool (inside) addrpool1 addrpool2 addrpool3
ciscoasa(config-tunnel-general)#
```

関連コマンド

コマンド	説明
ip local pool	VPN リモート アクセス トンネルに使用する IP アドレス プールを設定します。
clear configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group-map default-group	**crypto ca certificate map** コマンドを使用して作成された証明書マップ エントリをトンネル グループに関連付けます。

address-pools

アドレスをリモート クライアントに割り当てるためのアドレス プールのリストを指定するには、グループ ポリシー属性コンフィギュレーション モードで **address-pools** コマンドを使用します。グループ ポリシーから属性を削除し、別のグループ ポリシー ソースからの継承をイネーブルにするには、このコマンドの **no** 形式を使用します。

address-pools value *address_pool1* [*...address_pool6*]

no address-pools value *address_pool1* [*...address_pool6*]

address-pools none

no address-pools none

構文の説明

address_pool	**ip local pool** コマンドで設定したアドレス プールの名前を指定します。最大 6 個のローカル アドレス プールを指定できます。
none	アドレス プールを設定しないことを指定し、他のグループ ポリシーからの継承をディセーブルにします。
value	アドレスの割り当てに使用する最大 6 個のアドレス プールのリストを指定します。

デフォルト

デフォルトでは、アドレス プールの属性は継承を許可します。

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
グループ ポリシー属性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
7.2(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

このコマンドによるアドレス プール設定は、グループ内のローカル プール設定を上書きします。ローカル アドレスの割り当てに使用する最大 6 個のローカル アドレス プールのリストを指定できます。

プールの指定順序は重要です。ASA では、このコマンドでプールを指定した順序に従って、それらのプールからアドレスが割り当てられます。

address-pools none コマンドは、この属性が他のポリシー（DefaultGrpPolicy など）から継承されないようにします。**no address pools none** コマンドは、**address-pools none** コマンドをコンフィギュレーションから削除して、デフォルト値（継承の許可）に戻します。

例

次に、GroupPolicy1 の設定一般コンフィギュレーション モードで、アドレスをリモート クライアントに割り当てるために使用するアドレス プールのリストとして pool_1 および pool_20 を設定する例を示します。

```
ciscoasa(config)# ip local pool pool_1 192.168.10.1-192.168.10.100 mask 255.255.0.0
ciscoasa(config)# ip local pool pool_20 192.168.20.1-192.168.20.200 mask 255.255.0.0
ciscoasa(config)# group-policy GroupPolicy1 attributes
ciscoasa(config-group-policy)# address-pools value pool_1 pool_20
ciscoasa(config-group-policy)#
```

関連コマンド

コマンド	説明
ip local pool	VPN グループ ポリシーで使用する IP アドレス プールを設定します。
clear configure group-policy	設定されているすべてのグループ ポリシーをクリアします。
show running-config group-policy	すべてのグループ ポリシーまたは特定のグループ ポリシーのコンフィギュレーションを表示します。

admin-context

システム コンフィギュレーションの管理コンテキストを設定するには、グローバル コンフィギュレーション モードで **admin-context** コマンドを使用します。

admin-context *name*

構文の説明

name	名前を最大 32 文字のストリングで設定します。コンテキストをまだ定義していない場合は、まずこのコマンドで管理コンテキスト名を指定します。次に、**context** コマンドを使用して最初に追加するコンテキストを、指定した管理コンテキスト名にする必要があります。 この名前では大文字と小文字が区別されるため、たとえば、「customerA」および「CustomerA」という 2 つのコンテキストを保持できます。文字、数字、またはハイフンを使用できますが、名前の先頭または末尾にハイフンは使用できません。 「System」および「Null」（大文字と小文字の両方）は予約されている名前であり、使用できません。

デフォルト

マルチ コンテキスト モードの新しい ASA の場合、管理コンテキスト名は「admin」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
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

コンテキスト コンフィギュレーションが内部フラッシュ メモリにある限り、任意のコンテキストを管理コンテキストに設定できます。

現在の管理コンテキストを削除するには、**clear configure context** コマンドを使用してすべてのコンテキストを削除する必要があります。

システム コンフィギュレーションには、システム自体のネットワーク インターフェイスまたはネットワーク設定は含まれません。代わりに、システムは、ネットワーク リソースにアクセスする必要がある場合に（ASA ソフトウェアをダウンロードしたり、管理者に対してリモート アクセスを許可する場合など）、管理コンテキストとして指定されたコンテキストのいずれかを使用します。

例

次に、管理コンテキストを「administrator」に設定する例を示します。

```
ciscoasa(config)# admin-context administrator
```

関連コマンド

コマンド	説明
clear configure context	システム コンフィギュレーションからすべてのコンテキストを削除します。
context	システム コンフィギュレーションにコンテキストを設定し、コンテキスト コンフィギュレーション モードを開始します。
show admin-context	現在の管理コンテキスト名を表示します。

advertise passive-only

パッシブ インターフェイスに属するプレフィックスだけをアドバタイズするように IS-IS 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 **advertise passive-only** コマンドを使用します。制限を削除するには、このコマンドの **no** 形式を使用します。

advertise passive-only

no advertise passive-only

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

このコマンドには、デフォルトの動作はありません。

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
ルータ isis 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

このコマンドは、リンクステート パケット（LSP）アドバタイズメントから、接続されたネットワークの IP プレフィックスを除外し、IS-IS コンバージェンス時間を削減するための IS-IS メカニズムです。

IS-IS インスタンスごとにこのコマンドを設定すると、ルータの非疑似ノード LSP でアドバタイズされるプレフィックスの数が少なくなるため、IS-IS コンバージェンス時間の削減という課題をスケーラブルに解決することができます。

このコマンドは、「ループバック インターフェイスで IS-IS をイネーブルにする場合、通常、ループバックを受動に設定する」という事実に依存しています。この設定は、ループバックの背後にネイバーが見つかる可能性はないため、ループバックを通じて、必要のない Hello パケットの送信を防ぐために行われます。したがって、アドバタイズする必要があるものがループバックだけで、このループバックがすでに受動に設定されている場合、IS-IS インスタンスごとに **advertise passive-only** コマンドを設定することにより、ルーティング テーブルのデータ過剰を防ぐことができます。

このコマンドの代わりは **no isis advertise-prefix** コマンドです。**no isis advertise-prefix** コマンドは、インターフェイスごとに設定される、規模の小さいソリューションです。

例

次に、**advertise passive-only** コマンドを使用する例を示します。このコマンドは、IS-IS インスタンスに作用し、イーサネット インターフェイス 0 の IP ネットワークのアドバタイズを阻止します。ループバック インターフェイス 0 の IP アドレスだけがアドバタイズされます。

```
!
!
!
interface Gi0/0
 ip address 192.168.20.1 255.255.255.0
router isis
!.
int gi0/1
  ip add 171.1.1.1 255.255.255.0
   router isis
!.
router isis
 passive-interface outside
 net 47.0004.004d.0001.0001.0c11.1111.00
 advertise-passive-only
 log-adjacency-changes
!
```

関連コマンド

コマンド	説明
area-password	IS-IS エリア認証パスワードを設定します。
authentication key	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。

コマンド	説明
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。
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。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
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。
protocol shutdown	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。

コマンド	説明
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。

aggregate-address

Border Gateway Protocol（BGP）データベース内に集約エントリを作成するには、アドレス ファミリ コンフィギュレーション モードで **aggregate-address** 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。

aggregate-address *address mask* [**as-set**] [**summary-only] [suppress-map** *map-name*]**[advertise-map** *map-name*] [**attribute-map** *map-name*]

no aggregate-address *address mask* [**as-set**] [**summary-only] [suppress-map** *map-name*]**[advertise-map** *map-name*] [**attribute-map** *map-name*]

構文の説明

address	集約アドレス。
mask	集約マスク。
as-set	（オプション）自律システム設定パス情報を生成します。
summary-only	（任意）アップデートからのすべてのより具体的なルートをフィルタ処理します。
suppress-map *map-name*	（オプション）抑制するルートの選択に使用されるルート マップの名前を指定します。
advertise-map *map-name*	（オプション）AS_SET 送信元コミュニティを作成するルートの選択に使用されるルート マップの名前を指定します。
attribute-map *map-name*	（オプション）集約ルートの属性を設定するために使用されるルート マップの名前を指定します。

デフォルト

アトミック集約属性は、**as-set** キーワードが指定されない限り、このコマンドによって集約ルートが作成されるときに自動的に設定されます。

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
コンテキスト コンフィギュレーション、アドレス ファミリ 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
9.2(1)	このコマンドが追加されました。
9.3(2)	このコマンドは、アドレス ファミリ ipv6 サブモードでサポートされるように変更されました。

使用上のガイドライン

集約ルートを BGP またはマルチプロトコル BGP（mBGP）に再配布するか、条件付きの集約ルーティング機能を使用することにより、BGP および mBGP に集約ルーティングを実装できます。

キーワードなしで **aggregate-address** コマンドを使用すると、指定された範囲内にあるより具体的な BGP または mBGP ルートが使用できる場合、BGP または mBGP ルーティング テーブルに集約エントリが作成されます（集約に一致する長いプレフィックスは、ルーティング情報ベース（RIB）に存在する必要があります）。集約ルートは自律システムからのルートとしてアドバタイズされます。また、この集約ルートには、情報が失われている可能性を示すために、アトミック集約属性が設定されます（アトミック集約属性は、**as-set** キーワードを指定しない限りデフォルトで設定されます）。

as-set キーワードを使用すると、コマンドがこのキーワードなしで従う同じルールを使用する集約エントリが作成されますが、このルートにアドバタイズされるパスは、集約されているすべてのパス内に含まれるすべての要素で構成される AS_SET になります。このルートは集約されたルート変更に関する自律システム パス到着可能性情報として継続的に削除してアップデートする必要があるため、多くのパスを集約する際に **aggregate-address** コマンドのこの形式を使用しないでください。

summary-only キーワードを使用すると、集約ルート（192.*.*.* など）が作成されるだけでなく、すべてのネイバーへのより具体的なルートのアドバタイズメントが抑制されます。特定のネイバーへのアドバタイズメントのみを抑制したい場合、**neighbor distribute-list** コマンドを使用できますが、慎重に使用すべきです。より具体的なルートがリークした場合、すべての BGP または mBGP ルータは、生成中の具体的でない集約よりもこのルートを優先します（最長一致ルーティングによる）。

suppress-map キーワードを使用すると、集約ルートは作成されますが、指定されたルートのアドバタイズメントが抑制されます。ルート マップの **match** 句を使用して、集約のより具体的な一部のルートを選択的に抑制し、他のルートを抑制しないでおくことができます。IP アクセス リストと自律システム パス アクセス リストの一致句がサポートされています。

advertise-map キーワードを使用すると、集約ルートの異なるコンポーネント（AS_SET やコミュニティなど）を構築するために使用する特定のルートが選択されます。集約のコンポーネントが別々の自律システムにあり、AS_SET で集約を作成して同じ自律システムの一部にアドバタイズしたい場合、**aggregate-address** コマンドのこの形式が役立ちます。AS_SET から特定の自律システム番号を省略し、集約が受信ルータの BGP ループ検出メカニズムによってドロップされるのを防ぐことを忘れてはなりません。IP アクセス リストと自律システム パス アクセス リストの **match** 句がサポートされています。

attribute-map キーワードを使用すると、集約ルートの属性を変更できます。AS_SET を構成するルートの 1 つが community no-export 属性（集約ルートがエクスポートされるのを防ぐ）などの属性で設定されている場合、**aggregate-address** コマンドのこの形式が役立ちます。属性マップ ルート マップを作成し、集約の属性を変更することができます。

例

次に、集約ルートを作成し、すべてのネイバーへのより具体的なルートのアドバタイズメントを抑制する例を示します。

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router)# aggregate-address 10.0.0.0 255.0.0.0 summary-only
```

関連コマンド

コマンド	説明
address-family ipv4	アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv4 を使用するルーティング セッションを設定します。

alarm contact description

ISA 3000 でアラーム入力の説明を入力するには、グローバル コンフィギュレーション モードで **alarm contact description** コマンドを使用します。デフォルトの説明を対応するコンタクト番号に設定するには、このコマンドの no 形式を使用します。

alarm contact {**1** | **2**} **description** *string*

no alarm contact {**1** | **2**} **description**

構文の説明

1	**2** 説明が設定されているアラーム コンタクトを指定します。1 または 2 を入力します。
string	説明を指定します。説明には最大 80 文字の英数字を使用でき、syslog メッセージに含められます。

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	• 対応	—	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

例

次に、アラーム コンタクト 1 の説明を指定する例を示します。

```
ciscoasa(config)# alarm contact 1 description Door Open
```

関連コマンド

コマンド	説明
alarm contact severity	ISA 3000 の LED 状態に順に影響を与えるアラームの重大度を指定します。
alarm contact trigger	1 つまたはすべてのアラーム入力のトリガーを指定します。

コマンド	説明
alarm facility input-alarm	アラーム入力のロギング オプションと通知オプションを指定します。
alarm facility power-supply rps	電源アラームを設定します。
alarm facility temperature	温度アラームを設定します。
alarm facility temperature（上限および下限のしきい値）	温度しきい値の下限または上限を設定します。
show alarm settings	すべてのグローバル アラーム設定を表示します。
show environment alarm-contact	すべての外部アラーム設定を表示します。
show facility-alarm relay	アクティブ化された状態のリレーを表示します。
show facility-alarm status	トリガーされたすべてのアラームを表示するか、または指定された重大度に基づいてアラームを表示します。
clear facility-alarm output	出力リレーの電源を切り、LED のアラーム状態をクリアします。

alarm contact severity

ISA 3000 でアラームの重大度を指定するには、グローバル コンフィギュレーション モードで **alarm contact severity** コマンドを使用します。デフォルトの重大度に戻すには、このコマンドの **no** 形式を使用します。

alarm contact {**1** | **2** | **all**} **severity** {**major** | **minor** | **none**}

no alarm contact {**1** | **2** | **all**} **severity**

構文の説明

{**1** | **2** | **all**}	重大度を設定するアラーム コンタクトを指定します。1、2、または all を入力します。
severity {**major** | **minor** | **none**}	このアラーム コンタクトによってトリガーされたアラームの重大度。この重大度でアラームをラベル付けするほか、この重大度により、コンタクトに関連付けられた LED の動作が制御されます。 • **major**：LED が赤色で点滅します。 • **minor**：LED が赤色で点灯します。これはデフォルトです。 • **none**：LED が消灯します。

コマンド デフォルト

デフォルトでは、重大度はマイナーになっています。

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
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
9.7(1)	このコマンドが追加されました。

例

次に、アラーム コンタクト 1 の重大度を指定する例を示します。

```
ciscoasa(config)# alarm contact 1 severity major
```

関連コマンド

コマンド	説明
alarm contact description	アラーム入力の説明を指定します。
alarm contact trigger	1 つまたはすべてのアラーム入力のトリガーを指定します。
alarm facility input-alarm	アラーム入力のロギング オプションと通知オプションを指定します。
alarm facility power-supply rps	電源アラームを設定します。
alarm facility temperature	温度アラームを設定します。
alarm facility temperature（上限および下限のしきい値）	温度しきい値の下限または上限を設定します。
show alarm settings	すべてのグローバル アラーム設定を表示します。
show environment alarm-contact	すべての外部アラーム設定を表示します。
show facility-alarm relay	アクティブ化された状態のリレーを表示します。
show facility-alarm status	トリガーされたすべてのアラームを表示するか、または指定された重大度に基づいてアラームを表示します。
clear facility-alarm output	出力リレーの電源を切り、LED のアラーム状態をクリアします。

alarm contact trigger

ISA 3000 で 1 つまたはすべてのアラーム入力にトリガーを指定するには、グローバル コンフィギュレーション モードで **alarm contact trigger** コマンドを使用します。デフォルトのトリガーに戻すには、このコマンドの **no** 形式を使用します。

alarm contact {**1** | **2** | **all**} **trigger** {**open** | **closed**}

alarm contact {**1** | **2** | **all**} **trigger**

構文の説明

{**1** | **2** | **all**}	トリガーを設定するアラーム コンタクトを指定します。1、2、または all を入力します。
trigger {**open** | **closed**}	トリガーは、アラート信号を発する電気条件を決定します。 • **open**: コンタクトの通常状態はクローズです。つまり、コンタクトに電流が流れています。コンタクトがオープンになる、つまり電流が停止するとアラートがトリガーされます。 • **closed**: コンタクトの通常状態はオープンです。つまり、コンタクトに電流は流れていません。コンタクトがクローズになる、つまり電流がコンタクトを流れ始めるとアラートがトリガーされます。これはデフォルトです。

コマンド デフォルト

デフォルトでは、クローズ状態がトリガーです。

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
9.7(1)	このコマンドが追加されました。

例

次に、アラーム コンタクト 1 にトリガーを設定する例を示します。

```
ciscoasa(config)# alarm contact 1 trigger open
```

関連コマンド

コマンド	説明
alarm contact description	アラーム入力の説明を指定します。
alarm contact severity	アラームの重大度を指定します。
alarm facility input-alarm	アラーム入力のロギング オプションと通知オプションを指定します。
alarm facility power-supply rps	電源アラームを設定します。
alarm facility temperature	温度アラームを設定します。
alarm facility temperature（上限および下限のしきい値）	温度しきい値の下限または上限を設定します。
show alarm settings	すべてのグローバル アラーム設定を表示します。
show environment alarm-contact	すべての外部アラーム設定を表示します。
show facility-alarm relay	アクティブ化された状態のリレーを表示します。
show facility-alarm status	トリガーされたすべてのアラームを表示するか、または指定された重大度に基づいてアラームを表示します。
clear facility-alarm output	出力リレーの電源を切り、LED のアラーム状態をクリアします。

alarm facility input-alarm

ISA 3000 でアラーム入力のロギングおよび通知オプションを指定するには、グローバル コンフィギュレーション モードで **alarm facility input-alarm** コマンドを使用します。ロギングおよび通知オプ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。

alarm facility input-alarm {**1** | **2**} {**notifies** | **relay** | **syslog**}

no alarm facility input-alarm {**1** | **2**} {**notifies** | **relay** | **syslog**}

構文の説明

{**1** | **2**}	アラーム コンタクト(1 または 2)を指定します。
notifies	アラームがトリガーされたときに SNMP トラップの送信を有効にします。
relay	アラームがトリガーされたときにハードウェア出力リレーを有効にします。これにより、接続されている外部アラームがアクティブになります。
syslog	アラームがトリガーされたとき、およびアラーム条件が終了したときに syslog メッセージの送信を有効にします。

コマンド デフォルト

デフォルトでは、syslog は有効になっていますが、その他のオプション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
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
9.7(1)	このコマンドが追加されました。

例

次に、アラーム入力 1 にロギングおよび通知オプションを指定する例を示します。

```
ciscoasa(config)# alarm facility input-alarm 1 notifies
ciscoasa(config)# alarm facility input-alarm 1 relay
ciscoasa(config)# alarm facility input-alarm 1 syslog
```

関連コマンド

コマンド	説明
alarm contact description	アラーム入力の説明を指定します。
alarm contact severity	アラームの重大度を指定します。
alarm contact trigger	1 つまたはすべてのアラーム入力のトリガーを指定します。
alarm facility power-supply rps	電源アラームを設定します。
alarm facility temperature	温度アラームを設定します。
alarm facility temperature（上限および下限のしきい値）	温度しきい値の下限または上限を設定します。
show alarm settings	すべてのグローバル アラーム設定を表示します。
show environment alarm-contact	すべての外部アラーム設定を表示します。
show facility-alarm relay	アクティブ化された状態のリレーを表示します。
show facility-alarm status	トリガーされたすべてのアラームを表示するか、または指定された重大度に基づいてアラームを表示します。
clear facility-alarm output	出力リレーの電源を切り、LED のアラーム状態をクリアします。

alarm facility power-supply rps

ISA 3000 で電源アラームを設定するには、グローバル コンフィギュレーション モードで **alarm facility power-supply rps** コマンドを使用します。電源アラーム、リレー、SNMP トラップおよび syslog を無効にするには、**alarm facility power-supply rps disable** コマンドまたは **no** バージョンを使用します。

alarm facility power-supply rps {**disable** | **notifies** | **relay** | **syslog**}

no alarm facility power-supply rps {**disable** | **notifies** | **relay** | **syslog**}

構文の説明

disable	電源アラーム、リレー、SNMP トラップおよび syslog を無効にします。
notifies	アラームがトリガーされたときに SNMP トラップの送信を有効にします。
relay	アラームがトリガーされたときにハードウェア出力リレーを有効にします。これにより、接続されている外部アラームがアクティブになります。
syslog	アラームがトリガーされたとき、およびアラーム条件が終了したときに syslog メッセージの送信を有効にします。

コマンド デフォルト

デフォルトでは、**syslog** が有効で、**リレー**および**通知**は無効になっています。このアラームは、デフォルトで有効になっています。

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
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
9.7(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

ISA 3000 には、電源装置が 2 台搭載されています。デフォルトでは、システムはシングル電源モードで稼働しています。ただし、デュアルモードでシステムを稼働するよう設定できます。その場合、プライマリ電源が故障すると 2 つ目の電源が自動的に電力を供給します。デュアル モードを有効にすると、電源アラームが自動的に有効になって syslog アラートが送信されますが、アラートを無効にしたり、SNMP トラップまたはアラーム ハードウェア リレーを有効にすることもできます。

alarm facility power-supply rps disable コマンドを使用すると、電源アラーム、リレー、トラップおよび syslog が無効になります。**no alarm facility power-supply rps disable** コマンドを使用すると、電源アラームのみが有効になります。リレー、SNMP トラップ、および syslog を個別に有効にする必要があります。

また、デュアル モードを有効にするには、**power-supply dual** コマンドも設定する必要があります。このアラームは、デュアル モードで自動的に有効になります。

例

次に、デュアル電源モードを有効にし、すべてのアラート オプションを設定する例を示します。

```
ciscoasa(config)# power-supply dual
ciscoasa(config)# alarm facility power-supply rps relay
ciscoasa(config)# alarm facility power-supply rps syslog
ciscoasa(config)# alarm facility power-supply rps notifies
```

次に、デュアル電源アラームを無効にする例を示します。

```
ciscoasa(config)# alarm facility power-supply rps disable
```

関連コマンド

コマンド	説明
alarm contact description	アラーム入力の説明を指定します。
alarm contact severity	アラームの重大度を指定します。
alarm contact trigger	1 つまたはすべてのアラーム入力のトリガーを指定します。
alarm facility input-alarm	アラーム入力のロギング オプションと通知オプションを指定します。
alarm facility temperature	温度アラームを設定します。
alarm facility temperature（上限および下限のしきい値）	温度しきい値の下限または上限を設定します。
show alarm settings	すべてのグローバル アラーム設定を表示します。
show environment alarm-contact	すべての外部アラーム設定を表示します。
show facility-alarm relay	アクティブ化された状態のリレーを表示します。
show facility-alarm status	トリガーされたすべてのアラームを表示するか、または指定された重大度に基づいてアラームを表示します。
clear facility-alarm output	出力リレーの電源を切り、LED のアラーム状態をクリアします。

alarm facility temperature（アクション）

ISA 3000 で温度アラームを設定するには、グローバル コンフィギュレーション モードで **alarm facility temperature** コマンドを使用します。温度アラームを無効にするには、このコマンドの **no** 形式を使用します。

alarm facility temperature {**primary** | **secondary**} {**notifies** | **relay** | **syslog**}

no alarm facility temperature {**primary** | **secondary**} {**notifies** | **relay** | **syslog**}

構文の説明

primary	プライマリ温度アラームを設定します。
secondary	セカンダリ温度アラームを設定します。
notifies	アラームがトリガーされたときに SNMP トラップの送信を有効にします。
relay	アラームがトリガーされたときにハードウェア出力リレーを有効にします。これにより、接続されている外部アラームがアクティブになります。
syslog	アラームがトリガーされたとき、およびアラーム条件が終了したときに syslog メッセージの送信を有効にします。

コマンド デフォルト

プライマリ温度アラームは、すべてのアラーム アクションに対して有効になっています。

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
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
9.7(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

デバイスの CPU カードの温度に基づいてアラームを設定できます。

alarm facility temperature コマンドで **high** および **low** キーワードを使用して、プライマリとセカンダリの温度範囲を設定できます。温度が下限しきい値以下になるか上限しきい値以上になると、アラームがトリガーされます。

プライマリ温度アラームは、すべてのアラームアクション（出力リレー、syslog、および SNMP）についてデフォルトで有効になっています。プライマリ温度範囲のデフォルト設定値は -40 °C ～ 92 °C です。

セカンダリ温度アラームはデフォルトでディセーブルになっています。セカンダリ温度は、-35 °C ～ 85 °C の範囲で設定できます。

セカンダリ温度範囲はプライマリ範囲よりも制限されているため、セカンダリの低温または高温のいずれかを設定すると、プライマリ設定にデフォルト以外の値を設定していたとしても、対応するプライマリ設定はこの設定によって無効になります。2 つの異なる高温アラームと 2 つの異なる低温アラームを有効にすることはできません。

したがって、実際には、プライマリのみまたはセカンダリのみの高温値および低温値を設定する必要があります。

例

次の例では、セカンダリ アラームの高温値および低温値を設定し、すべてのアラート アクションを有効にしています。

```
ciscoasa(config)# alarm facility temperature secondary low -20
ciscoasa(config)# alarm facility temperature secondary high 80
ciscoasa(config)# alarm facility temperature secondary notifies
ciscoasa(config)# alarm facility temperature secondary relay
ciscoasa(config)# alarm facility temperature secondary syslog
```

関連コマンド

コマンド	説明
alarm contact description	アラーム入力の説明を指定します。
alarm contact severity	アラームの重大度を指定します。
alarm contact trigger	1 つまたはすべてのアラーム入力のトリガーを指定します。
alarm facility input-alarm	アラーム入力のロギング オプションと通知オプションを指定します。
alarm facility power-supply rps	電源アラームを設定します。
alarm facility temperature（上限および下限のしきい値）	温度しきい値の下限または上限を設定します。
show alarm settings	すべてのグローバル アラーム設定を表示します。
show environment alarm-contact	すべての外部アラーム設定を表示します。
show facility-alarm relay	アクティブ化された状態のリレーを表示します。
show facility-alarm status	トリガーされたすべてのアラームを表示するか、または指定された重大度に基づいてアラームを表示します。
clear facility-alarm output	出力リレーの電源を切り、LED のアラーム状態をクリアします。

alarm facility temperature（上限および下限しきい値）

ISA 3000 で上限および下限の温度しきい値を設定するには、グローバル コンフィギュレーション モードで **alarm facility temperature** {**low** | **high**} コマンドを使用します。しきい値を削除するか、プライマリの値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。

alarm facility temperature {**primary** | **secondary**} {**high** | **low**} *threshold*

no alarm facility temperature {**primary** | **secondary**} {**high** | **low**} *threshold*

構文の説明

primary	プライマリ温度アラームを設定します。
secondary	セカンダリ温度アラームを設定します。
high *threshold*	上限しきい値を摂氏で設定します。プライマリの最大値は 92 です。セカンダリの最大値は 85 です。
low *threshold*	下限しきい値を摂氏で設定します。プライマリの最小値は -40 です。セカンダリの最小値は -35 です。

コマンド デフォルト

デフォルトのプライマリ高温値は 92 °C、低温値は -40 °C 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
9.7(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

デバイスの CPU カードの温度に基づいてアラームを設定できます。

alarm facility temperature コマンドで **high** および **low** キーワードを使用して、プライマリとセカンダリの温度範囲を設定できます。温度が下限しきい値以下になるか上限しきい値以上になると、アラームがトリガーされます。

プライマリ温度アラームは、すべてのアラームアクション（出力リレー、syslog、および SNMP）についてデフォルトで有効になっています。プライマリ温度範囲のデフォルト設定値は -40 °C ～ 92 °C です。

セカンダリ温度アラームはデフォルトでディセーブルになっています。セカンダリ温度は、-35 °C ～ 85 °C の範囲で設定できます。

セカンダリ温度範囲はプライマリ範囲よりも制限されているため、セカンダリの低温または高温のいずれかを設定すると、プライマリ設定にデフォルト以外の値を設定していたとしても、対応するプライマリ設定はこの設定によって無効になります。2 つの異なる高温アラームと 2 つの異なる低温アラームを有効にすることはできません。

したがって、実際には、プライマリのみまたはセカンダリのみの高温値および低温値を設定する必要があります。

例

次の例では、セカンダリ アラームの高温値および低温値を設定し、すべてのアラート アクションを有効にしています。

```
ciscoasa(config)# alarm facility temperature secondary low -20
ciscoasa(config)# alarm facility temperature secondary high 80
ciscoasa(config)# alarm facility temperature secondary notifies
ciscoasa(config)# alarm facility temperature secondary relay
ciscoasa(config)# alarm facility temperature secondary syslog
```

関連コマンド

コマンド	説明
alarm contact description	アラーム入力の説明を指定します。
alarm contact severity	アラームの重大度を指定します。
alarm contact trigger	1 つまたはすべてのアラーム入力のトリガーを指定します。
alarm facility input-alarm	アラーム入力のロギング オプションと通知オプションを指定します。
alarm facility power-supply rps	電源アラームを設定します。
alarm facility temperature	温度アラームを設定します。
show alarm settings	すべてのグローバル アラーム設定を表示します。
show environment alarm-contact	すべての外部アラーム設定を表示します。
show facility-alarm relay	アクティブ化された状態のリレーを表示します。
show facility-alarm status	トリガーされたすべてのアラームを表示するか、または指定された重大度に基づいてアラームを表示します。
clear facility-alarm output	出力リレーの電源を切り、LED のアラーム状態をクリアします。

allocate-interface

インターフェイスをセキュリティ コンテキストに割り当てるには、コンテキスト コンフィギュレーション モードで **allocate-interface** コマンドを使用します。インターフェイスをコンテキストから削除するには、このコマンドの **no** 形式を使用します。

allocate-interface *physical_interface* [*map_name*] [**visible** | **invisible**]

no allocate-interface *physical_interface*

allocate-interface *physical_interface*.*subinterface*[-*physical_interface*.*subinterface*] [*map_name*[-*map_name*]] [**visible** | **invisible**]

no allocate-interface *physical_interface*.*subinterface*[-*physical_interface*.*subinterface*]

構文の説明

invisible	（デフォルト）コンテキスト ユーザが **show interface** コマンドでマッピング名（設定されている場合）だけを表示できるようにします。
map_name	（任意）マッピング名を設定します。 *map_name* は、インターフェイス ID の代わりにコンテキスト内で使用できるインターフェイスの英数字のエイリアスです。マッピング名を指定しない場合、インターフェイス ID がコンテキスト内で使用されます。セキュリティのために、コンテキストで使用されているインターフェイスをコンテキスト管理者に知らせない場合があります。 マッピング名はアルファベットで始まり、アルファベットまたは数字で終わる必要があります。その間の文字には、アルファベット、数字、または下線のみを使用できます。たとえば、次の名前を使用できます。 **int0** **inta** **int_0** サブインターフェイスの場合は、マッピング名の範囲を指定できます。 範囲の詳細については、「使用上のガイドライン」を参照してください。
physical_interface	**gigabitethernet0/1** などのインターフェイス ID を設定します。有効値については、**interface** コマンドを参照してください。インターフェイス タイプとポート番号の間にスペースを含めないでください。
subinterface	サブインターフェイス番号を設定します。サブインターフェイスの範囲を指定できます。
visible	（任意）マッピング名を設定した場合でも、コンテキスト ユーザが **show interface** コマンドで物理インターフェイスのプロパティを表示できるようにします。

デフォルト

マッピング名を設定した場合、デフォルトでは、**show interface** コマンドの出力にインターフェイス ID は表示されません。

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		
	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
コンテキスト 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

このコマンドを複数回入力して、異なる範囲を指定できます。マッピング名または表示設定を変更するには、特定のインターフェイス ID に対してコマンドを再入力し、新しい値を設定します。**no allocate-interface** コマンドを入力して最初からやり直す必要はありません。**allocate-interface** コマンドを削除すると、ASA によって、コンテキスト内のインターフェイス関連のコンフィギュレーションがすべて削除されます。

トランスペアレント ファイアウォール モードでは、2 つのインターフェイスのみがトラフィックを通過させることができます。ただし、ASA では、専用の管理インターフェイス Management 0/0（物理インターフェイスまたはサブインターフェイス）を管理トラフィック用の第 3 のインターフェイスとして使用できます。

（注） トランスペアレント モードの管理インターフェイスは、MAC アドレス テーブルにないパケットをインターフェイスにフラッディングしません。

ルーテッド モードでは、必要に応じて同じインターフェイスを複数のコンテキストに割り当てることができます。トランスペアレント モードでは、インターフェイスを共有できません。

サブインターフェイスの範囲を指定する場合は、マッピング名の一致範囲を指定できます。範囲については、次のガイドラインに従ってください。

- マッピング名は、アルファベット部分と、それに続く数値部分で構成する必要があります。マッピング名のアルファベット部分は、範囲の両端で一致している必要があります。たとえば、次のような範囲を入力します。

  ```
  int0-int10
  ```

  たとえば、**gigabitethernet0/1.1-gigabitethernet0/1.5 happy1-sad5** と入力した場合、コマンドは失敗します。

- マッピング名の数値部分には、サブインターフェイスの範囲と同じ個数の数値を含める必要があります。たとえば、次の例では、両方の範囲に 100 個のインターフェイスが含まれています。

  ```
  gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int100
  ```

  たとえば、**gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int15** と入力した場合、コマンドは失敗します。

例

次に、gigabitethernet0/1.100、gigabitethernet0/1.200、および gigabitethernet0/2.300 ～ gigabitethernet0/1.305 をコンテキストに割り当てる例を示します。マッピング名は、int1 ～ int8 です。

```
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/2.300-gigabitethernet0/2.305
int3-int8
```

関連コマンド

コマンド	説明
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードを開始します。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show context	コンテキストのリスト(システム実行スペース)または現在のコンテキストに関する情報を表示します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。
vlan	サブインターフェイスに VLAN ID を割り当てます。

allocate-ips

IPS 仮想センサーをセキュリティ コンテキストに割り当てるには、AIP SSM がインストールされている場合には、コンテキスト コンフィギュレーション モードで **allocate-ips** コマンドを使用します。仮想センサーをコンテキストから削除するには、このコマンドの **no** 形式を使用します。

allocate-ips *sensor_name* [*mapped_name*] [**default**]

no allocate-ips *sensor_name* [*mapped_name*] [**default**]

構文の説明

default	(任意) コンテキストごとに 1 つのセンサーをデフォルト センサーとして設定します。コンテキスト コンフィギュレーションでセンサー名が指定されていない場合は、コンテキストでこのデフォルト センサーが使用されます。コンテキストごとに設定できるデフォルト センサーは 1 つのみです。デフォルト センサーを変更する場合は、**no allocate-ips** コマンドを入力して現在のデフォルト センサーを削除してから、新しいデフォルト センサーを割り当てます。センサーをデフォルトとして指定せず、コンテキスト コンフィギュレーションにセンサー名が含まれていない場合、トラフィックは AIP SSM のデフォルト センサーを使用します。
mapped_name	(任意) コンテキスト内で実際のセンサー名の代わりに使用できるセンサー名のエイリアスとして、マッピング名を設定します。マッピング名を指定しない場合、センサー名がコンテキスト内で使用されます。セキュリティのために、コンテキストで使用されているセンサーをコンテキスト管理者に知らせない場合があります。または、コンテキスト コンフィギュレーションを一般化する場合もあります。たとえば、すべてのコンテキストで「sensor1」および「sensor2」というセンサーを使用する場合、コンテキスト A の sensor1 と sensor2 に「highsec」センサーと「lowsec」センサーをマッピングし、コンテキスト B の sensor1 と sensor2 に「medsec」センサーと「lowsec」センサーをマッピングできます。
sensor_name	AIP SSM に設定されているセンサー名を設定します。AIP SSM に設定されているセンサーを表示するには、**allocate-ips ?** と入力します。使用可能なすべてのセンサーが表示されます。**show ips** コマンドを入力することもできます。システム実行スペースで **show ips** コマンドを入力すると、使用可能なすべてのセンサーが表示されます。このコマンドをコンテキストで入力すると、そのコンテキストにすでに割り当てられているセンサーが表示されます。AIP SSM にまだ存在しないセンサー名を指定した場合は、エラーが表示されますが、**allocate-ips** コマンドはそのまま入力されます。AIP SSM にその名前のセンサーが作成されるまで、コンテキストはそのセンサーがダウンしていると見なします。

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。

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
コンテキスト 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。

使用上のガイドライン

各コンテキストに 1 つ以上の IPS 仮想センサーを割り当てることができます。その後、**ips** コマンドを使用して AIP SSM にトラフィックを送信するようにコンテキストを設定するときに、コンテキストに割り当てられているセンサーを指定できます。コンテキストに割り当てられていないセンサーは指定できません。コンテキストにセンサーが割り当てられていない場合は、AIP SSM に設定されているデフォルト センサーが使用されます。同じセンサーを複数のコンテキストに割り当てることができます。

(注) 仮想センサーを使用するためにマルチ コンテキスト モードを開始する必要はありません。シングル モードでトラフィック フローごとに異なるセンサーを使用できます。

例

次に、sensor1 と sensor2 をコンテキスト A に、sensor1 と sensor3 をコンテキスト B に割り当てる例を示します。どちらのコンテキストもセンサー名を「ips1」と「ips2」にマップします。コンテキスト A では sensor1 をデフォルト センサーとして設定しますが、コンテキスト B ではデフォルトを設定しないため、AIP SSM に設定されているデフォルトが使用されます。

```
ciscoasa(config-ctx)# context A
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx)# allocate-ips sensor1 ips1 default
ciscoasa(config-ctx)# allocate-ips sensor2 ips2
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
ciscoasa(config-ctx)# member gold

ciscoasa(config-ctx)# context sample
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
ciscoasa(config-ctx)# allocate-ips sensor1 ips1
ciscoasa(config-ctx)# allocate-ips sensor3 ips2
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
ciscoasa(config-ctx)# member silver
```

関連コマンド

コマンド	説明
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードを開始します。
ips	トラフィックをインスペクションのために AIP SSM に転送します。
show context	コンテキストのリスト(システム実行スペース)または現在のコンテキストに関する情報を表示します。
show ips	AIP SSM に設定されている仮想センサーを表示します。

allowed-eid

IP アドレスに基づいて検査対象 EID を制限するための LISP インスペクション マップを設定するには、パラメータ コンフィギュレーション モードで **allowed-eid** コマンドを使用します。パラメータ コンフィギュレーション モードにアクセスするには、まず **policy-map type inspect lisp** コマンドを入力します。すべての EID を許可するには、このコマンドの **no** 形式を使用します。

allowed-eid access-list *eid_acl_name*

no allowed-eid access-list *eid_acl_name*

構文の説明

access-list *eid_acl_name*	宛先 IP アドレスのみが EID 組み込みアドレスと照合される拡張 ACL 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
パラメータ 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)	このコマンドが追加されました。

使用上のガイドライン

IP アドレスに基づいて検査対象 EID を制限するための LISP インスペクション マップを設定します。

クラスタ フロー モビリティの LISP インスペクションについて

ASA は、場所の変更について LISP トラフィックを検査し、シームレスなクラスタリング操作のためにこの情報を使用します。LISP の統合により、ASA クラスタ メンバーは、最初のホップ ルータと ETR または ITR との間で渡される LISP トラフィックを検査し、その後、フローの所有者を新しいサイトへ変更できます。

クラスタ フロー モビリティには複数の相互に関連する設定が含まれています。

1. （オプション）ホストまたはサーバの IP アドレスに基づく検査される EID の限定：最初のホップ ルータは、ASA クラスタが関与していないホストまたはネットワークに関する EID 通知メッセージを送信することがあるため、EID をクラスタに関連するサーバまたはネットワークのみに限定することができます。たとえば、クラスタが 2 つのサイトのみに関連しているが、LISP は 3 つのサイトで稼働している場合は、クラスタに関連する 2 つのサイトの EID のみを含めます。**policy-map type inspect lisp**、**allowed-eid** および **validate-key** コマンドを参照してください。
2. LISP トラフィックのインスペクション：ASA は、最初のホップ ルータと ITR または ETR 間で送信された EID 通知メッセージに関して LISP トラフィックを検査します。ASA は EID とサイト ID を相関付ける EID テーブルを維持します。たとえば、最初のホップ ルータの送信元 IP アドレスと ITR または ETR の宛先アドレスをもつ LISP トラフィックを検査する必要があります。**inspect lisp** コマンドを参照してください。
3. 指定されたトラフィックでのフロー モビリティを有効にするサービス ポリシー：ビジネスクリティカルなトラフィックでフロー モビリティを有効にする必要があります。たとえば、フロー モビリティを、HTTPS トラフィックのみに制限したり、特定のサーバとの間でやり取りされるトラフィックのみに制限したりできます。**cluster flow-mobility lisp** コマンドを参照してください。
4. サイト ID：ASA は各クラスタ ユニットのサイト ID を使用して、新しい所有者を判別します。**site-id** コマンドを参照してください。
5. フロー モビリティを有効にするクラスタレベルの設定：クラスタ レベルでもフロー モビリティを有効にする必要があります。このオン/オフの切り替えを使用することで、特定のクラスのトラフィックまたはアプリケーションに対してフロー モビリティを簡単に有効または無効にできます。**flow-mobility lisp** コマンドを参照してください。

例

次に、EID を 10.10.10.0/24 ネットワーク上の EID に制限する例を示します。

```
ciscoasa(config)# access-list TRACKED_EID_LISP extended permit ip any 10.10.10.0
255.255.255.0
ciscoasa(config)# policy-map type inspect lisp LISP_EID_INSPECT
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# allowed-eid access-list TRACKED_EID_LISP
ciscoasa(config-pmap-p)# validate-key MadMaxShinyandChrome
```

関連コマンド

コマンド	説明
clear cluster info flow-mobility counters	フロー モビリティ カウンタをクリアします。
clear lisp eid	ASA EID テーブルから EID を削除します。
cluster flow-mobility lisp	サービス ポリシーのフロー モビリティを有効にします。
flow-mobility lisp	クラスタのフロー モビリティを有効にします。
inspect lisp	LISP トラフィックを検査します。
policy-map type inspect lisp	LISP 検査をカスタマイズします。
site-id	クラスタ シャーシのサイト ID を設定します。

コマンド	説明
show asp table classify domain inspect-lisp	LISP 検査用の ASP テーブルを表示します。
show cluster info flow-mobility counters	フロー モビリティ カウンタを表示します。
show conn	LISP フロー モビリティの対象となるトラフィックを表示します。
show lisp eid	ASA EID テーブルを表示します。
show service-policy	サービス ポリシーを表示します。
validate-key	LISP メッセージを検証するための事前共有キーを入力します。

allow-ssc-mgmt

ASA 5505 のインターフェイスを SSC 管理インターフェイスとして設定するには、インターフェイス コンフィギュレーション モードで **allow-ssc-mgmt** コマンドを使用します。インターフェイスの割り当てを解除するには、このコマンドの **no** 形式を使用します。

allow-ssc-mgmt

no allow-ssc-mgmt

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

このコマンドは、VLAN 1 用の出荷時のデフォルトのコンフィギュレーション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
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	—	—

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

SSC に外部インターフェイスはありません。管理 VLAN として VLAN を設定し、バックプレーン経由での内部 IP 管理アドレスへのアクセスを許可できます。デフォルトでは、VLAN 1 は SSC 管理アドレスでイネーブルになります。SSC 管理 VLAN として割り当てることができるのは 1 つの VLAN だけです。

ASDM を使用してアクセスする場合は、管理アドレス用に NAT を設定しないでください。ASDM の初期セットアップでは、実際のアドレスにアクセスする必要があります。初期セットアップ後（SSC でパスワードを設定した後）は、NAT を設定し、SSC にアクセスするときの変換アドレスを ASDM に提供できます。

例

次に、管理アクセスを VLAN 1 でディセーブルにし、VLAN 2 でイネーブルにする例を示します。

```
ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# no allow-ssc-mgmt
ciscoasa(config-if)# interface vlan 2
ciscoasa(config-if)# allow-ssc-mgmt
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定します。
ip address	ブリッジ グループの管理 IP アドレスを設定します。
nameif	インターフェイス名を設定します。
security-level	インターフェイスのセキュリティ レベルを設定します。
hw-module module ip	SSC の管理 IP アドレスを設定します。
hw-module module allow-ip	管理 IP アドレスにアクセスできるホストを設定します。

allow-tls

TLS セッションを許可または禁止するように ESMTP インスペクションを設定するには、パラメータ コンフィギュレーション モードで **allow-tls** 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。

allow-tls [**action log**]

no allow-tls

構文の説明

action log	暗号化された接続をログに記録するかどうか。

コマンド デフォルト

allow-tls コマンドが ESMTP インスペクションのデフォルトです。

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
パラメータ 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
8.0(3)	このコマンドが追加されました。
9.4(1)	デフォルトが **no allow-tls** から **allow-tls** に変更されました。ただし、このデフォルトは新しい、または再イメージングされたシステムに適用されます。**no allow-tls** を含むシステムをアップグレードする場合は、このコマンドは変更されません。

使用上のガイドライン

ESMTP インスペクションでは、暗号化された接続を検査できません。すべての ESMTP セッションの検査を強制するには、**no allow-tls** コマンドを使用します。TLS を無効にすると、STARTTLS インジケータが接続要求から削除され、強制的にクライアントとサーバがクリア テキスト接続をネゴシエートします。

クライアントとサーバが暗号化された接続をネゴシエートできるようにする場合は、ESMTP インスペクション ポリシー マップのパラメータ セクションに **allow-tls** コマンドを含め、マップを ESMTP インスペクション サービス ポリシーに接続します。また、_default_esmtp_map（これは独自のマップを適用しない場合に適用されます）を編集することもできます。

例

次に、ESMTP インスペクションをバイパスする暗号化された ESMTP セッションを許可する方法の例を示します。

```
ciscoasa(config)# policy-map type inspect esmtp esmtp_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# allow-tls
```

関連コマンド

コマンド	説明
policy-map type inspect esmtp	インスペクションの ESMTP ポリシー マップを設定します。

always-on-vpn

AnyConnect Always-On-VPN 機能の動作を設定するには、グループ ポリシー コンフィギュレーション モードで **always-on-vpn** コマンドを使用します。

always-on-vpn [**profile-setting** | **disable**]

構文の説明

disable	Always-On-VPN 機能をオフにします。
profile-setting	AnyConnect プロファイルに設定された **always-on-vpn** 設定を使用します。

コマンド デフォルト

Always-On-VPN 機能は、デフォルトでオンになっています。

コマンド履歴

リリース	変更内容
8.3(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

AnyConnect ユーザのために Always-On-VPN 機能をイネーブルにするには、プロファイル エディタで AnyConnect プロファイルを設定します。次に、適切なポリシーのグループ ポリシー属性を設定します。

例

次の例では、設定されたグループ ポリシーに対して Always-On 機能を有効にしています。

```
ciscoasa(config)# group-policy <group policy> attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# always-on-vpn profile-setting
```

関連コマンド

コマンド	説明
webvpn	WebVPN のグループ ポリシーを設定します。

anti-replay

GTP-U メッセージ シーケンス番号のアンチリプレイを有効にするには、GTP インスペクション ポリシー マップのパラメータ コンフィギュレーション モードで **anti-replay** コマンドを使用します。アンチリプレイを無効にするには、このコマンドの **no** 形式を使用します。

anti-replay [*window_size*]

no anti-replay [*window_size*]

構文の説明

window_size	スライディング ウィンドウのサイズはメッセージの数です。ウィンドウのサイズは、128、256、512、または 1024 になります。値を入力しない場合は、デフォルトの 512 になります。

デフォルト

デフォルトでは、アンチリプレイ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
9.10(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-U メッセージのスライディング ウィンドウを指定することによって、アンチリプレイを有効にできます。

スライディング ウィンドウのサイズはメッセージの数であり、128、256、512、または 1024 になります。有効なメッセージが表示されると、ウィンドウは新しいシーケンス番号に移行します。シーケンス番号は 0 ～ 65535 の範囲であり、最大値に達するとラッピングされます。また、これらは PDP コンテキストごとに一意です。メッセージは、シーケンス番号がウィンドウ内であれば有効と見なされます。

アンチリプレイは、ハッカーが GTP データ パケットをキャプチャし、それらをリプレイするときに発生する可能性があるセッション ハイジャックや DoS 攻撃を防ぐのに役立ちます。

例

次の例では、ウィンドウ サイズ 512 のアンチリプレイを有効にしています。

```
ciscoasa(config)# policy-map type inspect gtp gtp-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# anti-replay 512
```

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。

anyconnect ask

ASA がリモート SSL VPN クライアント ユーザに対してクライアントのダウンロードを要求するには、グループ ポリシー webvpn またはユーザ名 webvpn コンフィギュレーション モードで **anyconnect ask** コマンドを使用します。このコマンドを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。

anyconnect ask {**none** | **enable** [**default** {**webvpn** | **anyconnect**} **timeout** *value*]}

no anyconnect ask none [**default** {**webvpn** | **anyconnect**}]

構文の説明

default anyconnect timeout *value*	リモート ユーザにクライアントのダウンロードを要求するか、クライアントレス接続のポータル ページに移動して、*value* の時間待機してから、デフォルト アクション(クライアントのダウンロード)を実行します。
default webvpn timeout *value*	リモート ユーザにクライアントのダウンロードを要求するか、クライアントレス接続のポータル ページに移動して、*value* の時間待機してから、デフォルト アクション(WebVPN ポータル ページの表示)を実行します。
enable	リモート ユーザにクライアントのダウンロードを要求するか、クライアントレス接続のポータル ページに移動してユーザ応答を無期限に待機します。
none	デフォルト アクションをただちに実行します。

デフォルト

このコマンドのデフォルトは、**anyconnect ask none default webvpn** です。ASA によって、クライアントレス接続のポータル ページがただちに表示されます。

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
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザ名 webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

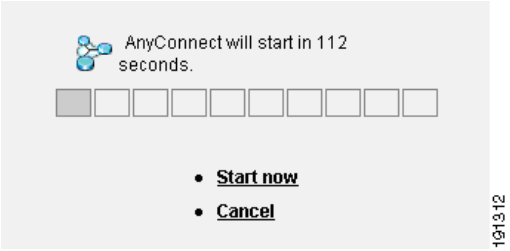
コマンド履歴

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。
8.4(1)	**svc ask** コマンドが **anyconnect ask** コマンドに置き換えられました。

使用上のガイドライン

図 2-1 に、**default anyconnect timeout** *value* コマンドまたは **default webvpn timeout** *value* コマンドが設定された場合にリモート ユーザに表示されるプロンプトを示します。

図 2-1　SSL VPN Client のダウンロードに関してリモート ユーザに表示されるプロンプト



例

次に、ASA を設定して、リモート ユーザにクライアントのダウンロードを要求するか、ポータル ページに移動して、ユーザの応答を 10 秒待機してからクライアントをダウンロードするように設定する例を示します。

```
ciscoasa(config-group-webvpn)# anyconnect ask enable default svc timeout 10
```

関連コマンド

コマンド	説明
show webvpn anyconnect	インストールされている SSL VPN クライアントに関する情報を表示します。
anyconnect	特定のグループまたはユーザに対して SSL VPN クライアントをイネーブルまたは必須にします。
anyconnect image	リモート PC へのダウンロードのために ASA がキャッシュ メモリで展開するクライアント パッケージ ファイルを指定します。

anyconnect-custom（バージョン 9.0 から 9.2 まで）

カスタム属性の値を設定または更新するには、AnyConnect カスタム属性コンフィギュレーション モードで **anyconnect-custom** コマンドを使用します。カスタム属性の値を削除するには、このコマンドの **no** 形式を使用します。

anyconnect-custom *attr-name* **value** *attr-value*

anyconnect-custom *attr-name* **none**

no anyconnect-custom *attr-name*

構文の説明

attr-name	**anyconnnect-custom-attr** コマンドで定義された、現在のグループ ポリシーでの属性の名前。
none	デフォルト アクションをただちに実行します。
value *attr-value*	属性値を含む文字列。値は、属性名に関連付けられ、接続の確立時にクライアントに渡されます。450 文字以内で指定します。

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
AnyConnect カスタム属性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
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

このコマンドは、グループ ポリシーにカスタム属性の値を設定します。『*AnyConnect Administrator's Guide*』に、そのリリースに適用されるカスタム属性の有効な値を示します。カスタム属性は、**anyconnect-custom-attr** コマンドで作成します。

属性のマルチライン値を作成するために、このコマンドの複数のインスタンスがサポートされています。特定の属性名に関連付けられたすべてのデータが、CLI で入力された順序に従ってクライアントに提供されます。マルチライン値の個別の行は削除できません。

このコマンドの **no** 形式では、**value** キーワードおよび **none** キーワードは使用できません。

属性名に関連付けられたデータを複数の CLI 行に入力した場合、そのデータは改行文字（\n）で区切られた単一の連結文字列としてエンドポイントに送信されます。

例

次に、AnyConnect 遅延アップデートのカスタム属性を設定する例を示します。

```
ciscoasa(config-group-policy)# anyconnect-custom DeferredUpdateAllowed true
```

関連コマンド

コマンド	説明
show run webvpn	**anyconnect** コマンドを含む、WebVPN に関するコンフィギュレーション情報を表示します。
show run group-policy	現在のグループ ポリシーに関する設定情報を表示します。
anyconnect-custom-attr	カスタム属性を作成します。

anyconnect-custom（バージョン 9.3 以降）

カスタム属性の値を設定または更新するには、グループ ポリシーまたはダイナミック アクセス ポリシー レコード コンフィギュレーション モードで **anyconnect-custom** コマンドを使用します。カスタム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。

anyconnect-custom *attr-type* **value** *attr-name*

anyconnect-custom *attr-type* **none**

no anyconnect-custom *attr-type*

構文の説明

attr-type	**anyconnnect-custom-attr** コマンドで定義されたカスタム属性のタイプ。
none	このカスタム属性は、ポリシーから明示的に除外されます。
value *attr-name*	**anyconnect-custom-data** コマンドで定義されたカスタム属性値の名前。 カスタム属性のタイプと名前付き値は、接続の確立時にクライアントに渡されます。

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
グループ ポリシーまたはダイナミック アクセス ポリシー レコード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.3(1)	このコマンドが再定義されました。

使用上のガイドライン

このコマンドは、グループ ポリシーまたは DAP にカスタム属性の値を設定します。

『*AnyConnect Administrator's Guide*』に、そのリリースに適用されるカスタム属性の有効な値を示します。カスタム属性は、**anyconnect-custom-attr** コマンドおよび **anyconnect-custom-data** コマンドで作成します。

このコマンドの **no** 形式では、**none** キーワードは使用できません。

例

次に、AnyConnect 遅延アップデートのカスタム属性を設定する例を示します。

```
ciscoasa(config-webvpn)# anyconnect-custom-attr DeferredUpdateAllowed
ciscoasa(config-webvpn)# exit
ciscoasa(config)# anyconnect-custom-data DeferredUpdateAllowed def-allowed true
ciscoasa(config-group-policy)# anyconnect-custom DeferredUpdateAllowed def-allowed
```

関連コマンド

コマンド	説明
show run webvpn	**anyconnect** コマンドを含む、WebVPN に関するコンフィギュレーション情報を表示します。
show run group-policy	現在のグループ ポリシーに関する設定情報を表示します。
show running-config dynamic-access-policy-record	DAP ポリシーで使用されるカスタム属性を表示します。
anyconnect-custom-attr	このコマンドで使用されるカスタム属性のタイプを作成します。
anyconnect-custom-data	このコマンドで使用されるカスタム属性の名前付き値を作成します。

anyconnect-custom-attr（バージョン 9.0 から 9.2 まで）

カスタム属性を作成するには、AnyConnect カスタム属性コンフィギュレーション モードで **anyconnect-custom-attr** コマンドを使用します。カスタム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。

[no] anyconnect-custom-attr *attr-name* **[description** *description***]**

構文の説明

attr-name	属性の名前。この名前は、グループ ポリシー構文および集約認証プロトコル メッセージで参照されます。最大長は 32 文字です。
description *description*	属性の使用方法の自由形式の説明。このテキストは、カスタム属性がグループ ポリシー属性コンフィギュレーション モードから参照された場合に、コマンド ヘルプで表示されます。最大長は 128 文字です。

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
AnyConnect カスタム属性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
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

このコマンドは、AnyConnect の特殊機能をサポートするカスタム属性を作成します。特定の機能に対してカスタム属性を作成した後、それらをグループ ポリシーに追加して、機能が VPN クライアントに適用されるようにします。このコマンドでは、定義されたすべての属性名が一意であることが保証されます。

一部のバージョンの AnyConnect では、機能の設定にカスタム属性が使用されます。各バージョンのリリース ノートおよび『*AnyConnect Administrator's Guide*』に、カスタム属性を必要とするすべての機能を示します。

グループ ポリシーで使用される属性の定義を削除しようとすると、エラー メッセージが表示され、操作は失敗します。ユーザが既存の属性をカスタム属性として追加しようとすると、説明への変更は組み込まれますが、それ以外についてはコマンドは無視されます。

属性のマルチライン値を作成するために、このコマンドの複数のインスタンスがサポートされています。特定の属性名に関連付けられたすべてのデータが、CLI で入力された順序に従ってクライアントに提供されます。マルチライン値の個別の行は削除できません。

例

次に、AnyConnect 遅延アップデートのカスタム属性を設定する例を示します。

```
ciscoasa(config-webvpn)# anyconnect-custom-attr DeferredUpdateAllowed description
Indicates if the deferred update feature is enabled or not
```

関連コマンド

コマンド	説明
show run webvpn	**anyconnect** コマンドを含む、WebVPN に関するコンフィギュレーション情報を表示します。
show run group-policy	現在のグループ ポリシーに関する設定情報を表示します。
anyconnect-custom	カスタム属性のタイプおよび名前付き値をグループ ポリシーまたはダイナミック アクセス ポリシーに関連付けます。

anyconnect-custom-attr（バージョン 9.3 以降）

カスタム属性のタイプを作成するには、config-webvpn コンフィギュレーション モードで **anyconnect-custom-attr** コマンドを使用します。カスタム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。

[no] anyconnect-custom-attr *attr-type* **[description** *description***]**

構文の説明

attr-type	属性のタイプ。このタイプは、グループ ポリシー構文、DAP ポリシー構文、および集約認証プロトコル メッセージで参照されます。最大長は 32 文字です。
description *description*	属性の使用方法の自由形式の説明。このテキストは、カスタム属性がグループ ポリシー属性コンフィギュレーション モードから参照された場合に、コマンド ヘルプで表示されます。最大長は文字です。

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
config-webvpn	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.3(1)	このコマンドが再定義されました。

使用上のガイドライン

このコマンドは、AnyConnect の特殊機能をサポートするカスタム属性を作成します。特定の機能に対してカスタム属性を作成した後、その属性の値を定義し、その属性をグループ ポリシーに追加して、対応する機能が VPN クライアントに適用されるようにします。このコマンドでは、定義されたすべての属性名が一意であることが保証されます。

一部のバージョンの AnyConnect では、機能の設定にカスタム属性が使用されます。各バージョンのリリース ノートおよび『*AnyConnect Administrator's Guide*』に、カスタム属性を必要とするすべての機能を示します。

グループ ポリシーで使用される属性の定義を削除しようとすると、エラー メッセージが表示され、操作は失敗します。ユーザが既存の属性をカスタム属性として追加しようとすると、説明への変更は組み込まれますが、それ以外についてはコマンドは無視されます。

例

次に、AnyConnect 遅延アップデートのカスタム属性を設定する例を示します。

```
ciscoasa(config-webvpn)# anyconnect-custom-attr DeferredUpdateAllowed description
Indicates if the deferred update feature is enabled or not
ciscoasa(config)# anyconnect-custom-data DeferredUpdateAllowed def-allowed true
```

関連コマンド

コマンド	説明
show run webvpn	**anyconnect** コマンドを含む、WebVPN に関するコンフィギュレーション情報を表示します。
show run group-policy	現在のグループ ポリシーに関する設定情報を表示します。
show running-config dynamic-access-policy-record	DAP ポリシーで使用されるカスタム属性を表示します。
anyconnect-custom	ポリシーで使用するためのカスタム属性の値を設定します。
anyconnect-custom-data	カスタム属性の名前付き値を作成します。

anyconnect-custom-data

カスタム属性の名前付き値を作成するには、グローバル コンフィギュレーション モードで **anyconnect-custom-data** コマンドを使用します。カスタム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。

anyconnect-custom-data *attr-type attr-name attr-value*

no anyconnect-custom-data *attr-type attr-name*

構文の説明

attr-type	**anyconnect-custom-attr** を使用して以前に定義された属性のタイプ。
attr-name	指定した値を持つ属性の名前。これは、グループ ポリシーおよびダイナミック アクセス ポリシー レコード コンフィギュレーション モードで参照できます。
attr-value	属性値を含む文字列。 最大 420 文字です。

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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.3(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、AnyConnect の特殊機能をサポートするカスタム属性の名前付き値を定義します。特定の機能に対してカスタム属性を作成した後、その属性の値を定義し、その属性を DAP またはグループ ポリシーに追加して、対応する機能が VPN クライアントに適用されるようにします。

一部のバージョンの AnyConnect では、機能の設定にカスタム属性が使用されます。各バージョンのリリース ノートおよび『*AnyConnect Administrator's Guide*』に、カスタム属性を必要とするすべての機能を示します。

グループ ポリシーで使用される属性の名前付き値を削除しようとすると、エラー メッセージが表示され、操作は失敗します。

属性のマルチライン値を作成するために、このコマンドの複数のインスタンスがサポートされています。特定の属性名に関連付けられたすべてのデータが、CLI で入力された順序に従ってクライアントに提供されます。マルチライン値の個別の行は削除できません。

例

次に、AnyConnect 遅延アップデートのカスタム属性を設定する例を示します。

```
ciscoasa(config)# anyconnect-custom-data DeferredUpdateAllowed def-allowed true
```

関連コマンド

コマンド	説明
show run webvpn	**anyconnect** コマンドを含む、WebVPN に関するコンフィギュレーション情報を表示します。
show run group-policy	現在のグループ ポリシーに関する設定情報を表示します。
show running-config dynamic-access-policy-record	DAP ポリシーで使用されるカスタム属性を表示します。
show run anyconnect-custom-data	定義されているすべてのカスタム属性の名前付き値を表示します。
anyconnect-custom	カスタム属性のタイプおよび値をグループ ポリシーまたは DAP に関連付けます。
anyconnect-custom-attr	カスタム属性を作成します。

anyconnect df-bit-ignore

フラグメンテーションが必要なパケットの DF ビットを無視するには、グループ ポリシー webvpn コンフィギュレーション モードで **anyconnect-df-bit-ignore** コマンドを使用します。フラグメンテーションが必要な DF ビットを許可するには、このコマンドの **no** 形式を使用します。

anyconnect df-bit-ignore {enable | none}

no anyconnect df-bit-ignore {enable | none}

構文の説明

enable	AnyConnect クライアントで DF ビットの無視をイネーブルにします。
none	AnyConnect クライアントで DF ビットをディセーブルにします。

デフォルト

デフォルトでは、このオプションはイネーブルになっていません。

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
グループ ポリシー webvpn 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(2)	**svc df-bit-ignore** コマンドが追加されました。
8.4(3)	**svc df-bit-ignore** コマンドが **anyconnect df-bit-ignore** コマンドに置き換えられました。

例

```
vmb-5520(config-group-webvpn)# anyconnect routing-filtering-ignore ?

config-group-webvpn mode commands/options:
  enable  Enable Routing/Filtering for AnyConnect Client
  none    Disable Routing/Filtering for AnyConnect Client
```

anyconnect dpd-interval

デッド ピア検出（DPD）を ASA でイネーブルにし、リモート クライアントと ASA のいずれかで SSL VPN 接続を介した DPD を実行する頻度を設定するには、グループ ポリシー webvpn またはユーザ名 webvpn コンフィギュレーション モードで **anyconnect dpd-interval** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

anyconnect dpd-interval {[**gateway** {*seconds* | **none**}] | [**client** {*seconds* | **none**}]}

no anyconnect dpd-interval {[**gateway** {*seconds* | **none**}] | [**client** {*seconds* | **none**}]}

構文の説明

client none	クライアントで実行される DPD をディセーブルにします。
client *seconds*	クライアントで DPD が実行される頻度（30 ～ 3600 秒）を指定します。
gateway none	ASA で実行される DPD テストをディセーブルにします。
gateway *seconds*	ASA で DPD が実行される頻度（30 ～ 3600 秒）を指定します。値 300 が推奨されます。

デフォルト

デフォルトでは、DPD はイネーブルであり、ASA（ゲートウェイ）とクライアントの両方で 30 秒に設定されます。

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
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザ名 webvpn 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。
8.0(3)	デフォルト設定が、ディセーブルから、ASA（ゲートウェイ）とクライアントの両方で 30 秒に変更されました。
8.4(1)	**svc dpd-interval** コマンドが **anyconnect dpd-interval** コマンドに置き換えられました。

使用上のガイドライン

gateway は、ASA のことです。DPD をイネーブルにし、ASA がクライアントからのパケットを待機する間隔を指定します。その間隔内にパケットが受信されない場合、ASA は同じ間隔で DPD テストを 3 回試行します。クライアントからの応答を受信しない場合、ASA は TLS/DTLS トンネルを切断します。

（注） ASA の DPD プロセスは、TLS/DTLS トンネルを介してクライアントに送信するパケットが ASA にある場合にのみトリガーされます。

例

次に、既存のグループ ポリシー *sales* について、ASA（ゲートウェイ）で実行される DPD の頻度を 3000 秒に設定し、クライアントで実行される DPD の頻度を 1000 秒に設定する例を示します。

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect dpd-interval gateway 3000
ciscoasa(config-group-webvpn)# anyconnect dpd-interval client 1000
```

anyconnect dtls compression

特定のグループまたはユーザに対して低帯域幅リンクの圧縮をイネーブルにするには、グループ ポリシー webvpn またはユーザ名 webvpn コンフィギュレーション モードで **anyconnect dtls compression** コマンドを使用します。グループから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。

anyconnect dtls compression {lzs | none}

no anyconnect dtls compression {lzs | none}

構文の説明

lzs	ステートレス圧縮アルゴリズムをイネーブルにします。
none	圧縮をディセーブルにします。

デフォルト

デフォルトでは、AnyConnect 圧縮はイネーブルではありません。

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
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザ名 webvpn 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(2)	このコマンドが追加されました。

例

次に、圧縮をディセーブルにするシーケンスの例を示します。

```
asa# config terminal
asa(config)# group-policy DfltGrpPolicy attributes
asa(config-group-policy)# webvpn
asa(config-group-webvpn)# anyconnect ssl compression none
asa(config-group-webvpn)# anyconnect dtls compression none
```

anyconnect enable

ASA が AnyConnect クライアントをリモート コンピュータにダウンロードしたり、SSL または IKEv2 搭載の AnyConnect クライアントを使用して ASA に接続したりできるようにするには、webvpn コンフィギュレーション モードで **anyconnect enable** コマンドを使用します。このコマンドを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。

anyconnect enable

no anyconnect enable

デフォルト

このコマンドのデフォルトはディセーブルです。ASA はクライアントをダウンロードしません。

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
webvpn 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 **svc enable** として追加されました。
8.4(1)	**svc enable** コマンドが **anyconnect enable** コマンドに置き換えられました。

使用上のガイドライン

no anyconnect enable コマンドを入力しても、アクティブなセッションは終了しません。

anyconnect enable コマンドは、**anyconnect image xyz** コマンドで AnyConnect イメージを設定した後に発行する必要があります。AnyConnect クライアントまたは AnyConnect WebLaunch を使用するには、**anyconnect enable** が必要です。**anyconnect enable** コマンドを SSL または IKEv2 とともに発行しないと、AnyConnect は想定どおりに動作せず、IPsec VPN 接続終了エラーでタイムアウトします。この結果、**show webvpn svc** コマンドは SSL VPN クライアントがイネーブルであると見なさず、インストールされた AnyConnect パッケージをリストしません。

例

次に、ASA でクライアントをダウンロードできるようにする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# anyconnect enable
```

関連コマンド

コマンド	説明
anyconnect image	リモート PC へのダウンロードのために ASA がキャッシュ メモリで展開する AnyConnect SSL VPN クライアント パッケージ ファイルを指定します。
anyconnect modules	AnyConnect SSL VPN Client でオプション機能に必要なモジュールの名前を指定します。
anyconnect profiles	ASA によって Cisco AnyConnect SSL VPN Client にダウンロードされるプロファイルを保管するために使用するファイルの名前を指定します。
show webvpn anyconnect	ASA にインストールされ、リモート PC へのダウンロード用にキャッシュ メモリにロードされた SSL VPN クライアントの情報を表示します。
anyconnect localization	Cisco AnyConnect VPN Client にダウンロードされたローカリゼーション ファイルを保管するために使用するパッケージ ファイルを指定します。

anyconnect-essentials

ASA の AnyConnect Essentials をイネーブルにするには、グループ ポリシー webvpn コンフィギュレーション モードで **anyconnect-essentials** コマンドを使用します。AnyConnect Essentials の使用をディセーブルにし、代わりにプレミアム AnyConnect クライアントをイネーブルにするには、このコマンドの **no** 形式を使用します。

anyconnect-essentials

no anyconnect-essentials

デフォルト

AnyConnect Essentials 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
webvpn 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

このコマンドでは、完全な AnyConnect クライアント ライセンスがインストールされていることを前提として、AnyConnect SSL VPN Client 全体の使用と AnyConnect Essentials SSL VPN Client の使用を切り替えます。AnyConnect Essentials は、個別にライセンス供与される SSL VPN クライアントで、すべて ASA 上に設定されます。プレミアム AnyConnect の機能を提供しますが、次の例外があります。

- CSD を使用できない（HostScan/Vault/Cache Cleaner を含む）
- クライアントレス SSL VPN 非対応

AnyConnect Essentials クライアントは、Microsoft Windows Vista、Windows Mobile、Windows XP、Windows 2000、Linux、または Macintosh OS X を実行しているリモート エンド ユーザに Cisco SSL VPN Client の利点をもたらします。

AnyConnect Essentials ライセンスは、**anyconnect-essentials** コマンドを使用してイネーブルまたはディセーブルにします。このコマンドは、AnyConnect Essentials ライセンスが ASA にインストールされている場合にのみ有効です。このライセンスがない場合は、このコマンドを実行すると次のエラー メッセージが表示されます。

```
ERROR: Command requires AnyConnect Essentials license
```

(注) このコマンドは、AnyConnect Essentials の使用をイネーブルまたはディセーブルにするだけです。AnyConnect Essentials *ライセンス*自体は、**anyconnect-essentials** コマンドの設定の影響を受けません。

AnyConnect Essentials ライセンスがイネーブルの場合、AnyConnect クライアントは Essentials モードを使用し、クライアントレス SSL VPN アクセスはディセーブルになります。AnyConnect Essentials ライセンスがディセーブルの場合、AnyConnect クライアントは完全な AnyConnect SSL VPN Client ライセンスを使用します。

(注) このコマンドは、ASAv ではサポートされません。詳細については、ライセンスのマニュアルを参照してください。

アクティブなクライアントレス SSL VPN 接続がある場合に AnyConnect Essentials ライセンスをイネーブルにすると、すべての接続がログオフするため、接続を再確立する必要があります。

例

次に、ユーザが webvpn コンフィギュレーション モードを開始して AnyConnect Essentials VPN Client をイネーブルにする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# anyconnect-essentials
```

anyconnect firewall-rule

パブリックまたはプライベートの ACL ファイアウォールを確立するには、グループ ポリシー webvpn またはユーザ名 webvpn コンフィギュレーション モードで **AnyConnect firewall-rule** コマンドを使用します。

anyconnect firewall-rule client interface {public | private} *ACL*

構文の説明

ACL	アクセス コントロール リストを指定します。
client interface	クライアント インターフェイスを指定します。
private	プライベート インターフェイス ルールを設定します。
public	パブリック インターフェイス ルールを設定します。

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
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザ名 webvpn 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
8.3(1)	この **svc firewall-rule** コマンドが追加されました。
8.4(1)	**svc firewall-rule** コマンドが **anyconnect firewall-rule** コマンドに置き換えられました。
9.0(1)	コマンドの ACL を、IPv4 アドレスと IPv6 アドレスの両方を指定できるユニファイド アクセス コントロール ルールにすることができるようになりました。

使用上のガイドライン

このコマンドを想定どおりに機能させるためには、AnyConnect セキュア モビリティ クライアントの AnyConnect Secure Mobility ライセンス サポートを提供する AsyncOS for Web バージョン 7.0 のリリースが必要です。また、AnyConnect Secure Mobility、ASA 8.3、ASDM 6.3 をサポートする AnyConnect リリースも必要です。

ここに記載したのは、AnyConnect クライアントではファイアウォールがどのように使用されるかについての注意事項です。

- ファイアウォール ルールには送信元 IP は使用されません。クライアントでは、ASA から送信されたファイアウォール ルール内の送信元 IP 情報は無視されます。送信元 IP は、ルールがパブリックかプライベートかに応じてクライアントが特定します。パブリック ルールは、クライアント上のすべてのインターフェイスに適用されます。プライベート ルールは、仮想アダプタに適用されます。
- ASA は、ACL ルールに対して数多くのプロトコルをサポートしています。ただし、AnyConnect のファイアウォール機能でサポートされているのは、TCP、UDP、ICMP、および IP のみです。クライアントでは、異なるプロトコルでルールが受信された場合、そのルールは無効なファイアウォール ルールとして処理され、さらにセキュリティ上の理由からスプリット トンネリングが無効となり、フル トンネリングが使用されます。

ただし次のように、オペレーティング システムによって動作が異なるため注意が必要です。

- Windows コンピュータの場合、Windows Firewall では拒否ルールが許可ルールに優先します。ASA により許可ルールが AnyConnect クライアントへプッシュされても、ユーザがカスタムの拒否ルールを作成していれば、AnyConnect ルールは適用されません。
- Windows Vista では、ファイアウォール ルールが作成されると、ポート番号の範囲がカンマ区切りの文字列として認識されます（たとえば、1 ～ 300 や 5000 ～ 5300）。許可されているポートの最大数は 300 です。指定した数が 300 ポートを超える場合は、最初の 300 ポートに対してのみファイアウォール ルールが適用されます。
- ファイアウォール サービスが AnyConnect クライアントにより開始される必要がある（システムにより自動的に開始されない）Windows ユーザは、VPN 接続の確立にかなりの時間を要する場合があります。
- Mac コンピュータの場合、AnyConnect クライアントでは、ASA で適用されたのと同じ順序でルールが適用されます。グローバル ルールは必ず最後になるようにしてください。
- サードパーティ ファイアウォールの場合、AnyConnect クライアント ファイアウォールとサードパーティ ファイアウォールの双方で許可されたタイプのトラフィックのみ通過できます。AnyConnect クライアントで許可されているタイプのトラフィックであっても、サードパーティ ファイアウォールによってブロックされれば、そのトラフィックはクライアントでもブロックされます。

ローカル印刷およびテザー デバイス サポートに関する ACL ルールの例を含め、AnyConnect クライアント ファイアウォールの詳細については、『*AnyConnect Administrator's Guide*』を参照してください。

例

次に、*ACL AnyConnect_Client_Local_Print* をパブリック ファイアウォールとしてイネーブルにする例を示します。

```
ciscoasa(config)# group-policy example_group attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect firewall-rule client-interface public value
AnyConnect_Client_Local_Print
```

関連コマンド

コマンド	説明
show webvpn anyconnect	インストールされている SSL VPN クライアントに関する情報を表示します。
anyconnect	特定のグループまたはユーザに対して SSL VPN クライアントをイネーブルまたは必須にします。
anyconnect image	リモート PC へのダウンロードのために ASA がキャッシュ メモリで展開するクライアント パッケージ ファイルを指定します。

anyconnect image

AnyConnect 配布パッケージをインストールまたはアップグレードして、実行コンフィギュレーションに追加するには、webvpn コンフィギュレーション モードで **AnyConnect image** コマンドを使用します。AnyConnect 配布パッケージ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。

anyconnect image *path order* [**regex** *expression*]

no anyconnect image *path order* [**regex** *expression*]

構文の説明

order	クライアント パッケージ ファイルが複数である場合は、パッケージ ファイルの順序（1 ～ 65535）を指定します。ASA では、オペレーティング システムと一致するまで、指定した順序に従って、各クライアントの一部をリモート PC にダウンロードします。
path	AnyConnect パッケージのパスおよびファイル名を 255 文字以内で指定します。
regex *expression*	ブラウザから渡される user-agent 文字列と照合するために ASA によって使用される文字列を指定します。

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
webvpn 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 **svc image** として追加されました。
8.0(1)	**regex** キーワードが追加されました。
8.4(1)	**svc image** コマンドが **anyconnect image** コマンドに置き換えられました。

使用上のガイドライン

パッケージ ファイルの番号付けにより、ASA が、オペレーティング システムと一致するまで、パッケージ ファイルの一部をリモート PC にダウンロードする順序が確立されます。最も番号の小さいパッケージ ファイルが最初にダウンロードされます。したがって、リモート PC で最も一般的に使用されるオペレーティング システムと一致するパッケージ ファイルに、最も小さい番号を割り当てる必要があります。

デフォルトの順序は 1 です。*order* 引数を指定しない場合は、**svc image** コマンドを入力するたびに、以前に番号 1 と見なされたイメージに上書きします。

クライアント パッケージ ファイルごとに任意の順序で **anyconnect image** コマンドを入力できます。たとえば、2 番目（*order* 2）にダウンロードされるパッケージ ファイルを指定してから、最初（*order* 1）にダウンロードされるパッケージ ファイルを指定する **anyconnect image** コマンドを入力できます。

モバイル ユーザの場合、**regex** keyword を使用して、モバイル デバイスの接続時間を短縮できます。ブラウザが ASA に接続するとき、user-agent 文字列が HTTP ヘッダーに含められます。ASA によってストリングが受信され、そのストリングがあるイメージ用に設定された式と一致すると、そのイメージがただちにダウンロードされます。この場合、他のクライアント イメージはテストされません。

（注） スタンドアロン クライアントを使用している場合、**regex** コマンドは無視されます。また、パフォーマンス向上のため Web ブラウザでのみ使用され、正規表現文字列はスタンドアロン クライアントから提供されるユーザまたはエージェントと照合されません。

ASA では、AnyConnect クライアントと Cisco Secure Desktop（CSD）の両方のパッケージ ファイルがキャッシュ メモリに展開されます。ASA でパッケージ ファイルを正常に展開するには、パッケージ ファイルのイメージとファイルを保管するのに十分なキャッシュ メモリが必要です。

パッケージの展開に十分なキャッシュ メモリがないことを ASA が検出した場合、コンソールにエラー メッセージが表示されます。次に、**svc image** コマンドを使用してパッケージ ファイルをインストールしようとした後でレポートされるエラー メッセージの例を示します。

```
ciscoasa(config-webvpn)# anyconnect image disk0:/anyconnect-win-3.0.0520-k9.pkg
ERROR: File write error (check disk space)
ERROR: Unable to load SVC image - extraction failed
```

これがパッケージ ファイルのインストール試行中に発生した場合、グローバル コンフィギュレーション モードから **dir cache:/** コマンドを使用して、キャッシュ メモリの残りとこれまでにインストールされたパッケージのサイズを確認します。

（注） ASA にデフォルトの内部フラッシュ メモリ サイズまたはデフォルトの DRAM サイズ（キャッシュ メモリ用）だけがある場合、ASA 上で複数の AnyConnect クライアント パッケージを保存およびロードすると、問題が発生することがあります。フラッシュ メモリにパッケージ ファイルに十分な容量がある場合でも、クライアントの unzip とロードのときに ASA のキャッシュ メモリが不足する場合があります。AnyConnect を使用する場合の ASA のメモリ要件について、および ASA で行えるメモリ アップグレードの詳細については、Cisco ASA 5500 シリーズの最新のリリース ノートを参照してください。

例

次に、Windows、MAC、Linux 用の AnyConnect クライアント パッケージ ファイルをこの順序でロードする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# anyconnect image disk0:/anyconnect-win-3.0.0527-k9.pkg 1
ciscoasa(config-webvpn)# anyconnect image disk0:/anyconnect-macosx-i386-3.0.0414-k9.pkg 2
ciscoasa(config-webvpn)# anyconnect image disk0:/anyconnect-linux-3.0.0414-k9.pkg 3
ciscoasa(config-webvpn)
```

次に、ロードされた AnyConnect クライアント パッケージとその順序を表示する、**show webvpn anyconnect** コマンドの出力例を示します。

```
ciscoasa(config-webvpn)# show webvpn anyconnect
1. disk0:/anyconnect-win-3.0.0527-k9.pkg 1 dyn-regex=/Windows NT/
  CISCO STC win2k+
  3,0,0527
  Hostscan Version 3.0.0527
  Tue 10/19/2010 16:16:56.25

2. disk0:/anyconnect-macosx-i386-3.0.0414-k9.pkg 2 dyn-regex=/Intel Mac OS X/
  CISCO STC Darwin_i386
  3.0.0414
  Wed Oct 20 20:39:53 MDT 2010

3. disk0:/anyconnect-linux-3.0.0414-k9.pkg 3 dyn-regex=/Linux i[1-9]86/
  CISCO STC Linux
  3.0.0414
  Wed Oct 20 20:42:02 MDT 2010

3 AnyConnect Client(s) installed
ciscoasa(config-webvpn)#
```

関連コマンド

コマンド	説明
anyconnect modules	AnyConnect SSL VPN Client でオプション機能に必要なモジュールの名前を指定します。
anyconnect profiles	ASA によって Cisco AnyConnect SSL VPN Client にダウンロードされるプロファイルを保管するために使用するファイルの名前を指定します。
show webvpn anyconnect	ASA にインストールされ、リモート PC へのダウンロード用にキャッシュ メモリにロードされた SSL VPN クライアントの情報を表示します。
anyconnect localization	Cisco AnyConnect VPN Client にダウンロードされたローカリゼーション ファイルを保管するために使用するパッケージ ファイルを指定します。

anyconnect keep-installer

(注) このコマンドは、2.5 より後の AnyConnect バージョンには適用されませんが、下位互換性のため引き続き使用可能です。**anyconnect keep-installer** コマンドを設定しても、AnyConnect 3.0 以降には影響しません。

リモート PC への SSL VPN クライアントの永続インストールをイネーブルにするには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで、**AnyConnect keep-installer** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

anyconnect keep-installer {**installed** | **none**}

no anyconnect keep-installer {**installed** | **none**}

構文の説明

installed	クライアントの自動アンインストール機能をディセーブルにします。クライアントは、今後の接続のためにリモート PC 上にインストールされたままになります。
none	アクティブな接続の終了後にクライアントがリモート コンピュータからアンインストールされることを指定します。

デフォルト

デフォルトでは、クライアントの永続インストールがイネーブルです。セッションの終了時に、クライアントはリモート コンピュータ上に残ります。

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。

	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 webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザ名 webvpn 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)	**svc keep-installer** コマンドが追加されました。
8.4(1)	**svc keep-installer** コマンドが **anyconnect keep-installer** コマンドに置き換えられました。

例

次の例では、ユーザはグループ ポリシー webvpn コンフィギュレーション モードを開始し、セッションの終了時にクライアントを削除するようにグループ ポリシーを設定します。

```
ciscoasa(config-group-policy)#webvpn
ciscoasa(config-group-webvpn)# anyconnect keep-installer none
ciscoasa(config-group-webvpn)#
```

関連コマンド

コマンド	説明
show webvpn anyconnect	ASA にインストールされ、リモート PC へのダウンロード用にキャッシュ メモリにロードされた AnyConnect PCs クライアントの情報を表示します。
anyconnect	特定のグループまたはユーザに対して SSL VPN クライアントをイネーブルまたは必須にします。
anyconnect enable	ASA によって AnyConnect PCs クライアント ファイルをリモート PC にダウンロードできるようにします。
anyconnect image	リモート PC へのダウンロード用に ASA によってキャッシュ メモリに展開されている AnyConnect クライアント パッケージ ファイルを指定します。

anyconnect modules

オプション機能のために AnyConnect SSL VPN Client で必要となるモジュールの名前を指定するには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで、**anyconnect modules** コマンドを使用します。このコマンドを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。

anyconnect modules {**none** | **value** *string*}

no anyconnect modules {**none** | **value** *string*}

構文の説明

string	オプション モジュールの名前（最大 256 文字）。複数のストリングを指定する場合は、カンマで区切ります。

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
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザ名 webvpn 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)	**svc modules** コマンドが追加されました。
8.4(1)	**svc modules** コマンドが **anyconnect modules** コマンドに置き換えられました。

使用上のガイドライン

ダウンロード時間を最小にするために、クライアントでは、サポートする各機能に必要なモジュールのダウンロード（ASA から）のみを要求します。**anyconnect modules** コマンドにより、ASA でこれらのモジュールをダウンロードできます。

次の表に、AnyConnect モジュールを表す文字列値を示します。

AnyConnect モジュールを表す文字列	AnyConnect モジュール名
dart	AnyConnect DART（診断およびレポート ツール）
nam	AnyConnect ネットワーク アクセス マネージャ
vpngina	AnyConnect SBL（ログイン前の起動）
websecurity	AnyConnect Web セキュリティ モジュール
telemetry	AnyConnect テレメトリ モジュール
posture	AnyConnect ポスチャ モジュール
none	**none** を選択すると、ASA によって基本的なファイルがダウンロードされ、オプションのモジュールはダウンロードされません。既存のモジュールはグループ ポリシーから削除されます。

例

次の例では、ユーザはグループ ポリシー *PostureModuleGroup* のグループ ポリシー属性モードを開始し、そのグループ ポリシーの webvpn コンフィギュレーション モードを開始しています。さらに、ASA に接続すると AnyConnect ポスチャ モジュールおよび AnyConnect テレメトリ モジュールがエンドポイントにダウンロードされるように、文字列 *posture* および *telemetry* を指定しています。

```
ciscoasa> en
Password:
ciscoasa# config t
ciscoasa(config)# group-policy PostureModuleGroup attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect modules value posture,telemetry
ciscoasa(config-group-webvpn)# write mem
Building configuration...
Cryptochecksum: 40975338 b918425d 083b391f 9e5a5c69

22055 bytes copied in 3.440 secs (7351 bytes/sec)
[OK]
ciscoasa(config-group-webvpn)#
```

グループ ポリシーからモジュールを削除するには、保持するモジュールの値だけを指定したコマンドを再送信します。たとえば、このコマンドはテレメトリ モジュールを削除します。

```
ciscoasa(config-group-webvpn)# anyconnect modules value posture
```

関連コマンド

コマンド	説明
show webvpn anyconnect	ASA のキャッシュ メモリにロードされていてダウンロード可能な AnyConnect パッケージについての情報を表示します。
anyconnect enable	特定のグループまたはユーザに対して、AnyConnect クライアントをイネーブルにします。
anyconnect image	リモート PC へのダウンロード用に ASA によってキャッシュ メモリに展開されている AnyConnect クライアント パッケージ ファイルを指定します。

anyconnect mtu

Cisco AnyConnect VPN Client によって確立された VPN 接続の MTU サイズを調整するには、グループポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで、**anyconnect mtu** コマンドを使用します。このコマンドを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。

anyconnect mtu *size*

no anyconnect mtu *size*

構文の説明

size	MTU サイズ（バイト単位）。576 ～ 1406 バイトです。

デフォルト

デフォルトのサイズは 1406 バイトです。

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 webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザ名 webvpn 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)	**svc mtu** コマンドが追加されました。
8.4(1)	**svc mtu** コマンドが **anyconnect mtu** コマンドに置き換えられました。

使用上のガイドライン

このコマンドは、AnyConnect クライアントのみに影響します。VPN Client は、異なる MTU サイズに調整できません。

デフォルトのグループ ポリシーでのこのコマンドのデフォルトは、**no svc mtu** です。MTU サイズは、接続で使用されているインターフェイスの MTU に基づき、IP/UDP/DTLS のオーバーヘッドを差し引いて、自動的に調整されます。

IPv6 対応インターフェイスで許可される最小 MTU は 1280 バイトです。ただし、IPsec がインターフェイスでイネーブルになっている場合、MTU 値は、IPsec 暗号化のオーバーヘッドのために 1380 未満に設定できません。インターフェイスを 1380 バイト未満に設定すると、パケットのドロップが発生する可能性があります。

例

次に、グループ ポリシー *telecommuters* について、MTU サイズを 500 バイトに設定する例を示します。

```
ciscoasa(config)# group-policy telecommuters attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect mtu 500
```

関連コマンド

コマンド	説明
anyconnect keep-installer	クライアントの自動アンインストール機能をディセーブルにします。初期ダウンロード後、接続が終了した後もクライアントはリモート PC 上に残ります。
anyconnect ssl dtls	SSL VPN 接続を確立する CVC に対して DTLS をイネーブルにします。
show run webvpn	**anyconnect** コマンドを含む、WebVPN に関するコンフィギュレーション情報を表示します。

anyconnect profiles（グループ ポリシー属性 > webvpn、ユーザ名属性 > webvpn）

Cisco AnyConnect VPN Client（CVC）ユーザにダウンロードされる CVC プロファイル パッケージを指定するには、webvpn またはコンフィギュレーション モードで **anyconnect profiles** コマンドを使用します。webvpn コンフィギュレーション モードにアクセスするには、最初にグループ ポリシー属性コマンドまたはユーザ名属性を入力します。コンフィギュレーションからこのコマンドを削除し、値を継承するには、コマンドの **no** 形式を使用します。

anyconnect profiles {**value** *profile* | **none**}

no anyconnect profiles {**value** *profile* | **none** } **[type** *type*]

構文の説明

value *profile*	プロファイル名。
none	ASA によってプロファイルはダウンロードされません。
type *type*	標準 AnyConnect プロファイルまたは任意の英数字値に一致するユーザ。

デフォルト

デフォルトは none です。ASA によってプロファイルはダウンロードされません。

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
webvpn 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)	**svc profiles** コマンドが追加されました。
8.3(1)	オプションのタイプ **value** が追加されました。
8.4(1)	**svc profiles** コマンドが **anyconnect profiles** コマンドに置き換えられました。

使用上のガイドライン

このコマンドをグループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名属性 webvpn コンフィギュレーション モードで入力すると、ASA によってグループ ポリシーまたはユーザ名に基づいてプロファイルを CVC ユーザにダウンロードできます。CVC プロファイルをすべての CVC ユーザにダウンロードするには、このコマンドを webvpn コンフィギュレーション モードで使用します。

CVC プロファイルとは、CVC ユーザ インターフェイスに表示される接続エントリを設定するために CVC が使用するコンフィギュレーション パラメータのグループで、ホスト コンピュータの名前とアドレスが含まれます。CVC ユーザ インターフェイスを使用して、プロファイルを作成および保存できます。また、テキスト エディタでこのファイルを編集し、ユーザ インターフェイスからは設定できないパラメータの詳細を設定することもできます。

CVC のインストレーションには、他のプロファイル ファイルを編集し、作成するための基礎として使用できる、1 つのプロファイル テンプレート（cvcprofile.xml）が含まれています。CVC プロファイルの編集の詳細については、『*Cisco AnyConnect VPN Client Administrator Guide*』を参照してください。

例

次の例では、ユーザは使用可能なプロファイルを表示する **anyconnect profiles value** コマンドを入力します。

```
ciscoasa(config-group-webvpn)# anyconnect profiles value ?

config-group-webvpn mode commands/options:
Available configured profile packages:
  engineering
  sales
```

次に、ユーザは CVC プロファイル sales を使用するようにグループ ポリシーを設定します。

```
ciscoasa(config-group-webvpn)# anyconnect profiles sales
```

関連コマンド

コマンド	説明
show webvpn anyconnect	インストールされている AnyConnect クライアントに関する情報を表示します。
anyconnect	特定のグループまたはユーザに SSL VPN クライアントをイネーブルにします。または、要求します。
anyconnect image	リモート PC へのダウンロード用に ASA によってキャッシュ メモリに展開されている AnyConnect クライアント パッケージ ファイルを指定します。

anyconnect profiles（webvpn）

ASA によってキャッシュ メモリにロードされて、Cisco AnyConnect VPN Client（CVC）ユーザのグループ ポリシーおよびユーザ名属性で使用可能となるプロファイル パッケージとしてファイルを指定するには、webvpn コンフィギュレーション モードで **anyconnect profiles** コマンドを使用します。コンフィギュレーションからこのコマンドを削除し、ASA によってパッケージ ファイルがキャッシュ メモリからアンロードされるようにするには、このコマンドの **no** 形式を使用します。

anyconnect profiles {*profile path*}

no anyconnect profiles {*profile path*}

構文の説明

path	ASA のフラッシュ メモリ内のプロファイル ファイルのパスおよびファイル名。
profile	キャッシュ メモリ内に作成するプロファイルの名前。

デフォルト

デフォルトは none です。プロファイル パッケージは ASA によってキャッシュ メモリにロードされません。

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
webvpn 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)	**svc profiles** コマンドが追加されました。
8.4(1)	**svc profiles** コマンドが **anyconnect profiles** コマンドに置き換えられました。

使用上のガイドライン

CVC プロファイルとは、CVC ユーザ インターフェイスに表示される接続エントリを設定するために CVC が使用するコンフィギュレーション パラメータのグループで、ホスト コンピュータの名前とアドレスが含まれます。CVC ユーザ インターフェイスを使用して、プロファイルを作成および保存できます。

また、テキスト エディタでこのファイルを編集し、ユーザ インターフェイスからは設定できないパラメータの詳細を設定することもできます。CVC のインストレーションには、他のプロファイル ファイルを編集し、作成するための基礎として使用できる、1 つのプロファイル テンプレート（cvcprofile.xml）が含まれています。CVC プロファイルの編集の詳細については、『*Cisco AnyConnect VPN Client Administrator Guide*』を参照してください。

新しい CVC プロファイルを作成してフラッシュ メモリにアップロードした後、webvpn コンフィギュレーション モードで **anyconnect profiles** コマンドを使用して、ASA に対して XML ファイルをプロファイルとして指定します。このコマンドを入力すると、ファイルは ASA のキャッシュ メモリにロードされます。次に、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名属性コンフィギュレーション モードで **anyconnect profiles** コマンドを使用して、グループまたはユーザのプロファイルを指定できます。

例

次の例では、ユーザは、以前に CVC のインストールで提供された cvcprofile.xml ファイルから 2 つの新しいプロファイル ファイル（sales_hosts.xml および engineering_hosts.xml）を作成し、ASA のフラッシュ メモリにアップロードしています。

さらに、ユーザはそれらのファイルを CVC のプロファイルとして ASA に指定し、*sales* と *engineering* という名前を指定しています。

```
ciscoasa(config-webvpn)# anyconnect profiles sales disk0:sales_hosts.xml
ciscoasa(config-webvpn)# anyconnect profiles engineering disk0:engineering_hosts.xml
```

dir cache:stc/profiles コマンドを入力すると、キャッシュ メモリにロードされているプロファイルが表示されます。

```
ciscoasa(config-webvpn)# dir cache:stc/profiles

Directory of cache:stc/profiles/

0      ----  774         11:54:41 Nov 22 2006  engineering.pkg
0      ----  774         11:54:29 Nov 22 2006  sales.pkg

2428928 bytes total (18219008 bytes free)
ciscoasa(config-webvpn)#
```

これらのプロトコルは、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名属性コンフィギュレーション モードでの **svc profiles** コマンドで使用できます。

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect profiles value ?

config-group-webvpn mode commands/options:
Available configured profile packages:
  engineering
  sales
```

関連コマンド

コマンド	説明
show webvpn anyconnect	インストールされている AnyConnect クライアントに関する情報を表示します。
anyconnect	特定のグループまたはユーザに対して SSL VPN クライアントをイネーブルまたは必須にします。
anyconnect image	ASA がリモート PC にダウンロードするためにキャッシュ メモリに展開する AnyConnect パッケージ ファイルを指定します。

anyconnect ssl compression

特定のグループまたはユーザについて、SSL VPN 接続での http データの圧縮をイネーブルにするには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで、**anyconnect ssl compression** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

anyconnect ssl compression {**deflate** | **lzs** | **none**}

no anyconnect ssl compression {**deflate** | **lzs** | **none**}

構文の説明

deflate	デフレート圧縮アルゴリズムをイネーブルにします。
lzs	ステートレス圧縮アルゴリズムをイネーブルにします。
none	圧縮をディセーブルにします。

デフォルト

デフォルトでは、圧縮は none（ディセーブル）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。

	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 webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザ名 webvpn 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(2)	**anyconnect compression** コマンドが追加されました。

使用上のガイドライン

SSL VPN 接続の場合、webvpn コンフィギュレーション モードで設定された **compression** コマンドによって、グループ ポリシー webvpn モードおよびユーザ名 webvpn モードで設定された **anyconnect ssl compression** コマンドは上書きされます。

例

次の例では、グループ ポリシー sales に対して SVC 圧縮はディセーブルです。

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect ssl compression none
```

関連コマンド

コマンド	説明
anyconnect	特定のグループまたはユーザに対して SSL VPN クライアントをイネーブルまたは必須にします。
anyconnect keepalive	リモート コンピュータ上のクライアントから ASA にキープアライブ メッセージが SSL VPN 接続で送信される頻度を指定します。
anyconnect keep-installer	クライアントの自動アンインストール機能をディセーブルにします。クライアントは、今後の接続のためにリモート PC 上にインストールされたままになります。
anyconnect rekey	SSL VPN 接続でクライアントがキーの再生成を実行できるようにします。
compression	すべての SSL、WebVPN、および IPsec VPN 接続で、圧縮をイネーブルにします。
show webvpn anyconnect	インストールされている SSL VPN クライアントに関する情報を表示します。

anyconnect ssl df-bit-ignore

特定のグループまたはユーザについて SSL VPN 接続でパケットを強制的にフラグメント化できるようにする（トンネルを通過できるようにする）には、グループ ポリシー webvpn またはユーザ名 webvpn コンフィギュレーション モードで **anyconnect ssl df-bit-ignore** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

anyconnect ssl df-bit-ignore {enable | disable}

no anyconnect ssl df-bit-ignore

構文の説明

enable	SSL 搭載の AnyConnect で DF ビットの無視をイネーブルにします。
disable	SSL 搭載の AnyConnect で DF ビットをディセーブルにします。

デフォルト

DF ビットの無視は、*ディセーブル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。

	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 webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザ名 webvpn 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)	**svc df-bit-ignore** コマンドが **anyconnect ssl df-bit-ignore** コマンドに置き換えられました。

使用上のガイドライン

この機能では、DF ビットが設定されているパケットを強制的にフラグメント化して、トンネルを通過させることができます。使用例として、TCP MSS ネゴシエーションに適切に応答しないネットワークのサーバに対する使用などがあります。

例

次の例では、グループ ポリシー sales に対して DF ビットの無視がイネーブルになっています。

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect ssl df-bit-ignore enable
```

関連コマンド

コマンド	説明
anyconnect	特定のグループまたはユーザに対して SSL VPN クライアントをイネーブルまたは必須にします。
anyconnect keepalive	リモート コンピュータ上のクライアントから ASA にキープアライブ メッセージが SSL VPN 接続で送信される頻度を指定します。
anyconnect keep-installer	クライアントの自動アンインストール機能をディセーブルにします。クライアントは、今後の接続のためにリモート PC 上にインストールされたままになります。
anyconnect rekey	SSL VPN 接続でクライアントがキーの再生成を実行できるようにします。

anyconnect ssl dtls enable

Cisco AnyConnect VPN Client との SSL VPN 接続を確立している特定のグループまたはユーザのインターフェイスで Datagram Transport Layer Security（DTLS）接続をイネーブルにするには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名属性 webvpn コンフィギュレーション モードで **anyconnect ssl dtls enable** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

anyconnect ssl dtls enable *interface*

no anyconnect ssl dtls enable *interface*

構文の説明

interface	インターフェイスの名前。

デフォルト

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 webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザ名 webvpn 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)	**svc dtls** コマンドが追加されました。
8.4(1)	**svc dtls** コマンドが **anyconnect ssl dtls** コマンドに置き換えられました。

使用上のガイドライン

DTLS をイネーブルにすると、SSL VPN 接続を確立している AnyConnect クライアントで、2 つの同時トンネル（SSL トンネルと DTLS トンネル）を使用できます。DTLS によって、一部の SSL 接続に関連する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。

DTLS をイネーブルにしない場合、SSL VPN 接続を確立している AnyConnect クライアント ユーザは SSL トンネルのみで接続します。

このコマンドでは、特定のグループまたはユーザについて DTLS をイネーブルにします。すべての AnyConnect クライアント ユーザについて DTLS をイネーブルにするには、webvpn コンフィギュレーション モードで **anyconnect ssl dtls enable** コマンドを使用します。

例

次に、グループ ポリシー *sales* のグループ ポリシー webvpn コンフィギュレーション モードを開始し、DTLS をイネーブルにする例を示します。

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect ssl dtls enable
```

関連コマンド

コマンド	説明
dtls port	DTLS の UDP ポートを指定します。
anyconnect dtls	SSL VPN 接続を確立するグループまたはユーザに対して、DTLS をイネーブルにします。
vpn-tunnel-protocol	ASA がリモート アクセス用に許可する VPN プロトコル（SSL を含む）を指定します。

anyconnect ssl keepalive

SSL VPN 接続でリモート クライアントから ASA に送信されるキープアライブ メッセージの頻度を設定するには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで、**anyconnect ssl keepalive** コマンドを使用します。コンフィギュレーションからこのコマンドを削除し、値を継承するには、コマンドの **no** 形式を使用します。

anyconnect ssl keepalive {**none** | *seconds*}

no anyconnect ssl keepalive {**none** | *seconds*}

構文の説明

none	キープアライブ メッセージをディセーブルにします。
seconds	キープアライブ メッセージをイネーブルにし、メッセージの頻度（15 ～ 600 秒）を指定します。

デフォルト

デフォルトは 20 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
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザ名 webvpn 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)	**svc keepalive** コマンドが追加されました。
8.0(3)	デフォルト設定がディセーブルから 20 秒に変更されました。
8.4(1)	**svc keepalive** コマンドが **anyconnect ssl keepalive** コマンドに置き換えられました。

使用上のガイドライン

Cisco SSL VPN Client（SVC）と Cisco AnyConnect VPN Client の両方で、ASA への SSL VPN 接続を確立するときにキープアライブ メッセージを送信できます。

接続をアイドル状態で維持できる時間がデバイスによって制限されている場合も、プロキシ、ファイアウォール、または NAT デバイスを経由した SSL VPN 接続が確実に開いたままで保たれるように、キープアライブ メッセージの頻度を調整できます（*seconds* で指定）。

また、頻度を調整すると、リモート ユーザが Microsoft Outlook または Microsoft Internet Explorer などのソケット ベース アプリケーションをアクティブに実行していない場合でも、クライアントは切断および再接続されません。

(注) キープアライブはデフォルトでイネーブルになっています。キープアライブをディセーブルにすると、フェールオーバー イベントの際に、SSL VPN クライアント セッションはスタンバイ デバイスに引き継がれません。

例

次の例では、ユーザは、*sales* という名前の既存のグループ ポリシーについて、ASA を設定し、クライアントがキープアライブ メッセージを 300 秒(5 分)の頻度で送信できるようにします。

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect ssl keepalive 300
```

関連コマンド

コマンド	説明
anyconnect	特定のグループまたはユーザに SSL VPN クライアントをイネーブルにします。または、要求します。
anyconnect dpd-interval	ASA でデッド ピア検出(DPD)をイネーブルにし、クライアントまたは ASA によって DPD が実行される頻度を設定します。
anyconnect keep-installer	クライアントの自動アンインストール機能をディセーブルにします。クライアントは、今後の接続のためにリモート PC 上にインストールされたままになります。
anyconnect ssl rekey	セッションでクライアントがキーの再生成を実行できるようにします。

anyconnect ssl rekey

SSL VPN 接続でリモート クライアントがキーの再生成を実行できるようにするには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで **anyconnect ssl rekey** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

anyconnect ssl rekey {**method** {**ssl** | **new-tunnel**} | **time** *minutes* | **none**}

no anyconnect ssl rekey {**method** {**ssl** | **new-tunnel**} | **time** *minutes* | **none**}

構文の説明

method ssl	キーの再生成中にクライアントによって新しいトンネルが確立されることを指定します。
method new-tunnel	キーの再生成中にクライアントによって新しいトンネルが確立されることを指定します。
method none	キーの再生成をディセーブルにします。
time *minutes*	セッションの開始からキーの再生成が発生するまでの時間（分）を指定します。4 ～ 10080（1 週間）の範囲です。

デフォルト

デフォルトは none（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 webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザ名 webvpn 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)	**svc rekey** コマンドが追加されました。
8.0(2)	「中間者」攻撃の可能性を防ぐため、**svc rekey method ssl** コマンドの動作が **svc rekey method new-tunnel** コマンドの動作に変更されました。
8.4(1)	**svc rekey** コマンドが **anyconnect ssl rekey** コマンドに置き換えられました。

使用上のガイドライン

Cisco AnyConnect Secure Mobility Client は、ASA への SSL VPN 接続でキーの再生成を実行できます。キーの再生成方法を **ssl** または **new-tunnel** に設定すると、キー再生成時に SSL 再ネゴシエーションが行われず、クライアントがキー再生成時に新規トンネルを確立することが指定されます。

例

次の例では、ユーザは、グループ ポリシー *sales* に属するリモート クライアントがキーの再生成時に SSL と再ネゴシエートし、セッションの開始後 30 分でキーの再生成が発生することを指定します。

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anycoanynnect ssl rekey method ssl
ciscoasa(config-group-webvpn)# anyconnect ssl rekey time 30
```

関連コマンド

コマンド	説明
anyconnect enable	特定のグループまたはユーザに対して AnyConnect Secure Mobility Client をイネーブルまたは必須にします。
anyconnect dpd-interval	ASA でデッド ピア検出（DPD）をイネーブルにし、AnyConnect Secure Mobility Client または ASA によって DPD が実行される頻度を設定します。
anyconnect keepalive	リモート コンピュータ上の AnyConnect Secure Mobility Client から ASA にキープアライブ メッセージが送信される頻度を指定します。
anyconnect keep-installer	リモート コンピュータへの AnyConnect Secure Mobility Client の永続インストールをイネーブルにします。

apcf

Application Profile Customization Framework プロファイルをイネーブルにするには、webvpn コンフィギュレーション モードで **apcf** コマンドを使用します。特定の APCF スクリプト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。すべての APCF スクリプトをディセーブルにするには、このコマンドの **no** 形式を引数なしで使用します。

apcf URL/filename.ext

no apcf [URL/filename.ext]

構文の説明

filename.extension	APCF カスタマイゼーション スクリプトの名前を指定します。これらのスクリプトは、常に XML 形式です。拡張子は、.xml、.txt、.doc などです。
URL	ASA でロードして使用する APCF プロファイルの場所を指定します。http://、https://、tftp://、ftp://、flash:/、disk#:/' のいずれかの URL を使用します。 URL には、サーバ、ポート、およびパスを含めることができます。ファイル名のみを指定した場合、デフォルトの URL は flash:/ です。**copy** コマンドを使用して、APCF プロファイルをフラッシュ メモリにコピーできます。

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
webvpn 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

apcf コマンドを使用すると、ASA は非標準の Web アプリケーションと Web リソースを WebVPN 接続で正しくレンダリングされるように処理できます。APCF プロファイルには、特定のアプリケーションに関して、いつ(事前、事後)、どこの(ヘッダー、本文、要求、応答)、どのデータを変換するかを指定するスクリプトがあります。

ASA で複数の APCF プロファイルを使用できます。その場合、ASA は、それらのプロファイルを古いものから新しいものの順に 1 つずつ適用します。

APCF コマンドは、Cisco TAC のサポートがある場合にのみ使用することを推奨します。

例

次に、フラッシュ メモリの /apcf にある apcf1 という名前の APCF をイネーブルにする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# apcf flash:/apcf/apcf1.xml
ciscoasa(config-webvpn)#
```

次に、myserver という名前の HTTPS サーバ（ポート 1440）のパス /apcf にある apcf2.xml という名前の APCF をイネーブルにする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# apcf https://myserver:1440/apcf/apcf2.xml
ciscoasa(config-webvpn)#
```

関連コマンド

コマンド	説明
proxy-bypass	特定のアプリケーションに対してコンテンツの最低限の書き換えを設定します。
rewrite	トラフィックが ASA を通過するかどうかを決定します。
show running config webvpn apcf	APCF 設定を表示します。

app-agent heartbeat

ASA で実行されている app-agent（アプリケーション エージェント）のハートビート メッセージ間隔を設定して、Firepower シャーシの健全性をチェックするには、グローバル コンフィギュレーション モードで **app-agent heartbeat** コマンドを使用します。

app-agent heartbeat [**interval** *ms*] [**retry-count** *number*]

（注） Firepower シャーシでのみサポートされています。

構文の説明

interval *ms*	ハートビートの時間間隔を 100 ～ 6000 ms の範囲の 100 の倍数単位で設定します。デフォルトは 1000 ms です。
retry-count *number*	再試行の回数を 1 ～ 30 の間で設定します。デフォルトの試行回数は 3 回です。

コマンド デフォルト

デフォルトの間隔は 1000 ms です。

デフォルトの再試行回数は 3 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
9.6(2)	コマンドが追加されました。
9.9(1)	最小インターフェイスが 300 ms から 100 ms に変更されました。

使用上のガイドライン

ASA はホストの Firepower シャーシとのバックプレーンを介して通信できるかどうかをチェックします。

Firepower 4100/9300 の場合、最小の結合時間（*interval* x *retry-count*）は、600 ミリ秒未満にすることはできません。たとえば、間隔を 100 に、再試行回数を 3 に設定した場合、合計結合時間は 300 ミリ秒になりますが、これはサポートされていません。たとえば、間隔を 100 に設定し、再試行回数を 6 に設定して最小時間（600 ms）を満たすことができます。

例

次に、間隔を 300 ms に設定する例を示します。

```
ciscoasa(config)# app-agent heartbeat interval 300
```

関連コマンド

コマンド	説明
health-check	クラスタ ヘルス チェックのパラメータを設定します。

appl-acl

セッションに適用する設定済みの Web タイプ ACL を指定するには、DAP webvpn コンフィギュレーション モードで **appl-acl** コマンドを使用します。コンフィギュレーションから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。すべての Web タイプ ACL を削除するには、このコマンドの **no** 形式を引数なしで使用します。

appl-acl [*identifier***]**

no appl-acl [*identifier***]**

構文の説明

identifier	以前に設定した Web タイプ ACL の名前。最大長は 240 文字です。

デフォルト

デフォルトの値や動作はありません。

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
DAP webvpn 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
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

Web タイプ ACL 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 **access-list webtype** コマンドを使用します。

appl-acl コマンドを複数回使用して、複数の Web タイプ ACL を DAP ポリシーに適用できます。

例

次に、newacl という名前の設定済みの Web タイプ ACL をダイナミック アクセス ポリシーに適用する例を示します。

```
ciscoasa (config)# config-dynamic-access-policy-record Finance
ciscoasa(config-dynamic-access-policy-record)# webvpn
ciscoasa(config-dynamic-access-policy-record)# appl-acl newacl
```

関連コマンド

コマンド	説明
dynamic-access-policy-record	DAP レコードを作成します。
access-list_webtype	Web タイプ ACL を作成します。

application-access

認証された WebVPN ユーザに表示される WebVPN ホームページの [Application Access] フィールド、およびユーザがアプリケーションを選択したときに表示される [Application Access] ウィンドウをカスタマイズするには、カスタマイゼーション コンフィギュレーション モードで **application-access** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

application-access {**title** | **message** | **window**} {**text** | **style**} *value*

no application-access {**title** | **message** | **window**} {**text** | **style**} *value*

構文の説明

message	[Application Access] フィールドのタイトルの下に表示されるメッセージを変更します。
style	[Application Access] フィールドのスタイルを変更します。
text	[Application Access] フィールドのテキストを変更します。
title	[Application Access] フィールドのタイトルを変更します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）。
window	[Application Access] ウィンドウを変更します。

デフォルト

[Application Access] フィールドのデフォルトのタイトル テキストは「Application Access」です。

[Application Access] フィールドのデフォルトのタイトル スタイルは次のとおりです。

background-color:#99CCCC;color:black;font-weight:bold;text-transform:uppercase

[Application Access] フィールドのデフォルトのメッセージ テキストは「Start Application Client」です。

[Application Access] フィールドのデフォルトのメッセージ スタイルは次のとおりです。

background-color:#99CCCC;color:maroon;font-size:smaller.

[Application Access] ウィンドウのデフォルトのウィンドウ テキストは次のとおりです。

「Close this window when you finish using Application Access. Please wait for the table to be displayed before starting applications.」

[Application Access] ウィンドウのデフォルトのウィンドウ スタイルは次のとおりです。

background-color:#99CCCC;color:black;font-weight:bold

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
カスタマイゼーション 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

このコマンドには、**webvpn** コマンドまたは **tunnel-group webvpn-attributes** コマンドを使用してアクセスします。

style オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

次に、WebVPN ページに対する変更で最もよく行われるページ配色の変更に役立つヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注） WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次に、[Application Access] フィールドの背景色を RGB 16 進値 66FFFF（緑色の一種）にカスタマイズする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# application-access title style background-color:#66FFFF
```

関連コマンド

コマンド	説明
application-access hide-details	[Application Access] ウィンドウのアプリケーション詳細の表示をイネーブルまたはディセーブルにします。
browse-networks	WebVPN ホームページの [Browse Networks] フィールドをカスタマイズします。
file-bookmarks	WebVPN ホームページの [File Bookmarks] タイトルまたはリンクをカスタマイズします。
web-applications	WebVPN ホームページの [Web Application] フィールドをカスタマイズします。
web-bookmarks	WebVPN ホームページの [Web Bookmarks] タイトルまたはリンクをカスタマイズします。

application-access hide-details

WebVPN の [Application Access] ウィンドウに表示されるアプリケーション詳細を非表示にするには、カスタマイゼーション コンフィギュレーション モードで **application-access hide-details** コマンドを使用します。このモードには、**webvpn** コマンドまたは **tunnel-group webvpn-attributes** コマンドを使用してアクセスします。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

application-access hide-details {**enable** | **disable**}

no application-access [**hide-details** {**enable** | **disable**}]

構文の説明

disable	[Application Access] ウィンドウにアプリケーション詳細を表示します。
enable	[Application Access] ウィンドウのアプリケーション詳細を非表示にします。

デフォルト

デフォルトではディセーブルになっています。[Application Access] ウィンドウにアプリケーション詳細が表示されます。

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
カスタマイゼーション 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。

例

次に、アプリケーション詳細の表示をディセーブルにする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# application-access hide-details disable
```

関連コマンド

コマンド	説明
application-access	WebVPN ホームページの [Application Access] フィールドをカスタマイズします。
browse-networks	WebVPN ホームページの [Browse Networks] フィールドをカスタマイズします。
web-applications	WebVPN ホームページの [Web Application] フィールドをカスタマイズします。