g – h

gateway

特定のゲートウェイを管理しているコールエージェントのグループを指定するには、MGCP マップ コンフィギュレーション モードで **gateway** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

gateway *ip_address* [*group_id*]

構文の説明

gateway	特定のゲートウェイを管理するコール エージェント グループ。
group_id	コール エージェント グループの ID（0 ～ 2147483647）。
ip_address	ゲートウェイの IP アドレス。

コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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
MGCP マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
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

特定のゲートウェイを管理しているコール エージェントのグループを指定するには、**gateway** コマンドを使用します。>*ip_address* オプションを使用して、ゲートウェイの IP アドレスを指定します。>*group_id* オプションには 0 ～ 4294967295 の数字を指定します。この数字は、ゲートウェイを管理しているコールエージェントの >*group_id* に対応している必要があります。1 つのゲートウェイは 1 つのグループだけに所属できます。

例

次に、コール エージェント 10.10.11.5 および 10.10.11.6 にゲートウェイ 10.10.10.115 の制御を許可し、コール エージェント 10.10.11.7 および 10.10.11.8 にゲートウェイ 10.10.10.116 および 10.10.10.117 の制御を許可する例を示します。

```
ciscoasa(config)# mgcp-map mgcp_policy
ciscoasa(config-mgcp-map)# call-agent 10.10.11.5 101
```

```
ciscoasa(config-mgcp-map)# call-agent 10.10.11.6 101
ciscoasa(config-mgcp-map)# call-agent 10.10.11.7 102
ciscoasa(config-mgcp-map)# call-agent 10.10.11.8 102
ciscoasa(config-mgcp-map)# gateway 10.10.10.115 101
ciscoasa(config-mgcp-map)# gateway 10.10.10.116 102
ciscoasa(config-mgcp-map)# gateway 10.10.10.117 102
```

関連コマンド

コマンド	説明
debug mgcp	MGCP のデバッグ情報の表示をイネーブルにします。
mgcp-map	MGCP マップを定義し、MGCP マップ コンフィギュレーション モードをイネーブルにします。
show mgcp	MGCP のコンフィギュレーションおよびセッションの情報を表示します。

gateway-fqdn

ASA の FQDN を設定するには、**gateway-fqdn** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

gateway-fqdn value { **FQDN_Name** | **none** }
no gateway-fqdn

構文の説明

fqdn-name	ASA FQDN を定義して、AnyConnect クライアント にプッシュします。
none	FQDN をヌル値として指定して、FQDN が指定されないようにします。hostname コマンドおよび domain-name コマンドを使用して設定されたグローバル FQDN が使用されます（使用可能な場合）。

コマンド デフォルト

デフォルトFQDN名は、デフォルトのグループポリシーで設定されていません。新しいグループ ポリシーは、この値を継承するように設定されます。

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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
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

ASA 間にロード バランシングを設定した場合は、VPN セッションの再確立に使用される ASA IP アドレスを解決するために、ASA の FQDN を指定します。この設定は、さまざまな IP プロトコルのネットワーク間のクライアント ローミングをサポートするうえで重要です（IPv4 から IPv6 など）。

AnyConnect クライアント プロファイルにある ASA FQDN を使用してローミング後に ASA IP アドレスを取得することはできません。アドレスがロード バランシング シナリオの正しいデバイス（トンネルが確立されているデバイス）と一致しない場合があります。

ASA の FQDN がクライアントにプッシュされない場合、クライアントは、以前にトンネルが確立されている IP アドレスへの再接続を試みます。異なる IP プロトコル（IPv4 から IPv6）の

ネットワーク間のローミングをサポートするには、AnyConnect クライアント は、トンネルの再確立に使用する ASA アドレスを決定できるように、ローミング後にデバイス FQDN の名前解決を行う必要があります。クライアントは、初期接続中にプロファイルに存在する ASA FQDN を使用します。以後のセッション再接続では、使用可能な場合は常に、ASA によってプッシュされた（また、グループ ポリシーで管理者が設定した）デバイス FQDN を使用します。FQDN が設定されていない場合、ASA は、ASDM の [Device Setup] > [Device Name/Password and Domain Name] の設定内容からデバイス FQDN を取得（およびクライアントに送信）します。

デバイス FQDN が ASA によってプッシュされていない場合、クライアントは、異なる IP プロトコルのネットワーク間のローミング後に VPN セッションを再確立できません。

使用上のガイドライン

例

次に、ASA の FQDN を ASAName.example.cisco.com として定義する例を示します。

```
ciscoasa(config-group-policy)# gateway-fqdn value ASAName.example.cisco.com
ciscoasa(config-group-policy)#
```

次に、グループ ポリシーから ASA の FQDN を削除する例を示します。グループ ポリシーは、デフォルト グループ ポリシーからこの値を継承します。

```
ciscoasa(config-group-policy)# no gateway-fqdn
ciscoasa(config-group-policy)#
```

次に、FQDN を値なしとして定義する例を示します。ciscoasa コマンドおよび domain-name コマンドを使用して設定されたグローバル FQDN が使用されます（使用可能な場合）。

```
ciscoasa(config-group-policy)# gateway-fqdn none
ciscoasa(config-group-policy)#
```

graceful-restart

NSF 対応 ASA で OSPFv3 のグレースフル リスタートを設定するには、ルータ コンフィギュレーション モードで graceful-restart コマンドを使用します。必要に応じて、restart-interval オプションを使用してグレースフル リスタートの間隔を設定します。グレースフル リスター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。

graceful-restart [**restart-interval** *seconds*]
no graceful-restart

構文の説明

restart-interval seconds	（オプション）グレースフル リスタートの間隔を秒数で指定します。有効な範囲は 1 ～ 1800 です。デフォルトは 120 です。 （注） 30 秒未満の再起動間隔では、グレースフル リスタートが中断します。

コマンド デフォルト

OSPFv3 グレースフル リスタートはデフォルトでディセーブルです。

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。

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 コンフィギュレーション モード	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.3(1)	このコマンドが導入されました。

使用上のガイドライン

graceful-restart コマンドを使用し、OSPFv3 がプロセス再起動によりデータ フォワーディング パスに留まるようにします。

（注） ASA の一般的なリブート サイクルを許可するには、再起動間隔を十分長く設定します。ネットワークが古いルート情報に依存することを回避するために、再起動間隔を過度に長く設定しないでください。

例

次に、OSPFv3 のグレースフル リスタートをイネーブルにする例を示します。

```
ciscoasa
(config)# ipv6 router ospf 1
ciscoasa
(config-router)# graceful-restart restart-interval 180
```

関連コマンド

コマンド	説明
graceful-restart helper	NSF 認識 ASA で OSPFv3 グレースフル リスタートをイネーブルにします。

graceful-restart helper

NSF 対応の ASA で OSPFv3 のグレースフル リスタートを設定するには、graceful-restart を使用します。グレースフル リスター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。

graceful-restart helper [**strict-lsa-checking**]
no graceful-restart helper

構文の説明

strict-lsa-checking	（オプション）ヘルパー モードの厳密なリンクステート アドバタイズメント（LSA）をイネーブルにします。

コマンド デフォルト

OSPFv3 グレースフル リスタート ヘルパー モードは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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 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
9.3(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

ASA が NSF をイネーブルにしている場合、ASA は NSF 対応であると考えられ、グレースフル リスタート モードで動作します。OSPF プロセスは、ルート プロセッサ（RP）スイッチオーバーのため、ノンストップ フォワーディングの復帰を実行します。デフォルトでは、NSF 対応 ASA に隣接する ASA は NSF 認識となり、NSF ヘルパー モードで動作します。NSF 対応 ASA がグレースフル リスタートを実行しているときは、ヘルパーの ASA はそのノンストップ フォワーディングの復帰プロセスを支援します。再起動するネイバーのノンストップ フォワーディングの復帰を ASA が支援しないようにする場合は、no nsf ietf helper コマンドを入力します。

NSF 認識 ASA および NSF 対応 ASA の両方で厳密な LSA チェックをイネーブルにするには、graceful-restart helper strict-lsa-checking コマンドを入力します。ただし、グレースフル リスタート プロセス時に ASA がヘルパー ASA になるまでは厳密な LSA チェックは有効になりません。厳密な LSA チェックをイネーブルにすると、ヘルパー ASA は、LSA の変更があるために再起

動 ASA にフラッディングされる場合、または、グレースフル リスタート プロセスが開始されたときに再起動 ASA の再送リスト内の LSA に変更があると検出された場合、再起動 ASA のプロセスの支援を終了します。

例

次に、厳密な LSA チェックを行うグレースフル リスタート ヘルパーをイネーブルにする例を示します。

```
ciscoasa
(config)# ipv6 router ospf 1
ciscoasa
(config-router)# graceful-restart helper strict-lsa-checking
```

関連コマンド

コマンド	説明
graceful-restart	NSF 対応 ASA で OSPFv3 グレースフル リスタートをイネーブルにします。

group

AnyConnect IPSec 接続に対して IKEv2 セキュリティ アソシエーション（SA）の Diffie-Hellman グループを指定するには、ikev2 ポリシー コンフィギュレーション モードで group コマンドを使用します。コマンドを削除してデフォルト設定を使用するには、このコマンドの **no** 形式を使用します。

group { **1** | **2** | **5** | **14** | **19** | **20** | **21** | **24** }
no group { **1** | **2** | **5** | **14** | **19** | **20** | **21** | **24** }

構文の説明

1	768 ビット Diffie-Hellman グループ 1 を指定します（FIPS モードではサポートされません）。
2	1024 ビット Diffie-Hellman グループ 2 を指定します。
5	1536 ビット Diffie-Hellman グループ 5 を指定します。
14	ECDH グループを IKEv2 DH キー交換グループとして選択します。
19	ECDH グループを IKEv2 DH キー交換グループとして選択します。
20	ECDH グループを IKEv2 DH キー交換グループとして選択します。
21	ECDH グループを IKEv2 DH キー交換グループとして選択します。
24	ECDH グループを IKEv2 DH キー交換グループとして選択します。

コマンド デフォルト

デフォルトの Diffie-Hellman グループはグループ 14 です。

使用上のガイドライン

IKEv2 SA は、IKEv2 ピアがフェーズ 2 で安全に通信できるようにするためにフェーズ 1 で使用されるキーです。crypto ikev2 policy コマンドを入力すると、group コマンドを使用して SA の Diffie-Hellman グループを設定できます。ASA および AnyConnect クライアント は、グループ ID を使用して共有秘密を取得します。共有秘密は相互に転送されません。Diffie-Hellman グループ番号が小さいほど、実行に必要な CPU 時間も少なくなります。Diffie-Hellman グループ番号が大きいほど、セキュリティも高くなります。

AnyConnect クライアント が非 FIPS モードで動作している場合、ASA は Diffie-Hellman グループ 1、2、および 5 をサポートします。FIPS モードでは、サポート グループ 2 および 5 をサポートします。したがって、グループ 1 だけを使用するように ASA を設定する場合、FIPS モードの AnyConnect クライアント は接続に失敗します。

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。

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
ikev2 ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(1)	ECDH グループを IKEv2 DH キー交換グループとして選択する機能が追加されました。
9.13.(1)	デフォルト DH グループは **group 14.** です。**group 2**, **group 5** および **group 24** コマンドオプションは廃止され、以降のリリースで削除されます。

例

次に、ikev2 ポリシー コンフィギュレーション モードを開始して、Diffie-Hellman グループをグループ 5 に設定する例を示します。

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# group 5
ciscoasa(config-ikev2-policy) group 2(Deprecated)
ciscoasa(config-ikev2-policy) group 5(Deprecated)
ciscoasa(config-ikev2-policy) group 24(Deprecated)
ciscoasa(config-ikev2-policy) group 14
```

関連コマンド

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

group-alias

ユーザーがトンネルグループの参照に使用する1つ以上の変換名を作成するには、トンネルグループwebvpnコンフィギュレーションモードで**group-alias**コマンドを使用します。リストからエイリアスを削除するには、このコマンドの**no**形式を使用します。

group-alias name [**enable** | **disable**]
no group-alias *name*

構文の説明

disable	グループ エイリアスをディセーブルにします。
enable	以前ディセーブルにしたグループ エイリアスをイネーブルにします。
name	トンネル グループ エイリアスの名前を指定します。選択した任意のストリングを指定できます。ただし、スペースを含めることはできません。

コマンド デフォルト

デフォルトのグループ エイリアスはありませんが、グループ エイリアスを指定すると、そのエイリアスがデフォルトでイネーブルになります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	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
トンネル グループ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

指定したグループ エイリアスが、ログイン ページのドロップダウン リストに表示されます。各グループに複数のエイリアスを指定することも、エイリアスを指定しないことも可能です。このコマンドは、同じグループが「Devtest」や「QA」などの複数の一般名で知られている場合に役立ちます。

例

次に、「devtest」という名前のトンネル グループを設定し、そのグループに対してエイリアス「QA」および「Fra-QA」を確立するコマンドの例を示します。

```
ciscoasa(config)# tunnel-group devtest type webvpn
ciscoasa(config)# tunnel-group devtest webvpn-attributes
ciscoasa(config-tunnel-webvpn)# group-alias QA
ciscoasa(config-tunnel-webvpn)# group-alias Fra-QA
ciscoasa(config-tunnel-webvpn)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループ データベース全体または指定したトンネル グループ コンフィギュレーションをクリアします。
show webvpn group-alias	指定したトンネル グループまたはすべてのトンネル グループのエイリアスを表示します。
tunnel-group webvpn-attributes	WebVPN トンネル グループ属性を設定するためのトンネル グループ webvpn コンフィギュレーション モードを開始します。

group-delimiter

グループ名の解析をイネーブルにして、トンネルのネゴシエート時に受信したユーザー名からグループ名を解析する場合に使用するデリミタを指定するには、グローバル コンフィギュレーション モードで **group-delimiter** コマンドを使用します。このグループ名解析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。

group-delimiter*デリミタ*
no group-delimiter

構文の説明

delimiter	グループ名のデリミタとして使用する文字を指定します。有効な値は、**@**、**#**、および **!** です。

コマンド デフォルト

デフォルトで、デリミタは指定されていないため、グループ名解析はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

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

デリミタは、トンネルがネゴシエートされるときに、ユーザー名からトンネル グループ名を解析するために使用されます。デフォルトで、デリミタは指定されていないため、グループ名解析はディセーブルです。

例

次に、グループデリミタをハッシュマスク（#）に変更する **group-delimiter** コマンドの例を示します。

```
ciscoasa(config)# group-delimiter #
```

関連コマンド

コマンド	説明
clear configure group-delimiter	設定したグループ デリミタをクリアします。

コマンド	説明
show running-config group-delimiter	現在のグループ デリミタ値を表示します。
strip-group	グループ除去処理をイネーブルまたはディセーブルにします。

group-lock

リモートユーザーがトンネルグループを介してしかアクセスできないように制限するには、グループ ポリシー コンフィギュレーション モードまたはユーザー名コンフィギュレーション モードで **group-lock** コマンドを発行します。実行コンフィギュレーションから **group-lock** 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。

group-lock { **value** *tunnel-grp-name* | **none** }
no group-lock

構文の説明

none	group-lock をヌル値に設定します。これにより、グループ ロックの制限が許可されなくなります。デフォルトまたは指定したグループ ポリシーの group-lock 値を継承しないようにします。
value *tunnel-grp-name*	ユーザーが接続する際にASAによって要求される既存のトンネルグループの名前を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザー名コンフィギュレーション	• 対応	—	• 対応	—	—

使用上のガイドライン

グループロックをディセーブルにするには、**group-lock none** コマンドを使用します。**no group-lock** コマンドを使用すると、別のグループポリシーの値を継承できます。

グループロックは、仮想プライベートネットワーク（VPN）クライアントに設定されているグループが、ユーザーが割り当てられたトンネルグループと一致しているかどうかを確認することにより、ユーザーを制約します。一致していない場合、ASAはユーザーが接続できないようにします。グループロックを設定しない場合、ASA は、割り当てられたグループとは関係なく、ユーザーを認証します。

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、FirstGroup という名前のグループ ポリシーにグループ ロックを設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# group-lock value tunnel group name
```

group-object

オブジェクトグループにグループオブジェクトを追加するには、オブジェクトの設定時に **group-object** コマンドを使用します。グループオブジェクトを削除するには、このコマンドの **no** 形式を使用します。

group-object*obj_grp_name*
no group-object *obj_grp_name*

構文の説明

obj_grp_name	オブジェクト グループ（1 ～ 64 文字）を指定します。文字、数字、および「_」、「-」、「.」の組み合わせが使用可能です。

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		
	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
プロトコル、ネットワーク、サービス、ICMP タイプ、セキュリティ グループおよびユーザー オブジェクト グループの各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
7.0(1)	このコマンドが追加されました。
8.4(2)	オブジェクトグループ ユーザー コンフィギュレーション モードでオブジェクト グループを追加して、アイデンティティ ファイアウォール機能で使用できるようになりました。

使用上のガイドライン

group-object コマンドは、それ自身がオブジェクトグループであるオブジェクトを追加するために、**object-group** コマンドとともに使用します。このサブコマンドを使用すると、同じタイプのオブジェクトを論理グループ化して、構造化されたコンフィギュレーションの階層オブジェクト グループを構築できます。

オブジェクト グループ内でのオブジェクトの重複は、それらのオブジェクトがグループ オブジェクトの場合は許可されます。たとえば、オブジェクト 1 がグループ A とグループ B の両方に存在する場合、A と B の両方を含むグループ C を定義することができます。ただし、グループ階層を循環型にするグループ オブジェクトを含めることはできません。たとえば、グループ A にグループ B を含め、さらにグループ B にグループ A を含めることはできません。

階層オブジェクト グループは 10 レベルまで許可されています。

（注） ASA は、ネストされた IPv6 ネットワーク オブジェクト グループはサポートしません。したがって、IPv6 エントリが含まれるオブジェクトを別の IPv6 オブジェクト グループの下でグループ化することはできません。

例

次に、ホストを重複させる必要性を排除するために **group-object** コマンドを使用する方法の例を示します。

```
ciscoasa(config)# object-group network host_grp_1
ciscoasa(config-network)# network-object host 192.168.1.1
ciscoasa(config-network)# network-object host 192.168.1.2
ciscoasa(config-network)# exit
ciscoasa(config)# object-group network host_grp_2
ciscoasa(config-network)# network-object host 172.23.56.1
ciscoasa(config-network)# network-object host 172.23.56.2
ciscoasa(config-network)# exit
ciscoasa(config)# object-group network all_hosts
ciscoasa(config-network)# group-object host_grp_1
ciscoasa(config-network)# group-object host_grp_2
ciscoasa(config-network)# exit
ciscoasa(config)# access-list grp_1 permit tcp object-group host_grp_1 any eq ftp
ciscoasa(config)# access-list grp_2 permit tcp object-group host_grp_2 any eq smtp
ciscoasa(config)# access-list all permit tcp object-group all-hosts any eq w
```

次に、ローカルユーザーグループをユーザーグループオブジェクトに追加するために **group-object** コマンドを使用する方法の例を示します。

```
ciscoasa(config)# object-group user sampleuser1-group
ciscoasa(config-object-group user)# description group members of sampleuser1-group
ciscoasa(config-object-group user)# user-group EXAMPLE\\group.sampleusers-all
ciscoasa(config-object-group user)# user EXAMPLE\user2
ciscoasa(config-object-group user)# exit
ciscoasa(config)# object-group user sampleuser2-group
ciscoasa(config-object-group user)# description group members of sampleuser2-group
ciscoasa(config-object-group user)# group-object sampleuser1-group
ciscoasa(config-object-group user)# user-group EXAMPLE\\group.sampleusers-marketing
ciscoasa(config-object-group user)# user EXAMPLE\user3
```

関連コマンド

コマンド	説明
clear configure object-group	すべての **object-group** コマンドをコンフィギュレーションから削除します。
object-group	コンフィギュレーションを最適化するためのオブジェクト グループを定義します。
show running-config object-group	現在のオブジェクト グループを表示します。

group-policy

グループポリシーを作成または編集するには、グローバル コンフィギュレーション モードで **group-policy** コマンドを使用します。コンフィギュレーションからグループポリシーを削除するには、このコマンドの **no** 形式を使用します。

group-policy *name* { **internal** [**from** *group-policy_name*] | **external server-group** *server_group* **password** *server_password* }
no group-policy *name*

構文の説明

external server-group *server_group*	グループポリシーを外部として指定し、ASA が属性を照会する AAA サーバーグループを識別します。
from *group-policy_name*	この内部グループ ポリシーの属性を、既存のグループ ポリシーの値に初期化します。
internal	グループ ポリシーを内部として識別します。
name	グループ ポリシーの名前を指定します。この名前は最大 64 文字で、スペースを含めることができます。スペースを含むグループ名は、二重引用符で囲む必要があります（"Sales Group" など）。
password *server_password*	外部AAAサーバーグループから属性を取得する際に使用するパスワードを指定します。パスワードは最大 128 文字です。スペースを含めることはできません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

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

使用上のガイドライン

ASA には、DefaultGroupPolicy という名前のデフォルトグループポリシーが常に存在しています。ただし、このデフォルトグループポリシーは、これを使用するように ASA を設定しない限り、有効ではありません。設定の方法については、CLI コンフィギュレーション ガイドを参照してください。

group-policy attributes コマンドを使用してグループ ポリシー 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、グループポリシーのあらゆる属性と値のペアを設定できます。DefaultGroupPolicy には、次の属性と値のペアがあります。

属性	デフォルト値
backup-servers	keep-client-config
banner	なし
client-access-rules	なし
client-firewall	なし
default-domain	なし
dns-server	なし
group-lock	なし
ip-comp	disable
ip-phone-bypass	無効
ipsec-udp	無効
ipsec-udp-port	10000
leap-bypass	無効
nem	無効
password-storage	無効
pfs	disable
re-xauth	disable
secure-unit-authentication	無効
split-dns	なし
split-tunnel-network-list	なし
split-tunnel-policy	tunnelall
user-authentication	無効

属性	デフォルト値
user-authentication-idle-timeout	なし
vpn-access-hours	unrestricted
vpn-filter	なし
vpn-idle-timeout	30 分
vpn-session-timeout	なし
vpn-simultaneous-logins	3
vpn-tunnel-protocol	IPsec WebVPN
wins-server	なし

また、グループ ポリシー コンフィギュレーション モードで **webvpn** コマンドを入力するか **group-policy attributes** コマンドを入力してから、グループ webvpn コンフィギュレーション モードで **webvpn** コマンドを入力することで、グループポリシーの webvpn コンフィギュレーション モード属性を設定できます。詳細については、**group-policy attributes** コマンドの説明を参照してください。

例

次に、「FirstGroup」という名前の内部グループ ポリシーを作成する例を示します。

```
ciscoasa
(config)#
 group-policy FirstGroup internal
```

次に、AAA サーバー グループに「BostonAAA」、パスワードに「12345678」を指定し、「ExternalGroup」という名前の外部グループ ポリシーを作成する例を示します。

```
ciscoasa
(config)#
 group-policy ExternalGroup external server-group BostonAAA password 12345678
```

関連コマンド

コマンド	説明
clear configure group-policy	特定のグループポリシーまたはすべてのグループポリシーのコンフィギュレーションを削除します。
group-policy attributes	グループポリシー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、指定したグループポリシーの属性と値を設定したり、webvpnコンフィギュレーションモードを開始して、グループの WebVPN 属性を設定したりできます。
show running-config group-policy	特定のグループポリシーまたはすべてのグループポリシーの実行コンフィギュレーションを表示します。

コマンド	説明
webvpn	webvpn コンフィギュレーションモードを開始し、指定したグループの WebVPN 属性を設定できるようにします。

group-policy attributes

グループ ポリシーコンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで、**group-policy attributes** コマンドを使用します。グループポリシーからすべての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。

group-policy*name***attributes**
no group-policy *name* **attributes**

構文の説明

name	グループ ポリシーの名前を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

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

グループ ポリシー コンフィギュレーション モードでは、指定したグループ ポリシーの属性と値のペアを設定したり、グループ ポリシー webvpn コンフィギュレーション モードを開始してグループの WebVPN 属性を設定したりできます。

属性モードのコマンド構文には、一般的に、次のような特徴があります。

- **no** 形式は実行コンフィギュレーションから属性を削除し、別のグループポリシーからの値の継承をイネーブルにします。
- **none** キーワードは実行コンフィギュレーションの属性をヌル値に設定し、これによって継承を禁止します。
- ブール型属性には、イネーブルおよびディセーブルの設定用に明示的な構文があります。

ASA には、DefaultGroupPolicy という名前のデフォルトグループポリシーが常に存在しています。ただし、このデフォルトグループポリシーは、これを使用するように ASA を設定しない

限り、有効ではありません。設定の方法については、CLI コンフィギュレーション ガイドを参照してください。

group-policy attributes コマンドを使用してグループ ポリシー 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、グループポリシーのあらゆる属性と値のペアを設定できます。DefaultGroupPolicy には、次の属性と値のペアがあります。

属性	デフォルト値
backup-servers	keep-client-config
banner	なし
client-access-rule	なし
client-bypass-protocol	disable
client-firewall	なし
default-domain	なし
dns-server	なし
group-lock	なし
ip-comp	disable
ip-phone-bypass	無効
ipsec-udp	無効
ipsec-udp-port	10000
leap-bypass	無効
nem	無効
password-storage	無効
pfs	disable
re-xauth	disable
secure-unit-authentication	無効
split-dns	なし
split-tunnel-network-list	なし
split-tunnel-policy	tunnelall
user-authentication	無効
user-authentication-idle-timeout	なし

属性	デフォルト値
vpn-access-hours	unrestricted
vpn-filter	なし
vpn-idle-timeout	30 分
vpn-session-timeout	なし
vpn-simultaneous-logins	3
vpn-tunnel-protocol	IPsec WebVPN
wins-server	なし

また、**group-policy attributes** コマンドを入力してから、グループ ポリシー コンフィギュレーション モードで **webvpn** コマンドを入力することで、グループポリシーの webvpn モード属性を設定できます。詳細については、**webvpn** コマンド（グループポリシー属性モードおよびユーザー名属性モード）の説明を参照してください。

例

次に、FirstGroup という名前のグループ ポリシーのグループ ポリシー属性モードを開始する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)#
```

関連コマンド

コマンド	説明
clear configure group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーのコンフィギュレーションを削除します。
group-policy	グループ ポリシーを作成、編集、または削除します。
show running-config group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーの実行コンフィギュレーションを表示します。
webvpn	グループ webvpn コンフィギュレーション モードを開始し、指定したグループの WebVPN 属性を設定できるようにします。

group-prompt

WebVPN ユーザーが ASA に接続したときに表示される WebVPN ページログインボックスのグループプロンプトをカスタマイズするには、webvpn 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 **group-prompt** 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。

group-prompt { **text** | **style** } *value*
group-prompt { **text** | **style** } *value*

構文の説明

text	テキストへの変更を指定します。
style	スタイルへの変更を指定します。
value	実際に表示するテキスト、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）。

コマンド デフォルト

グループ プロンプトのデフォルト テキストは「GROUP:」です。

グループ プロンプトのデフォルト スタイルは、color:black;font-weight:bold;text-align:right 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		
	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
webvpn 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

style オプションは、任意の有効な 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 コンソーシアム（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。

ここでは、WebVPNページに対する変更で最もよく行われるページの配色を変更するための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 進数値で入力します。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、テキストを「Corporate Group:」に変更し、デフォルト スタイルのフォント ウェイトを bolder に変更する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# group-prompt text Corporate Group:
ciscoasa(config-webvpn-custom)# group-prompt style font-weight:bolder
```

関連コマンド

コマンド	説明
password-prompt	WebVPNページのパスワードプロンプトをカスタマイズします。
username-prompt	WebVPN ページのユーザー名プロンプトをカスタマイズします。

group-search-timeout

show ad-groups コマンドを使用して照会した Active Directory サーバーからの応答を待機する最大時間を指定するには、AAA サーバー ホスト コンフィギュレーション モードで **group-search-timeout** 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するには、**no** 形式を使用します。

group-search-timeout*seconds*
no group-search-timeout *seconds*

構文の説明

seconds	Active Directory サーバーからの応答を待機する時間（1 ～ 300 秒）。

コマンド デフォルト

デフォルトは 10 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	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
AAA サーバー 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
8.0(4)	このコマンドが追加されました。

使用上のガイドライン

show ad-groups コマンドは LDAP を使用している Active Directory サーバーにのみ適用され、Active Directory サーバーでリストされているグループが表示されます。**group-search-timeout** コマンドを使用して、サーバーからの応答を待機する時間を調整します。

例

次に、タイムアウトを 20 秒に設定する例を示します。

```
ciscoasa(config-aaa-server-host)#group-search-timeout 20
```

関連コマンド

コマンド	説明
ldap-group-base-dn	サーバーが、ダイナミック グループ ポリシーで使用されるグループの検索を開始する Active Directory 階層のレベルを指定します。

コマンド	説明
show ad-groups	Active Directory サーバー上でリストされるグループを表示します。

group-url

グループに対する着信 URL または IP アドレスを指定するには、トンネルグループ webvpn コンフィギュレーション モードで **group-url** コマンドを使用します。リストから URL を削除するには、このコマンドの **no** 形式を使用します。

group-url *url* [**enable** | **disable**]
no group-url *url*

構文の説明

disable	URL をディセーブルにしますが、リストからは削除しません。
enable	URL をイネーブルにします。
url	このトンネル グループの URL または IP アドレスを指定します。

コマンド デフォルト

デフォルトの URL または IP アドレスはありませんが、URL または IP アドレスを指定すると、これがデフォルトでイネーブルになります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	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
トンネル グループ 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

グループの URL または IP アドレスを指定すると、ユーザーがログイン時にグループを選択する必要がなくなります。ユーザーがログインすると、ASA はトンネル グループ ポリシー テーブル内でユーザーの着信 URL/アドレスを検索します。URL/アドレスが見つかり、さらにトンネルグループでこのコマンドがイネーブルになっている場合、ASA は関連するトンネルグループを自動的に選択して、ユーザー名およびパスワードフィールドだけをログインウィンドウでユーザーに表示します。これによりユーザー インターフェイスが簡素化され、グループ リストがユーザーに表示されなくなるという利点が追加されます。ユーザーに表示されるログインウィンドウでは、そのトンネルグループ用に設定されているカスタマイゼーションが使用されます。

URL/アドレスがディセーブルで、**group-alias** コマンドが設定されている場合は、グループのドロップダウン リストも表示され、ユーザーによる選択が必要になります。

1 つのグループに対して複数の URL/アドレスを設定する（または、1 つも設定しない）ことができます。URL/アドレスごとに個別にイネーブルまたはディセーブルに設定できます。指定した URL/アドレスごとに個別の **group-url** コマンドを使用する必要があります。HTTP または HTTPS プロトコルを含めて、URL/アドレス全体を指定する必要があります。

複数のグループに同じ URL/アドレスを関連付けることはできません。ASA では、URL/アドレスの一意性を検証してから、これをトンネル グループに対して受け入れます。

例

次に、「test」という名前の WebVPN トンネル グループを設定し、そのグループに対して 2 つのグループ URL「http://www.cisco.com」および「https://supplier.example.com」を確立するコマンドの例を示します。

```
ciscoasa(config)# tunnel-group test type webvpn
ciscoasa(config)# tunnel-group test webvpn-attributes
ciscoasa(config-tunnel-webvpn)# group-url http://www.cisco.com
ciscoasa(config-tunnel-webvpn)# group-url https://supplier.example.com
ciscoasa(config-tunnel-webvpn)#
```

次に、RadiusServer という名前のトンネル グループに対して、グループ URL、http://www.cisco.com および http://192.168.10.10 をイネーブルにする例を示します。

```
ciscoasa(config)# tunnel-group RadiusServer type webvpn
ciscoasa(config)# tunnel-group RadiusServer general-attributes
ciscoasa(config-tunnel-general)# authentication server-group RADIUS
ciscoasa(config-tunnel-general)# accounting-server-group RADIUS
ciscoasa(config-tunnel-general)# tunnel-group RadiusServer webvpn-attributes
ciscoasa(config-tunnel-webvpn)# group-alias "Cisco Remote Access" enable
ciscoasa(config-tunnel-webvpn)# group-url http://www.cisco.com
enable
ciscoasa(config-tunnel-webvpn)# group-url http://192.168.10.10
enable
ciscoasa(config-tunnel-webvpn)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループ データベース全体または指定したトンネル グループ コンフィギュレーションをクリアします。
show webvpn group-url	指定したトンネル グループまたはすべてのトンネル グループの URL を表示します。
tunnel-group webvpn-attributes	WebVPN トンネル グループ属性を設定する webvpn コンフィギュレーション モードを開始します。

gtp-u-header-check

GTP データパケットの内部ペイロードが有効な IP パケットであるかどうかを確認し、そうでない場合はドロップします。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 **gtp-u-header-check** コマンドを使用します。確認を無効にするには、このコマンドの **no** 形式を使用します。

gtp-u-header-check [**anti-spoofing** [**gtpv2-dhcp-bypass** | **gtpv2-dhcp-drop**]]
no gtp-u-header-check [**anti-spoofing** [**gtpv2-dhcp-bypass** | **gtpv2-dhcp-drop**]]

構文の説明

anti-spoofing	内部ペイロードの IP ヘッダー内のモバイル ユーザー IP アドレスが、セッション作成応答などの GTP 制御メッセージに割り当てられている IP アドレスと一致するかどうかを確認し、IP アドレスが一致しない場合は GTP-U メッセージをドロップします。このチェックでは、IPv4、IPv6、および IPv4v6 PDN タイプがサポートされています。 モバイル端末が DHCP を使用してそのアドレスを取得する場合、GTPv2 でのエンドユーザーの IP アドレスは 0.0.0.0（IPv4）または *prefix*::0（IPv6）になります。その場合、システムは内部パケットで検出した最初の IP アドレスを使用してエンドユーザー IP アドレスを更新します。**gtpv2-dhcp** キーワードを使用して、DHCP で取得したアドレスのデフォルトの動作を変更できます。
gtpv2-dhcp-bypass	0.0.0.0 または *prefix*::0 アドレスを更新しません。その代わりに、エンドユーザーの IP アドレスが 0.0.0.0 または *prefix*::0 の場合はパケットを許可します。IP アドレスの取得に DHCP を使用すると、このオプションはアンチスプーフィング チェックをバイパスします。
gtpv2-dhcp-drop	0.0.0.0 または *prefix*::0 アドレスを更新しません。その代わりに、エンドユーザーの IP アドレスが 0.0.0.0 または *prefix*::0 の場合はすべてのパケットをドロップします。このオプションは、IP アドレスの取得に DHCP を使用するユーザーへのアクセスを防ぎます。

コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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
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

このコマンドを使用して、アンチスプーフィングを実装できます。GTP-C を通じて割り当てたものではない別の IP アドレスを使用してハッカーが別の顧客であるように装う（スプーフィング）可能性があります。アンチスプーフィングは、使用されている GTP-U アドレスが実際に GTP-C を使用して割り当てたものであるかどうかを確認します。

例

次に、デフォルトの動作でアンチスプーフィングを有効にする例を示します。

```
ciscoasa(config)# policy-map type inspect gtp gtp-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# gtp-u-header-check anti-spoofing
```

関連コマンド

コマンド	説明
anti-replay	GTP インスペクションで GTP アンチリプレイを有効にします。
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。

h245-tunnel-block

H.323 で H.245 トンネリングをブロックするには、パラメータ コンフィギュレーション モードで **h245-tunnel-block** 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。

h245-tunnel-block action [**drop-connection** | **log**]
no h245-tunnel-block action [**drop-connection** | **log**]

構文の説明

drop-connection	H.245 トンネルが検出された場合、コール設定接続をドロップします。
log	H.245 トンネルが検出された場合、ログを発行します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	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
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
7.2(1)	このコマンドが追加されました。

例

次に、H.323 コールで H.245 トンネリングをブロックする例を示します。

```
ciscoasa(config)# policy-map type inspect h323 h323_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# h245-tunnel-block action drop-connection
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。

コマンド	説明
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

hardware-bypass

Cisco ISA 3000 のハードウェアバイパスをイネーブルにし、停電時もインターフェイスペア間のトラフィックフローを続行させるには、グローバル コンフィギュレーション モードで **hardware-bypass** コマンドを使用します。ハードウェアバイパス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。

hardware-bypass GigabitEthernet { **1/1-1/2** | **1/3-1/4** } [**sticky**]
no hardware-bypass GigabitEthernet { **1/1-1/2** | **1/3-1/4** } [**sticky**]

（注） この機能は、Cisco ISA 3000 アプライアンスのみで使用できます。

構文の説明

GigabitEthernet {**1/1-1/2** | **1/3-1/4**}	サポートされているインターフェイス ペアは、銅線 GigabitEthernet 1/1 と 1/2 および GigabitEthernet 1/3 と 1/4 です。光ファイバ イーサネット モデルがある場合は、銅線イーサネット ペア（GigabitEthernet 1/1 および 1/2）のみがハードウェア バイパスをサポートします。このコマンドは、ペアごとに別々に入力します。
sticky	（任意）電源が回復し、アプライアンスが起動した後は、アプライアンスをハードウェア バイパス モードに保ちます。この場合、**no hardware-bypass manual** コマンドを使用する準備が整った時点でハードウェアバイパスを手動でオフにする必要があります。このオプションを使用すると、短時間の割り込みがいつ発生するかを制御できます。

コマンド デフォルト

ハードウェア バイパスは、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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	—	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.4(1.225)	このコマンドが追加されました。

使用上のガイドライン

ハードウェア バイパスがアクティブな場合はファイアウォール機能が設定されていません。したがって、トラフィックの通過を許可しているリスクをご自身が理解していることを確認してください。ハードウェア バイパスを非アクティブ化すると、ASA がフローを引き継ぐため、接続が短時間中断されます。

（注） ISA 3000 への電源が切断され、ハードウェア バイパス モードに移行すると、通信できるのは上記のインターフェイス ペアのみになります。つまり、デフォルトの設定を使用している場合は、inside1 <---> inside2 および outside1 <---> outside2 は通信できなくなります。これらのインターフェイス間の既存の接続がすべて失われます。

例

次に、GigabitEthernet 1/1 および 1/2 のハードウェア バイパスをディセーブルにし、1/3 および 1/4 をイネーブルにする例を示します。

```
ciscoasa(config)# no hardware-bypass GigabitEthernet 1/1-1/2
ciscoasa(config)# hardware-bypass GigabitEthernet 1/3-1/4
```

関連コマンド

コマンド	説明
hardware-bypass boot-delay	ハードウェア バイパスを設定して、ASA FirePOWER が起動するまでアクティブに維持します。
hardware-bypass manual	手動でハードウェア バイパスをアクティブまたは非アクティブにします。

hardware-bypass boot-delay

Cisco ISA 3000 にハードウェアバイパスを設定し、ASA Firepower モジュールが起動するまでアクティブに維持するには、グローバル コンフィギュレーション モードで **hardware-bypass boot-delay** コマンドを使用します。ブート遅延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。

hardware-bypass boot-delay module-up sfr
no hardware-bypass boot-delay module-up sfr

（注） この機能は、Cisco ISA 3000 アプライアンスのみで使用できます。

構文の説明

module-up sfr	ASA FirePOWER が起動するまでハードウェア バイパスをディセーブルにするのを遅延します。

コマンド デフォルト

ブート遅延はデフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	—	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.4(1.225)	このコマンドが追加されました。

使用上のガイドライン

hardware-bypass boot-delay コマンドが動作するようにするには、**sticky** オプションを設定せずに **hardware-bypass** コマンドを使用してハードウェアバイパスをイネーブルにする必要があります。**hardware-bypass boot-delay** コマンドを使用しないと、ASA FirePOWER モジュールが起動を完了する前にハードウェアバイパスが非アクティブになる可能性があります。たとえば、モジュールをフェールクローズに設定していた場合、このような状況では、トラフィックがドロップされる可能性があります。

例

次に、（**sticky** オプションを設定せずに）ハードウェアバイパスをイネーブルにし、ブート遅延をイネーブルにする例を示します。

```
ciscoasa(config)# hardware-bypass GigabitEthernet 1/1-1/2
ciscoasa(config)# hardware-bypass GigabitEthernet 1/3-1/4
ciscoasa(config)# hardware-bypass boot-delay module-up sfr
```

関連コマンド

コマンド	説明
hardware-bypass	サポートされているインターフェイス ペアのハードウェア バイパスを設定します。
hardware-bypass manual	手動でハードウェア バイパスをアクティブまたは非アクティブにします。

hardware-bypass manual

Cisco ISA 3000 でハードウェアバイパスを手動でアクティブまたは非アクティブにするには、特権 EXEC モードで **hardware-bypass manual** コマンドを使用します

hardware-bypass manual GigabitEthernet { **1/1-1/2** | **1/3-1/4** }
no hardware-bypass manual GigabitEthernet { **1/1-1/2** | **1/3-1/4** }

（注） この機能は、Cisco ISA 3000 アプライアンスのみで使用できます。

構文の説明

GigabitEthernet {**1/1-1/2** | **1/3-1/4**}	サポートされているインターフェイス ペアは、銅線 GigabitEthernet 1/1 と 1/2 および GigabitEthernet 1/3 と 1/4 です。光ファイバ イーサネット モデルがある場合は、銅線イーサネット ペア（GigabitEthernet 1/1 および 1/2）のみがハードウェア バイパスをサポートします。このコマンドは、ペアごとに別々に入力します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	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
特権 EXEC	—	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.4(1.225)	このコマンドが追加されました。

使用上のガイドライン

hardware-bypass コマンドの **sticky** オプションを設定してバイパスをイネーブルに維持する場合は、 **hardware-bypass manual** コマンドを使用して電源回復後にハードウェアバイパスを非アクティブ化する必要があります。

このコマンドによって、現在のハードウェア バイパスの状態が変更されます。電源障害が発生した場合は、**hardware-bypass** コンフィギュレーション コマンドのアクションが優先されます。たとえば、**hardware-bypass** がディセーブルに設定されている場合にハードウェアバイパスを手動でイネーブルにした後で電源障害が発生したときは、ハードウェアバイパスは設定に従ってディセーブルになります。

例

次に、手動で GigabitEthernet 1/2 および 1/2 のハードウェア バイパスを非アクティブ化する例を示します。

```
ciscoasa# no hardware-bypass manual GigabitEthernet 1/1-1/2
```

関連コマンド

コマンド	説明
hardware-bypass	サポートされているインターフェイス ペアのハードウェア バイパスを設定します。
hardware-bypass boot-delay	ハードウェア バイパスを設定して、ASA FirePOWER が起動するまでアクティブに維持します。

health-check

クラスタのヘルスチェック機能をイネーブルにするには、クラスタ グループ コンフィギュレーション モードで **health-check** コマンドを使用します。ヘルスチェック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。

health-check ［ **holdtime** *timeout* ］ ［ **vss-enabled** ］
no health-check ［ **holdtime** *timeout* ］ ［ **vss-enabled** ］

構文の説明

holdtime *timeout*	キープアライブまたはインターフェイス ステータス メッセージの間隔を 3 ～ 45 秒（9.8(1) 以降）または 8 ～ 45 秒（9.7 以前）の間で決定します。デフォルトは 3 秒です。低い保留時間を設定すると、CCL メッセージングおよび CPU アクティビティが向上します。保留時間を .3 ～ .7 に設定した後に ASA ソフトウェアをダウングレードした場合、新しい設定がサポートされていないので、この設定はデフォルトの 3 秒に戻ります。
vss-enabled	EtherChannel としてクラスタ制御リンクを設定し（推奨）、VSS または vPC ペアに接続している場合、**vss-enabled** オプションをイネーブルにする必要がある場合があります。一部のスイッチでは、VSS/vPC の 1 つのユニットがシャット ダウンまたは起動すると、そのスイッチに接続された EtherChannel メンバー インターフェイスが ASA に対してアップ状態であるように見えますが、これらのインターフェイスはスイッチ側のトラフィックを通していません。ASA holdtime timeout を低い値（0.8 秒など）に設定した場合、ASA が誤ってクラスタから削除される可能性があり、ASA はキープアライブ メッセージをこれらのいずれかの EtherChannel インターフェイスに送信します。**vss-enabled** をイネーブルにすると、ASA はクラスタ制御リンクのすべての EtherChannel インターフェイスでキープアライブメッセージをフラッディングして、少なくとも 1 台のスイッチがそれを受信できることを確認します。

コマンド デフォルト

デフォルトでは、ヘルス チェックがイネーブルで、holdtime が 3 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	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
クラスタ グループ コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。
9.1(4)	**vss-enabled** キーワードが追加されました。
9.8(1)	**holdtime** の最小値が 3 秒に下がりました。

使用上のガイドライン

何らかのトポロジ変更（たとえばデータ インターフェイスの追加/削除、ASA、またはスイッチ上のインターフェイスの有効化/無効化、VSS または vPC を形成するスイッチの追加）を行うときには、ヘルス チェック機能を無効にし、無効化したインターフェイスのモニタリングも無効にしてください（**no health-check monitor-interface**）。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、ヘルス チェック機能を再度イネーブルにできます。

メンバー間のキープアライブ メッセージによって、メンバーのヘルス状態が特定されます。ユニットが holdtime 期間内にピア ユニットからキープアライブ メッセージを受信しない場合は、そのピア ユニットは応答不能またはデッド状態と見なされます。

（注） 9.8(1) では、ユニット ヘルス チェック メッセージング スキームが、コントロール プレーンのキープアライブからデータ プレーンのハートビートに変更されました。データ プレーンを使用しると、CPU の使用率および信頼性が向上します。

このコマンドは、ブートストラップ コンフィギュレーションの一部ではなく、マスター ユニットからスレーブ ユニットに複製されます。

例

次に、ヘルス チェックをディセーブルにする例を示します。

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# no health-check
```

関連コマンド

コマンド	説明
clacp system-mac	スパンド EtherChannel を使用するときは、ASA は cLACP を使用してネイバースイッチとの間で EtherChannel のネゴシエーションを行います。
cluster group	クラスタに名前を付け、クラスタ コンフィギュレーション モードを開始します。
cluster-interface	クラスタ制御リンク インターフェイスを指定します。
cluster interface-mode	クラスタ インターフェイス モードを設定します。

コマンド	説明
conn-rebalance	接続の再分散をイネーブルにします。
console-replicate	スレーブユニットからマスターユニットへのコンソール複製をイネーブルにします。
enable (cluster group)	クラスタリングをイネーブルにします。
health-check auto-rejoin	ヘルスチェック失敗後の自動再結合クラスタ設定をカスタマイズします。
health-check	クラスタのヘルスチェック機能（ユニットのヘルスモニタリングおよびインターフェイスのヘルスモニタリングを含む）をイネーブルにします。
key	クラスタ制御リンクの制御トラフィックの認証キーを設定します。
local-unit	クラスタ メンバーに名前を付けます。
mtu cluster-interface	クラスタ制御リンク インターフェイスの最大伝送ユニットを指定します。
priority (cluster group)	マスター ユニット選定のこのユニットのプライオリティを設定します。

health-check application

クラウド Web セキュリティのアプリケーション健全性チェックをイネーブルにするには、ScanSafe 汎用オプション コンフィギュレーション モードで **health-check application** コマンドを使用します。健全性チェックを削除するか、デフォルトタイムアウトに戻すには、このコマンドの **no** 形式を使用します。

health-check application { [**url** *url_string*] | **timeout** *seconds* }
no health-check application { [**url** *url_string*] | **timeout** *seconds* }

構文の説明

url *url_string*	（任意）アプリケーションをポーリングするときに使用する URL を指定します。URL を指定しない場合は、デフォルトの URL が使用されます。デフォルトの URL は http://gs.scansafe.net/goldStandard?type=text&size=10 です。 URL は、Cisco クラウド Web セキュリティによって指示された場合にのみ指定します。
timeout *seconds*	ASA が健全性チェック URL の GET リクエストを送信してから応答を待機する時間を指定します。ASA は、タイムアウト後にサーバーのポーリングに対する再試行制限まで要求を再試行します。その後、サーバーがダウンして、フェールオーバーが開始します。デフォルトは 15 秒で、範囲は 5 ～ 120 秒です。

コマンド デフォルト

健全性チェックは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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
scansafe 汎用オプション 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)	このコマンドが追加されました。

使用上のガイドライン

Cisco Cloud Web Security サービスに登録すると、プライマリ Cloud Web Security プロキシ サーバーとバックアップ プロキシ サーバーが割り当てられます。これらのサーバーは、アベイラ

ビリティをチェックするために定期的にポーリングされます。ASA がクラウド Web セキュリティ プロキシ サーバーに到達することができない場合（SYN/ACK パケットがプロキシサーバーから到着しない場合など）、プロキシサーバーは TCP スリーウェイハンドシェイクを介してポーリングされて、アベイラビリティがチェックされます。設定した試行回数（デフォルトは 5）後に、プロキシ サーバーが使用不可の場合、サーバーは到達不能として宣言され、バックアップ プロキシ サーバーがアクティブになります。

クラウド Web セキュリティ アプリケーションの状態をチェックすることで、フェールオーバーをさらに改善することができます。場合によっては、サーバーが TCP スリーウェイ ハンドシェイクを完了できても、サーバー上のクラウド Web セキュリティ アプリケーションが正しく機能していないことがあります。アプリケーション健全性チェックを有効にすると、スリーウェイ ハンドシェイクが完了しても、アプリケーション自体が応答しない場合、システムはバックアップ サーバーにフェールオーバーできます。これにより、より信頼性の高いフェールオーバー設定が確立されます。この追加のチェックを有効にするには、**health-check application** コマンドを使用します。

ヘルス チェックでは、クラウド Web セキュリティ アプリケーションにテストの URL を使用して GET リクエストが送信されます。設定されているタイムアウト期限とリトライ限度内で応答に失敗すると、サーバーはダウンとしてマーキングされ、システムはフェールオーバーを開始します。バックアップ サーバーもまた、アクティブ サーバーとしてマーキングされる前に、正しく機能していることを確認するためにテストされます。フェールオーバーの後、プライマリ サーバーのアプリケーションは、オンラインに戻り再度アクティブ サーバーとしてマーキングされるまで 30 秒ごとに再テストされます。

継続ポーリングによってプライマリサーバーが連続する 2 回の再試行回数の期間にアクティブであることが示されると、ASA はバックアップサーバーからプライマリクラウド Web セキュリティ プロキシ サーバーに自動的にフォールバックします。このポーリング間隔を変更するには、 **retry-count** コマンドを使用します。

例

次に、プライマリ サーバーとバックアップ サーバーを設定し、デフォルトの URL とタイムアウトを使用して健全性チェックをイネーブルにする例を示します。健全性チェックをイネーブルにし、デフォルト以外のタイムアウトを設定するには、**health-check application** コマンドを別個に入力する必要があります。

```
scansafe general-options
 server primary ip 10.24.0.62 port 8080
 server backup ip 10.10.0.7 port 8080
 health-check application
 retry-count 7
 license 366C1D3F5CE67D33D3E9ACEC265261E5
```

関連コマンド

コマンド	説明
class-map type inspect scansafe	ホワイトリストに記載されたユーザーとグループのインスペクション クラス マップを作成します。
default user group	ASA に入ってくるユーザーのアイデンティティを ASA が判別できない場合のデフォルトのユーザー名やグループを指定します。

コマンド	説明
http[**s**]（パラメータ）	インスペクション ポリシー マップのサービス タイプ（HTTP または HTTPS）を指定します。
inspect scansafe	このクラスのトラフィックに対するクラウド Web セキュリティ インスペクションをイネーブルにします。
license	要求の送信元の組織を示すため、ASA がクラウド Web セキュリティ プロキシ サーバーに送信する認証キーを設定します。
match user group	ユーザーまたはグループをホワイトリストと照合します。
policy-map type inspect scansafe	インスペクション ポリシー マップを作成すると、ルールのために必要なパラメータを設定し、任意でホワイトリストを識別できます。
retry-count	再試行回数値を入力します。この値は、可用性をチェックするために、クラウド Web セキュリティプロキシサーバーをポーリングする前に ASA が待機する時間です。
scansafe	マルチ コンテキスト モードでは、コンテキストごとにクラウド Web セキュリティを許可します。
scansafe general-options	汎用クラウド Web セキュリティ サーバー オプションを設定します。
server {**primary** | **backup**}	プライマリまたはバックアップのクラウド Web セキュリティ プロキシ サーバーの完全修飾ドメイン名または IP アドレスを設定します。
show conn scansafe	大文字の Z フラグに示されたようにすべてのクラウド Web セキュリティ接続を表示します。
show scansafe server	サーバーが現在のアクティブ サーバー、バックアップ サーバー、または到達不能のいずれであるか、サーバーのステータスを表示します。
show scansafe statistics	合計と現在の HTTP 接続を表示します。
user-identity monitor	AD エージェントから指定したユーザーまたはグループ情報をダウンロードします。
whitelist	トラフィックのクラスでホワイトリスト アクションを実行します。

health-check auto-rejoin

ヘルスチェック失敗後の自動再結合クラスタ設定をカスタマイズするには、クラスタ グループ コンフィギュレーション モードで **health-check auto-rejoin** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

health-check { **data-interface** | **cluster-interface** | **system** } **auto-rejoin** { **unlimited** | *auto_rejoin_max* } [*auto_rejoin_interval* [*auto_rejoin_interval_variation*]]
no health-check { **data-interface** | **cluster-interface** | **system** } **auto-rejoin** [{ **unlimited** | *auto_rejoin_max* } [*auto_rejoin_interval* [*auto_rejoin_interval_variation*]]]

構文の説明

auto_rejoin_interval	（任意）再結合試行の間隔を 2 ～ 60 分の範囲で定義します。デフォルト値は**5**分です。クラスタへの再結合をユニットが試行する最大合計時間は、最後の失敗から 14,400 分に限られています。
auto_rejoin_interval_variation	（任意）間隔を長くするかを 1 ～ 3 の範囲で定義します。 • **1**：変更なし • **2**：2 x 以前の時間 • **3**：3 x 以前の時間。 たとえば、間隔を 5 分に設定し、変分を **2** に設定した場合は、最初の試行が 5 分後、2 回目の試行が 10 分後（2 x 5）、3 階目の試行が 20 分後（2 x 10）となります。デフォルト値は、クラスタインターフェイスの場合は**1**、データインターフェイスおよびシステムの場合は **2** です。
auto_rejoin_max	クラスタ再結合時の試行回数を 0 ～ 65535 で定義します。 **0** では自動再結合がディセーブルになります。デフォルト値は、クラスタインターフェイスの場合は **unlimited**、データインターフェイスおよびシステムの場合は **3** です。
cluster-interface	クラスタ制御リンクの自動再結合の設定を行います。
data-interface	データ インターフェイスの自動再結合の設定を行います。
system	システムにおける内部エラー時の自動再結合の設定を行います。内部の障害には、アプリケーション同期のタイムアウト、矛盾したアプリケーション ステータスなどがあります。
unlimited	クラスタの再結合の試行回数を、クラスタ インターフェイスのデフォルト値である unlimited に設定します。

コマンド デフォルト

• 失敗したクラスタ制御リンクのクラスタ再結合機能が 5 分おきに無制限に試行されます。

- 失敗したデータインターフェイスのクラスタ自動再結合機能は、5 分後と、2 に設定された増加間隔で合計で 3 回試行されます。
- 内部システム エラーの場合のクラスタ自動再結合機能は、5 分後と、2 に設定された増加間隔で、合計で 3 回試行されます。

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。

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
クラスタ グループ コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.9(2)	**system**キーワードが追加されました。
9.5(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、ネットワークの状態に合うように自動再結合オプションをカスタマイズできます。

例

次に、両方のインターフェイス タイプについて10回の試行を設定する例を示します。データ インターフェイスについては再結合間隔を10分、間隔の延長は3倍に設定し、クラスタ制御リンクについては再結合間隔を 7 分、間隔の延長は 2 倍に設定します。

```
ciscoasa(config)# cluster group pod1
ciscoasa(cfg-cluster)# local-unit unit1
ciscoasa(cfg-cluster)# cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
ciscoasa(cfg-cluster)# site-id 1
ciscoasa(cfg-cluster)# health-check data-interface auto-rejoin 10 10 3
ciscoasa(cfg-cluster)# health-check cluster-interface auto-rejoin 10 7 2
ciscoasa(cfg-cluster)# priority 1
ciscoasa(cfg-cluster)# key chuntheunavoidable
ciscoasa(cfg-cluster)# enable noconfirm
```

関連コマンド

コマンド	説明
clacp system-mac	スパンド EtherChannel を使用するときは、ASA は cLACP を使用してネイバースイッチとの間で EtherChannel のネゴシエーションを行います。

コマンド	説明
cluster group	クラスタに名前を付け、クラスタ コンフィギュレーション モードを開始します。
cluster-interface	クラスタ制御リンク インターフェイスを指定します。
cluster interface-mode	クラスタ インターフェイス モードを設定します。
conn-rebalance	接続の再分散をイネーブルにします。
console-replicate	スレーブユニットからマスターユニットへのコンソール複製をイネーブルにします。
enable (cluster group)	クラスタリングをイネーブルにします。
health-check	クラスタのヘルスチェック機能（ユニットのヘルスモニタリングおよびインターフェイスのヘルス モニタリングを含む）をイネーブルにします。
key	クラスタ制御リンクの制御トラフィックの認証キーを設定します。
local-unit	クラスタ メンバーに名前を付けます。
mac-address site-id	各サイトのサイト固有の MAC アドレスを設定します。
mtu cluster-interface	クラスタ制御リンク インターフェイスの最大伝送ユニットを指定します。
priority (cluster group)	マスター ユニット選定のこのユニットのプライオリティを設定します。
site-id	サイト ID を設定して、サイト間クラスタリングでの MAC アドレスのフラッピングを回避します。

health-check monitor-interface

インターフェイスをモニターするには、クラスタ グループ コンフィギュレーション モードで **health-check monitor-interface** コマンドを使用します。モニタリングを無効にするには、このコマンドの **no** 形式を使用します。

health-check monitor-interface { *interface_id* | **service-module** | **service-application** | **debounce-time** }
no health-check monitor-interface { *interface_id* | **service-module** | **service-application** | **debounce-time** }

構文の説明

interface_id	インターフェイスのモニタリングを有効にします。ポートチャネルIDと冗長 ID、または単一の物理インターフェイス ID を指定できます。ヘルス モニタリングは VLAN サブインターフェイス、または VNI や BVI などの仮想インターフェイスでは実行されません。クラスタ制御リンクのモニタリングは設定できません。このリンクは常にモニターされています。
service-application	Firepower 4100/9300 でデコレータアプリケーションのモニタリングを有効にします。
service-module	ASA ハードウェアモデルのソフトウェアまたはハードウェアモジュール（ASA FirePOWER モジュールなど）のモニタリングを有効にします。
debounce-time	障害が発生したインターフェイスをASAが削除するまでのデバウンス時間を設定します。デバウンス時間は300～9000 msの範囲の値を設定します。デフォルトは500 msです。値を小さくすると、インターフェイスの障害をより迅速に検出できます。デバウンス時間を短くすると、誤検出の可能性が高くなることに注意してください。インターフェイスのステータス更新が発生すると、ASAはインターフェイスを削除するまでに指定されたミリ秒数待機します。EtherChannel がダウン状態からアップ状態に移行する場合（スイッチがリロードされた、スイッチで EtherChannel が有効になったなど）、デバウンス時間がより長くなり、ポートのバンドルにおいて別のクラスタ ユニットの方が高速なため、クラスタ ユニットでインターフェイスの障害が表示されることを妨げることがあります。

コマンド デフォルト

デフォルトでは、すべてのインターフェイスでインターネット ヘルス モニタリングがイネーブルになっています。

デバウンス時間は 500 ms 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		
	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
クラスタ グループ コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。
9.5(1)	**service-module** キーワードが追加されました。
9.6(1)	**service-application** キーワードが追加されました。
9.8(1)	Firepower 4100/9300 に **debounce-time** キーワードが追加されました。
9.9(2)	ASA アプライアンスに **debounce-time** キーワードが追加されました。
9.10(1)	**debounce-time** キーワードは、ダウン状態から稼働状態に変更するインターフェイスに適用されるようになりました。

使用上のガイドライン

何らかのトポロジ変更（データインターフェイスの追加/削除、ASA またはスイッチ上のインターフェイスの有効化/無効化、VSS または vPC を形成するスイッチの追加など）の実行時には、ヘルスチェック機能（**no health-check**）を無効にし、無効化したインターフェイスのインターフェイス モニタリングも無効にする必要があります（**no health-check monitor-interface**）。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、ヘルス チェック機能を再度イネーブルにできます。

インターフェイス ステータス メッセージによって、リンク障害が検出されます。あるインターフェイスが、特定のユニット上では障害が発生したが、別のユニットではアクティブの場合は、そのユニットはクラスタから削除されます。

ユニットがホールド時間内にインターフェイス ステータス メッセージを受信しない場合に、ASA がメンバをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのユニットが確立済みメンバであるか、またはクラスタに参加しようとしているかによって異なります。EtherChannel の場合（スパニングかどうかを問わない）は、確立済みメンバーのインターフェイスがダウン状態のときに、ASA はそのメンバーを 9 秒後に削除します。ユニットが新しいメンバーとしてクラスタに参加しようとしているときは、ASA は 45 秒待機してからその新しいユニットを拒否します。非 EtherChannel の場合は、メンバー状態に関係なく、ユニットは 500 ミリ秒後に削除されます。

このコマンドは、ブートストラップ コンフィギュレーションの一部ではなく、マスター ユニットからスレーブ ユニットに複製されます。

例

次に、ヘルス チェックをディセーブルにする例を示します。

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# no health-check monitor-interface ethernet1/1
```

関連コマンド

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

hello-interval

インターフェイス上で送信されるEIGRPhelloパケット間の間隔を指定するには、インターフェイス コンフィギュレーション モードで **hello-interval** コマンドを使用します。hello 間隔をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

hello-interval eigrp *as-number seconds*
no hello-interval eigrp *as-number seconds*

構文の説明

as-number	EIGRP ルーティング プロセスの自律システム番号を指定します。
seconds	インターフェイス上で送信される hello パケット間の間隔を指定します。有効な値は、1 ～ 65535 秒です。

コマンド デフォルト

デフォルトは 5 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	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
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
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

hello間隔を小さくするほど、トポロジの変更が速く検出されますが、より多くのルーティングトラフィックが発生します。この値は、特定のネットワーク上のすべてのルータおよびアクセス サーバーで同じにする必要があります。

例

次の例では、EIGRP hello 間隔を 10 秒に、ホールド タイムを 30 秒に設定します。

```
ciscoasa(config-if)# hello-interval eigrp 100 10
ciscoasa(config-if)# hold-time eigrp 100 30
```

関連コマンド

コマンド	説明
hold-time	hello パケットでアドバタイズされる EIGRP ホールドタイムを設定します。

hello padding multi-point

ルータ レベルで IS-IS hello パディングを再度イネーブルにするには、ルータ ISIS コンフィギュレーション モードで、**hello padding multi-point** コマンドを入力します。IS-IS hello パディング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。

hello padding multi-point
no hello padding multi-point

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

hello パディングは、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。

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 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

このコマンドを使用すると、最大伝送ユニット（MTU）サイズになるまで IS-IS hello をパディングできます。IS-IS hello をフル MTU に埋め込む利点は、大きなフレームに関連した送信問題によるエラーや隣接インターフェイスの MTU 不一致によるエラーを検出できることです。

両方のインターフェイスの MTU が同じである場合やトランスレーショナル ブリッジングの場合には、ネットワーク帯域幅の無駄を省くため、hello パディングをディセーブルにできます。hello パディングがディセーブルになっても、ASA は、MTU 不一致検出の利点を維持するために、最初の 5 回の IS-IS hello を最大 MTU にパディングして送信します。

IS-IS ルーティングプロセスに関して、ASA 上のすべてのインターフェイスの hello パディングをディセーブルにするには、ルータ コンフィギュレーション モードで **no hello padding multi-point** コマンドを入力します。特定のインターフェイスの hello パディングを選択的にディセーブルにするには、インターフェイス コンフィギュレーション モードで **no isis hello padding** コマンドを入力します。

例

次に、**no hello padding multi-point** コマンドを使用して、ルータレベルの Hello パディングをオフにする例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# hello padding multi-point
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
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。

コマンド	説明
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
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。

コマンド	説明
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。
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。

コマンド	説明
summary-address	IS-IS の集約アドレスを作成します。

help

指定するコマンドのヘルプ情報を表示するには、ユーザー EXEC モードで **help** コマンドを使用します。

help { *command* | **?** }

構文の説明

?	現在の特権レベルおよびモードで使用可能なすべてのコマンドを表示します。
command	CLI ヘルプを表示するコマンドを指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	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
ユーザー EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

help コマンドを使用すると、すべてのコマンドのヘルプ情報が表示されます。**help** コマンドの後にコマンド名を入力することによって、個々のコマンドのヘルプを参照できます。コマンド名を指定しないで、代わりに **?** を入力すると、現在の特権レベルおよびモードで使用可能なすべてのコマンドが表示されます。

pager コマンドがイネーブルの場合、24 行表示されると、リスト表示が一時停止して次のプロンプトが表示されます。

```
<--- More --->
```

More プロンプトでは、次のように、UNIX の **more** コマンドに類似した構文が使用されます。

- 次のテキスト画面を表示するには、**Space** バーを押します。
- 次の行を表示するには、**Enter** キーを押します。
- コマンドラインに戻るには、q キーを押します。

例

次に、**rename** コマンドのヘルプを表示する例を示します。

```
ciscoasa
#
help rename
USAGE:
        rename /noconfirm [{disk0:|disk1:|flash:}] <source path> [{disk0:|disk1:
|flash:}] <destination path>
DESCRIPTION:
rename          Rename a file
SYNTAX:
/noconfirm                      No confirmation
{disk0:|disk1:|flash:} Optional parameter that specifies the filesystem
<source path>           Source file path
<destination path>      Destination file path
ciscoasa
#
```

次に、コマンド名と疑問符を入力して、ヘルプを表示する例を示します。

```
ciscoasa(config)# enable ?
usage: enable password <pwd> [encrypted]
```

コマンドプロンプトで?を入力すると、主要コマンド（show、no、またはclearコマンド以外）に関するヘルプを表示できます。

```
ciscoasa(config)# ?
aaa
      Enable, disable, or view TACACS+ or RADIUS

                        user authentication, authorization and accounting
...
```

関連コマンド

コマンド	説明
show version	オペレーティング システム ソフトウェアに関する情報を表示します。

hidden-parameter

ASA が SSO 認証のために認証 Web サーバーに送信する HTTP POST 要求の非表示パラメータを指定するには、AAA サーバー ホスト コンフィギュレーション モードで **hidden-parameter** コマンドを使用します。実行コンフィギュレーションからすべての非表示パラメータを削除するには、このコマンドの **no** 形式を使用します。

hidden-parameter文字列
nohidden-parameter

（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 フォームに組み込まれて SSO サーバーに送信される非表示パラメータ。複数行に入力できます。各行の最大文字数は 255 です。すべての行をあわせた（非表示パラメータ全体の）最大文字数は 2048 文字です。

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		
	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
AAA サーバー 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。

ASA の WebVPN サーバーは、認証 Web サーバーに SSO 認証要求を送信するときに HTTP POST 要求を使用します。その要求では、ユーザーには表示されない SSO HTML フォームの特定の非表示パラメータ（ユーザー名およびパスワード以外）が必要になることがあります。Web

サーバーから受信したフォームに対して HTTP ヘッダー アナライザを使用することで、Web サーバーが POST 要求で想定している非表示パラメータを検出できます。

hidden-parameter コマンドを使用すると、Web サーバーが認証 POST 要求で必要としている非表示パラメータを指定できます。ヘッダーアナライザを使用する場合は、エンコーディング済みの URL パラメータを含む非表示パラメータ文字列全体をコピーして貼り付けることができます。

入力を簡単にするために、複数の連続行で非表示パラメータを入力できます。ASA では、その複数行を連結して単一の非表示パラメータにします。非表示パラメータ 1 行ごとの最大文字数は 255 文字ですが、各行にはそれより少ない文字しか入力できません。

（注） 文字列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、& で区切られた 4 つのフォーム エントリとその値で構成される非表示パラメータの例を示します。POST 要求から抜き出された 4 つのエントリおよびその値は、次のとおりです。

- SMENC、値は ISO-8859-1
- SMLOCALE、値は US-EN
- ターゲット、値は https%3A%2F%2Ftools.cisco.com%2Femco%2Fappdir%2FAreaRoot.do

%3FEMCOPageCode%3DENG

- smauthreason、値は 0

SMENC=ISO-8859-1&SMLOCALE=US-EN&targ=https%3A%2F%2Ftools.cisco.com%2Femco%2Fappdir%2FAreaRoot.do%3FEMCOPageCode%3DENG&smauthreason=0

```
ciscoasa(config)# aaa-server testgrp1 host example.com
ciscoasa(config-aaa-server-host)# hidden-parameter SMENC=ISO-8859-1&SMLOCALE=US-EN&targe
ciscoasa(config-aaa-server-host)# hidden-parameter t=https%3A%2F%2Ftools.cisco.com%2Femc
ciscoasa(config-aaa-server-host)# hidden-parameter o%2Fappdir%2FAreaRoot.do%3FEMCOPageCo
ciscoasa(config-aaa-server-host)# hidden-parameter de%3DENG&smauthreason=0
ciscoasa(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
action-uri	SSO 認証用のユーザー名およびパスワードを受信するための Web サーバー URI を指定します。
auth-cookie-name	認証クッキーの名前を指定します。
password-parameter	SSO 認証用にユーザー 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。

コマンド	説明
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認証用にユーザー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。

hidden-shares

CIFS ファイルの非表示共有の可視性を制御するには、グループ webvpn コンフィギュレーションモードで **hidden-shares** コマンドを使用します。非表示共有オプション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。

hidden-shares { **none** | **visible** }
[**no**] **hidden-shares** { **none** | **visible** }

構文の説明

none	設定済みの非表示共有の表示およびアクセスをユーザーが実行できないことを指定します。
visible	非表示共有を表示して、ユーザーがアクセスできるようにします。

コマンド デフォルト

このコマンドのデフォルト動作は none 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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ webvpn 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(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

非表示共有は、共有名の末尾のドル記号（$）で識別されます。たとえば、ドライブ C は C$ として共有されます。非表示共有では、共有フォルダは表示されず、ユーザーはこれらの非表示リソースを参照またはアクセスすることを禁止されます。

hidden-shares コマンドの **no** 形式を使用すると、コンフィギュレーションからオプションが削除され、グループポリシー属性として非表示共有がディセーブルになります。

例

次に、GroupPolicy2 に関連する WebVPN CIFS 非表示共有を可視にする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-group-policy)# group-policy GroupPolicy2 attributes
ciscoasa(config-group-policy)# webvpn
```

```
ciscoasa(config-group-webvpn)# hidden-shares visible
ciscoasa(config-group-webvpn)#
```

関連コマンド

コマンド	説明
debug webvpn cifs	CIFS に関するデバッグ メッセージを表示します。
group-policy attributes	グループ ポリシー 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、指定したグループ ポリシーの属性と値を設定したり、webvpn コンフィギュレーション モードを開始して、グループの WebVPN 属性を設定したりできます。
url-list	WebVPN ユーザーがアクセスする URL のセットを設定します。
url-list	特定のユーザーまたはグループ ポリシーに、WebVPN サーバーおよび URL のリストを適用します。

hold-time

ASA が EIGRP hello パケットでアドバタイズするホールドタイムを指定するには、インターフェイス コンフィギュレーション モードで **hold-time** コマンドを使用します。hello 間隔をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

hold-time eigrp *as-number seconds*
no hold-time eigrp *as-number seconds*

構文の説明

as-number	EIGRP ルーティング プロセスの自律システム番号です。
seconds	ホールド タイムを秒数で指定します。有効な値は、1 ～ 65535 秒です。

コマンド デフォルト

デフォルトは 15 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	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
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
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

この値は、ASA によって EIGRP hello パケットでアドバタイズされます。そのインターフェイスの EIGRP ネイバーは、この値を使用して ASA の可用性を判断します。アドバタイズされたホールドタイム中に ASA から hello パケットを受信しなかった場合、EIGRP ネイバーは ASA が使用不可であると見なします。

非常に混雑した大規模ネットワークでは、一部のルータおよびアクセス サーバーが、デフォルト ホールド タイム内にネイバーから hello パケットを受信できない可能性があります。この場合、ホールド タイムを増やすこともできます。

ホールド タイムは、少なくとも hello 間隔の 3 倍にすることを推奨します。指定したホールド タイム内に ASA で hello パケットを受信しなかった場合、このネイバーを通過するルートは使用不可であると見なされます。

ホールド タイムを増やすと、ネットワーク全体のルート収束が遅くなります。

例

次の例では、EIGRP hello 間隔を 10 秒に、ホールド タイムを 30 秒に設定します。

```
ciscoasa(config-if)# hello-interval eigrp 100 10
ciscoasa(config-if)# hold-time eigrp 100 30
```

関連コマンド

コマンド	説明
hello-interval	インターフェイス上で送信される EIGRP hello パケット間の間隔を指定します。

homepage

該当 WebVPN ユーザーまたはグループポリシーに対して、ログイン時に表示される Web ページの URL を指定するには、webvpn コンフィギュレーション モードで **homepage** コマンドを使用します。**homepage none** コマンドを発行して作成したヌル値を含めて、設定されているホームページを削除するには、このコマンドの **no** 形式を入力します。

homepage { **value** *url-string* | **none** }
no homepage

構文の説明

none	WebVPN ホームページがないことを指定します。ヌル値を設定して、ホームページを拒否します。ホームページを継承しないようにします。
value *url-string*	ホームページの URL を指定します。http:// または https:// のいずれかで始まるストリングにする必要があります。

コマンド デフォルト

デフォルトのホームページはありません。

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
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
7.0(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

グループ ポリシーに関連付けられているユーザーのホームページ URL を指定するには、このコマンドで URL 文字列値を入力します。デフォルト グローバル ポリシーからホームページを継承するには、このコマンドの **no** 形式を使用します。**no** オプションを使用すると、値を別のグループポリシーから継承できるようになります。ホームページを継承しないようにするには、**homepage none** コマンドを入力します。

認証に成功すると、クライアントレスユーザーにはすぐにこのページが表示されます。 VPN 接続が正常に確立されると、AnyConnect クライアント によってデフォルトの Web ブラウザが起動され、この URL が表示されます。Linux プラットフォームでは、AnyConnect クライアント は現在このコマンドをサポートしていないため、コマンドは無視されます。

例

次に、FirstGroup という名前のグループ ポリシーのホームページとして www.example.com を指定する例を示します。

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 webvpn
ciscoasa(config-group-webvpn)# homepage value http://www.example.com
```

関連コマンド

コマンド	説明
webvpn	webvpn コンフィギュレーション モードを開始して、グループ ポリシーまたはユーザー名に適用するパラメータを設定できるようにします。

homepage use-smart-tunnel

クライアントレス SSL VPN の使用時に、グループポリシーのホームページがスマートトンネル機能を使用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 モードで **homepage use-smart-tunnel** コマンドを使用します。

homepage { **value** *url-string* | **none** }
homepage use-smart-tunnel

構文の説明

none	WebVPN ホームページがないことを指定します。ヌル値を設定して、ホームページを拒否します。ホームページを継承しないようにします。
value *url-string*	ホームページの URL を指定します。http:// または https:// のいずれかで始まるストリングにする必要があります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ 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
8.3(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

ブラウザ セッションをモニターし、スマート トンネルが WebVPN 接続中に開始されたことを確認するために HTTP キャプチャ ツールを使用できます。ブラウザ キャプチャの表示内容により、要求が制限されることなく Web ページに転送されるかどうか、またスマート トンネルが使用されているかどうかが判断されます。https://172.16.16.23/+CSCOE+portal.html などが表示された場合、*+CSCO** はコンテンツが ASA によって制限されていることを示しています。スマートトンネルが開始されると、+CSCO* がない特定の URL に対する **http get** コマンドが表示されます（GET 200 html http://mypage.example.com など）。

例

ベンダー V がパートナー P に自社内部の在庫サーバー ページへのクライアントレス アクセスを提供する場合を考えます。この場合、ベンダー V の管理者は、次の事項を決定する必要があります。

- ユーザーは、クライアントレス SSL VPN にログインした後、クライアントレス ポータルを経由するかどうかに関係なく、在庫ページアクセスできますか。
- ページに Microsoft Silverlight コンポーネントが含まれていますが、アクセスするのにスマート トンネルは適切な選択肢ですか。
- ブラウザがトンネリングされると、すべてのトンネル ポリシーによりすべてのブラウザ トラフィックがベンダーVのASAを経由するように強制され、パートナーPのユーザーは内部リソースにアクセスできなくなりますが、すべてをトンネリングするポリシーは適切ですか。

在庫ページが inv.example.com（10.0.0.0）でホストされると仮定すると、次の例では、1 つのホストだけを含むトンネル ポリシーが作成されます。

```
ciscoasa(config-webvpn)# smart-tunnel network inventory ip 10.0.0.0
ciscoasa(config-webvpn)# smart-tunnel network inventory host inv.example.com
```

次に、トンネル指定トンネル ポリシーをパートナーのグループ ポリシーに適用する例を示します。

```
ciscoasa(config-group-webvpn)# smart-tunnel tunnel-policy tunnelspecified inventory
```

次に、グループ ポリシーのホームページを指定し、そこでスマート トンネルをイネーブルにする例を示します。

```
ciscoasa(config-group-webvpn)# homepage value http://inv.example.com
ciscoasa(config-group-webvpn)# homepage use-smart-tunnel
```

host（ネットワーク オブジェクト）

ネットワーク オブジェクトのホストを設定するには、ネットワーク オブジェクト コンフィギュレーション モードで **host** コマンドを使用します。ホストをオブジェク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。

host*ip_address*
no host *ip_address*

構文の説明

ip_address	オブジェクトのホスト IP アドレス（IPv4 または IPv6）を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	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
オブジェクト 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
8.3(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

既存のネットワーク オブジェクトを異なる IP アドレスを使用して設定すると、新しいコンフィギュレーションが既存のコンフィギュレーションに置き換わります。

例

次に、ホスト ネットワーク オブジェクトを作成する例を示します。

```
ciscoasa (config)# object network OBJECT1
ciscoasa (config-network-object)# host 10.1.1.1
```

関連コマンド

コマンド	説明
clear configure object	作成されたすべてのオブジェクトをクリアします。
nat	ネットワーク オブジェクトの NAT をイネーブルにします。

コマンド	説明
object network	ネットワーク オブジェクトを作成します。
object-group network	ネットワーク オブジェクト グループを作成します。
show running-config object network	ネットワーク オブジェクト コンフィギュレーションを表示します。

host（パラメータ）

RADIUSアカウンティングを使用して対話するホストを指定するには、RADIUSアカウンティング パラメータ コンフィギュレーション モードで **host** コマンドを使用します。このモードにアクセスするには、ポリシー マップ タイプ インスペクションのRADIUS アカウンティング サブモードで**parameters**コマンドを使用します。指定したホス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。

host *address* [**key** *secret*]
no host *address* [**key** *secret*]

構文の説明

host	RADIUS アカウンティング メッセージを送信する単一のエンドポイントを指定します。
address	RADIUS アカウンティング メッセージを送信するクライアントまたはサーバーの IP アドレス。
key	アカウンティング メッセージの無償コピーを送信するエンドポイントの秘密キーを指定するオプションのキーワード。
secret	メッセージの検証に使用されるアカウンティング メッセージを送信するエンドポイントの共有秘密キー。最大 128 の英数字を使用できます。

コマンド デフォルト

no オプションはデフォルトで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。

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
RADIUS アカウンティング 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
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

このコマンドは、インスタンスを複数設定できます。

例

次に、RADIUS アカウンティングを使用するホストを指定する例を示します。

```
ciscoasa(config)# policy-map type inspect radius-accounting ra
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# host 209.165.202.128 key cisco123
```

関連コマンド

コマンド	説明
inspect radius-accounting	RADIUS アカウンティングのインスペクションを設定します。
parameters	インスペクション ポリシーマップのパラメータを設定します。

hostname

ASA のホスト名を設定するには、グローバル コンフィギュレーション モードで **hostname** コマンドを使用します。デフォルトのホスト名に戻すには、このコマンドの **no** 形式を使用します。

hostname*name*
no hostname [*name*]

構文の説明

name	ホスト名を最大 63 文字で指定します。ホスト名はアルファベットまたは数字で開始および終了する必要があり、間の文字にはアルファベット、数字、またはハイフンのみを使用する必要があります。

コマンド デフォルト

デフォルトのホスト名はプラットフォームによって異なります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	英数字以外の文字（ハイフンを除く）は使用できなくなりました。

使用上のガイドライン

ホスト名は、コマンドラインプロンプトとして表示され、複数のデバイスへのセッションを確立している場合に、コマンドを入力している場所を把握するのに役立ちます。マルチコンテキスト モードでは、システム実行スペースに設定したホスト名がすべてのコンテキストのコマンドライン プロンプトに表示されます。

コンテキスト内に任意で設定したホスト名は、コマンドラインには表示されませんが、**banner** コマンドの **$(hostname)** トークンでは使用できます。

例

次に、ホスト名を firewall1 に設定する例を示します。

```
ciscoasa(config)# hostname firewall1
firewall1(config)#
```

関連コマンド

コマンド	説明
banner	ログイン バナー、Message-of-The-Day バナー、またはイネーブル バナーを設定します。
domain-name	デフォルトのドメイン名を設定します。

hostname dynamic

ASA で IS-IS ダイナミックホスト名機能をイネーブルにするには、ルータ ISIS コンフィギュレーション モードで **hostname dynamic** コマンドを使用します。ダイナミックホスト名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。

hostname dynamic
no hostname dynamic

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトでは、ダイナミック ホスト名はイネーブルです。

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。

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 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

IS-IS ルーティング ドメインでは、各 ASA はシステム ID により表されます。システム ID は、IS-IS ASA ごと構成されている Network Entity Title（NET）の一部です。たとえば、NET 49.0001.0023.0003.000a.00 が設定されている ASA のシステム ID が 0023.0003.000a であるとします。ネットワーク管理者にとって、ルータでのメンテナンスやトラブルシューティングの間、ルータ名とシステム ID の対応を覚えているのは難しいことです。**show isis hostname** コマンドを入力すると、システム ID とルータ名のマッピングテーブルに含まれるエントリが表示されます。

ダイナミック ホスト名メカニズムはリンクステート プロトコル（LSP）フラッディングを使用して、ネットワーク全体にルータ名に対するシステム ID のマッピング情報を配布します。ネットワーク上の ASA はすべて、このシステム ID に対するルータ名のマッピング情報をルーティング テーブルにインストールしようと試みます。

ネットワーク上で、ダイナミック名のタイプ、長さ、値（TLV）をアドバタイズしている ASA が突然アドバタイズメントを停止した場合、最後に受信されたマッピング情報が最大 1 時間、ダイナミック ホスト マッピング テーブルに残るため、ネットワークに問題が発生している間、

ネットワーク管理者はマッピング テーブル内のエントリを表示できます。**show isis hostname** コマンドを入力すると、マッピングテーブルに含まれるエントリが表示されます。

例

次に、ホスト名を firewall1 に設定する例を示します。

```
ciscoasa(config)# hostname firewall1
firewall1(config)#
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
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。

コマンド	説明
isis authentication mode	インターフェイスごとに、インスタンスに対してIS-ISパケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-ISパケットに対してのみ認証を実行するように、インターフェイスごとのIS-ISインスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS helloをインターフェイスごとのフルMTUサイズに設定します。
isis lsp-interval	インターフェイスごとの連続するIS-IS LSP送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定されたASAのプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各IS-IS LSPの再送信間の時間を設定します。
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。

コマンド	説明
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。
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。

コマンド	説明
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。

hostscan enable

クライアントレス SSL VPN リモートアクセスまたは AnyConnect クライアント を使用したリモートアクセスに対してホストスキャンを有効にするには、webvpn コンフィギュレーションモードで hostscan enable コマンドを使用します。ホストスキャンをディセーブルにするには、このコマンドの **no** 形式を使用します。

hostscan enable
no hostscan enable

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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
webvpn コンフィギュレーション モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
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

ホストスキャンは、1 つの例外を除いて、ASA へのすべてのリモート アクセス接続試行に対してグローバルにイネーブルまたはディセーブルに設定されます。

hostscan enable コマンドは次の処理を実行します。

1. 以前の hostscan image *path* コマンドによって実行されたチェックを補足する有効性チェックを提供します。
2. sdesktop フォルダがまだ存在しない場合は、disk0: 上に作成します。
3. data.xml（ホストスキャン コンフィギュレーション）ファイルが sdesktop フォルダにまだ存在しない場合は、追加します。
4. フラッシュ デバイスの data.xml を実行コンフィギュレーションにロードします。
5. ホストスキャンをイネーブルにします。

（注） **show webvpn hostscan** コマンドを入力して、ホストスキャンがイネーブルであるかどうかを確認できます。

- **hostscan enable** コマンドを入力する前に、実行コンフィギュレーション内に hostscan image *path* コマンドが存在する必要があります。
- **no hostscan enable** コマンドは、実行コンフィギュレーションでホストスキャンをディセーブルにします。ホストスキャンがディセーブルの場合、管理者は Hostscan Manager にアクセスできず、リモート ユーザーはホストスキャンを使用できません。
- data.xml ファイルを転送または置換する場合は、ホストスキャンをいったんディセーブルにしてからイネーブルにして、このファイルを実行コンフィギュレーションにロードします。
- ホストスキャンは、ASA へのすべてのリモート アクセス接続試行に対してグローバルにイネーブルまたはディセーブルに設定されます。個別の接続プロファイルやグループ ポリシーに対してホストスキャンをイネーブルまたはディセーブルに設定することはできません。

Exception：クライアントレス SSL VPN 接続の接続プロファイルは、コンピュータがグループ URL を使用して ASA への接続を試行し、ホストスキャンがグローバルにイネーブルの場合、ホストスキャンがクライアントコンピュータで実行されないように設定できます。次に例を示します。

ciscoasa(config)# **tunnel-group***group-name***webvpn-attributes**

ciscoasa(config-tunnel-webvpn)# **group-url https://www.url-string.com**

ciscoasa(config-tunnel-webvpn)# without-Hostscan

例

次に、ホストスキャンイメージのステータスを表示し、ホストスキャンイメージをイネーブルにするためのコマンドを示します。

```
ciscoasa(config-webvpn)# show webvpn hostscan
Hostscan is not enabled.
ciscoasa(config-webvpn)# hostscan enable
ciscoasa(config-webvpn)# show webvpn hostscan
Hostscan version 4.1.0.25 is currently installed and enabled.
ciscoasa(config-webvpn)#
```

関連コマンド

コマンド	説明
hostscan image	コマンドに指定されたホストスキャン イメージを、パスに指定されたフラッシュ ドライブから実行コンフィギュレーションにコピーします。
show webvpn hostscan	イネーブルの場合、ホストスキャンのバージョンを識別します。ディセーブルの場合、CLI に「Secure Desktop is not enabled.」と表示されます。

コマンド	説明
without-Hostscan	クライアントレス SSL VPN セッションの接続プロファイルを、コンピュータがグループ URL を使用して ASA への接続を試行し、ホストスキャンがグローバルにイネーブルの場合、ホストスキャンがクライアント コンピュータで実行されないように設定します。

hostscan image

シスコのホスト スキャン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、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 hostscan image コマンドを使用します。ホストスキャン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。

hostscan image *path*
no hostscan image *path*

構文の説明

path シスコのホスト スキャン 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。

ホストスキャンパッケージには、Cisco.com からダウンロードできるファイル名の命名規則（hostscan-version.pkg）を含むスタンドアロンのホストスキャンパッケージ、または Cisco.com からダウンロードできるファイル名の命名規則（anyconnect-win-version-k9.pkg）を含む完全な AnyConnect クライアント パッケージを指定できます。お客様が AnyConnect クライアント を指定すると、ASA は AnyConnect クライアント パッケージからホストスキャンパッケージを取得してインストールします。

ホスト スキャン パッケージには、ホスト スキャン ソフトウェアおよびホスト スキャン ライブラリとサポート チャートが含まれています。

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		
	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
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
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

現在インストールされ、イネーブルになっているホストスキャンイメージのバージョンを確認するには、**show webvpn hostscan** コマンドを入力します。

hostscan image コマンドを使用してホストスキャンをインストールしたら、enable コマンドを使用してイメージをイネーブルにします。

次回のASAのリブート時にホストスキャンイメージを確実に使用できるように、**write memory** コマンドを入力して実行コンフィギュレーションを保存します。

例

次に、シスコのホストスキャンパッケージをインストールし、イネーブルにして、表示およびフラッシュ ドライブへの設定の保存を行うコマンドを示します。

```
ciscoasa> en
Password: ******
ciscoasa# config t
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# show webvpn hostscan
Hostscan is not enabled.
ciscoasa(config-webvpn)# hostscan image disk0:/hostscan_3.0.0333-k9.pkg

ciscoasa(config-webvpn)# hostscan enable
ciscoasa(config-webvpn)# show webvpn hostscan
Hostscan version 3.0.0333 is currently installed and enabled
ciscoasa(config-webvpn)# write memory
Building configuration...
Cryptochecksum: 2e7126f7 71214c6b 6f3b28c5 72fa0a1e
22067 bytes copied in 3.460 secs (7355 bytes/sec)
[OK]
ciscoasa(config-webvpn)#
```

関連コマンド

コマンド	説明
show webvpn hostscan	シスコのホスト スキャンがイネーブルである場合、そのバージョンを示します。ディセーブルの場合、CLIに「Hostscan is not enabled..」と表示されます。
hostscan enable	管理およびリモート ユーザー アクセスのホストスキャンをイネーブルにします。

hpm topn enable

ASA 経由で接続している上位ホストに関する ASDM のリアルタイムレポート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 **hpm topn enable** コマンドを使用します。ホストのレポート作成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。

hpm topn enable
no hpm topn enable

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、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—

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

システム パフォーマンスを最大にする場合は、このコマンドをディセーブルにすることを推奨します。このコマンドにより、[ASDM Home] > [Firewall Dashboard] > [Top 200 Hosts] ペインに情報が入力されます。

例

次の例では、上位ホストのレポート作成をイネーブルします。

```
ciscoasa(config)# hpm topn enable
```

関連コマンド

コマンド	説明
clear configure hpm	HPM コンフィギュレーションをクリアします。
show running-config hpm	HPM コンフィギュレーションを表示します。

hsi

H.323 プロトコルインスペクションの HSI グループに HSI を追加するには、HSI グループ コンフィギュレーション モードで **hsi** 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。

hsi*ip_address*
no hsi *ip_address*

構文の説明

ip_address	追加するホストの IP アドレス。HSI グループごとに最大で 5 つの HSI を設定できます。

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		
	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
HSI グループ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、H.323 インスペクション ポリシー マップで HSI を HSI グループに追加する例を示します。

```
ciscoasa(config-pmap-p)# hsi-group 10
ciscoasa(config-h225-map-hsi-grp)# hsi 10.10.15.11
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
endpoint	HSI グループにエンドポイントを追加します。
hsi-group	HSI グループを作成します。

コマンド	説明
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

hsi-group

H.323 プロトコルインスペクション用の HSI グループを定義して、HSI コンフィギュレーション モードを開始するには、パラメータ コンフィギュレーション モードで **hsi-group** 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。

hsi-group*group_id*
no hsi-group *group_id*

構文の説明

group_id HSI グループの ID 番号（0 ～ 2147483647）。

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		
	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
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
7.2(1)	このコマンドが追加されました。

例

次に、H.323 インスペクション ポリシー マップで HSI グループを設定する例を示します。

```
ciscoasa(config-pmap-p)# hsi-group 10
ciscoasa(config-h225-map-hsi-grp)# hsi 10.10.15.11
ciscoasa(config-h225-map-hsi-grp)# endpoint 10.3.6.1 inside
ciscoasa(config-h225-map-hsi-grp)# endpoint 10.10.25.5 outside
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
endpoint	HSI グループにエンドポイントを追加します。
hsi	HSI を HSI グループに追加します。

コマンド	説明
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

hsts enable

ブラウザやその他のユーザーエージェントへの HTTP Strict Transport Security ヘッダーの送信を設定するには、webvpn コンフィギュレーション モードで **hsts enable** 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設定を削除するには、このコマンドの no 形式を使用します。このコマンドが有効になると、非セキュアな方法でアクセスが試行された場合、準拠しているブラウザおよびユーザー エージェントは HTTPS に切り替えられます。

hsts enable
no hsts enable

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトでは、Strict Transport Security ヘッダーは使用されません。

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
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
9.8(2)	このコマンドが導入されました。

使用上のガイドライン

HTTP Strict Transport Security（HSTS）は、Web セキュリティ ポリシーのメカニズムであり、プロトコル ダウングレード攻撃および Cokie ハイジャックから Web サイトを保護するのに役立ちます。これにより Web サーバーは、Web ブラウザ（またはその他の準拠しているユーザーエージェント）が Web サーバーと通信するにはセキュア HTTPS 接続を使用する必要があり、非セキュアな HTTP プロトコルを使用して通信することはできないことを宣言できます。

有効にすると、デフォルトのタイムアウト値である 10,886,400 秒（18 週）が使用されます。これは、**hsts max-age** コマンドを使用して変更できます。

例

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

関連コマンド

コマンド	説明
hsts max-age	ASA が HSTS ホストとして扱われ、セキュアな方法でアクセスされる期間の最大値です。
show running-config webvpn hsts	SSL VPN の実行コンフィギュレーションを、HTTP 設定も含めて表示します。

hsts max-age

ブラウザやその他のユーザーエージェントへの HTTP Strict Transport Security ヘッダーの送信が（**hsts enable** コマンドを使用して）設定されている場合、**hsts max-age** を使用すると、ASA が HSTS ホストとして扱われ、セキュアな方法でアクセスされる期間の最大値を設定できます。

hsts max-age *max-value-in-seconds*

構文の説明

max-value-in-seconds	HSTS が有効になる期間（秒数）。範囲は <0 ～ 31536000> 秒です。

コマンド デフォルト

デフォルトでは、最大値は 10,886,400（18 週）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		
	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
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
9.8(2)	このコマンドが導入されました。

使用上のガイドライン

HTTP Strict Transport Security（HSTS）は、Web セキュリティ ポリシーのメカニズムであり、プロトコル ダウングレード攻撃および Cokie ハイジャックから Web サイトを保護するのに役立ちます。これにより Web サーバーは、Web ブラウザ（またはその他の準拠しているユーザーエージェント）が Web サーバーと通信するにはセキュア HTTPS 接続を使用する必要があり、非セキュアな HTTP プロトコルを使用して通信することはできないことを宣言できます。

有効にすると、デフォルトのタイムアウト値である 10,886,400 秒（18 週）が使用されます。このコマンドは、タイムアウトを変更します。

例

```
ciscoasa
(config)#
 webvpn
ciscoasa(config-webvpn)# hsts max-age 31536000
ciscoasa(config-webvpn)#
```

関連コマンド

コマンド	説明
hsts enable	HSTS ヘッダーの送信を有効にします。
show running-config webvpn hsts	SSL VPN の実行コンフィギュレーションを、HTTP 設定も含めて表示します。

html-content-filter

このユーザーまたはグループポリシーに対して WebVPN セッションの Java、ActiveX、イメージ、スクリプト、およびクッキーをフィルタリングするには、webvpn コンフィギュレーション モードで **html-content-filter** コマンドを使用します。コンテンツフィルタを削除するには、このコマンドの **no** 形式を使用します。

html-content-filter { **java** | **images** | **scripts** | **cookies** | **none** }
no html-content-filter [**java** | **images** | **scripts** | **cookies** | **none**]

構文の説明

cookies	イメージからクッキーを削除して、限定的な広告フィルタリングとプライバシーを提供します。
images	イメージへの参照を削除します（<IMG> タグを削除します）。
java	Java および ActiveX への参照を削除します（<EMBED>、<APPLET>、および <OBJECT> タグ。
none	フィルタリングを行わないことを指定します。ヌル値を設定して、フィルタリングを拒否します。フィルタリング値を継承しないようにします。
scripts	スクリプティングへの参照を削除します（<SCRIPT> タグを削除します）。<SCRIPT> tags).

コマンド デフォルト

フィルタリングは行われません。

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
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
7.0(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

html-content-filter none コマンドを発行して作成したヌル値を含めて、すべてのコンテンツフィルタを削除するには、引数を指定せずにこのコマンドの **no** 形式を入力します。**no** オプション

を使用すると、値を別のグループ ポリシーから継承できるようになります。HTML コンテンツフィルタを継承しないようにするには、**html-content-filter none** コマンドを使用します。

次回このコマンドを使用すると、前回までの設定が上書きされます。

例

次に、FirstGroup という名前のグループ ポリシーに対して Java と ActiveX、クッキー、およびイメージのフィルタリングを設定する例を示します。

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 webvpn
ciscoasa(config-group-webvpn)# html-content-filter java cookies images
```

関連コマンド

コマンド	説明
webvpn	webvpn コンフィギュレーション モードを開始して、グループ ポリシーまたはユーザー名に適用するパラメータを設定できるようにします。グローバル コンフィギュレーション モードを開始して WebVPN のグローバル設定を設定できるようにします。

http（グローバル）

ASA 内部の HTTP サーバーにアクセスできるホストを指定するには、グローバル コンフィギュレーション モードで **http** コマンドを使用します。1 つ以上のホストを削除するには、このコマンドの **no** 形式を使用します。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** 形式を引数なしで使用します。

http*ip_addresssubnet_maskinterface_name*
no http

構文の説明

interface_name	ホストが HTTP サーバーにアクセスするために通過する ASA のインターフェイスの名前を指定します。物理インターフェイスまたは仮想インターフェイスを指定できます。BVI インターフェイスが指定されている場合、そのインターフェイスに対し **managenent-access** を設定する必要があります。
ip_address	HTTP サーバーにアクセスできるホストの IP アドレスを指定します。
subnet_mask	HTTP サーバーにアクセスできるホストのサブネット マスクを指定します。

コマンド デフォルト

HTTP サーバーにアクセスできるホストはありません。

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
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.7(1)	直接接続された HTTP 管理ステーションがある場合は、ASA とホストで /31 サブネットを使用して、ポイントツーポイント接続を作成できます。
9.9.(2)	仮想インターフェイスが指定可能になりました。

例

次に、IP アドレス 10.10.99.1 とサブネット マスク 255.255.255.255 を持つホストが、外部インターフェイス経由でHTTPサーバーにアクセスできるようにする例を示します。

```
ciscoasa(config)# http 10.10.99.1 255.255.255.255 outside
```

次に、任意のホストが、外部インターフェイス経由で HTTP サーバーにアクセスできるようにする例を示します。

```
ciscoasa(config)# http 0.0.0.0 0.0.0.0 outside
```

関連コマンド

コマンド	説明
clear configure http	HTTP コンフィギュレーションを削除します。HTTP サーバーをディセーブルにし、HTTP サーバーにアクセスできるホストを削除します。
http authentication-certificate	ASA への HTTPS 接続を確立するユーザーの証明書による認証を要求します。
http redirect	ASA が HTTP 接続を HTTPS にリダイレクトすることを指定します。
http server enable	HTTP サーバーをイネーブルにします。
show running-config http	HTTP サーバーにアクセスできるホストを表示し、さらに HTTP サーバーがイネーブルであるかどうかを表示します。

http[s]（パラメータ）

ScanSafe インスペクション ポリシー マップのサービスタイプを指定するには、パラメータ コンフィギュレーション モードで **http**[**s**] コマンドを使用します。サービスタイプを削除するには、このコマンドの **no** 形式を使用します。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 scansafe** コマンドを入力します。

{ **http** | **https** }
no { **http** | **https** }

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(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

ScanSafe インスペクション ポリシー マップには、**http** または **https** のいずれか 1 つのサービス タイプのみを指定できます。デフォルトはありません。タイプを指定する必要があります。

例

次に、インスペクション ポリシー マップを作成して、サービス タイプを HTTP に設定する例を示します。

```
ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap1
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# http
```

関連コマンド

コマンド	説明
class-map type inspect scansafe	ホワイトリストに記載されたユーザーとグループのインスペクション クラス マップを作成します。

コマンド	説明
default user group	ASA に入ってくるユーザーのアイデンティティを ASA が判別できない場合のデフォルトのユーザー名やグループを指定します。
http[**s**]（パラメータ）	インスペクション ポリシー マップのサービス タイプ（HTTP または HTTPS）を指定します。
inspect scansafe	このクラスのトラフィックに対するクラウド Web セキュリティ インスペクションをイネーブルにします。
license	要求の送信元の組織を示すため、ASA がクラウド Web セキュリティ プロキシ サーバーに送信する認証キーを設定します。
match user group	ユーザーまたはグループをホワイトリストと照合します。
policy-map type inspect scansafe	インスペクション ポリシー マップを作成すると、ルールのために必要なパラメータを設定し、任意でホワイトリストを識別できます。
retry-count	再試行回数値を入力します。この値は、可用性をチェックするために、クラウド Web セキュリティプロキシサーバーをポーリングする前に ASA が待機する時間です。
scansafe	マルチ コンテキスト モードでは、コンテキストごとにクラウド Web セキュリティを許可します。
scansafe general-options	汎用クラウド Web セキュリティ サーバー オプションを設定します。
server {**primary** | **backup**}	プライマリまたはバックアップのクラウド Web セキュリティ プロキシ サーバーの完全修飾ドメイン名または IP アドレスを設定します。
show conn scansafe	大文字の Z フラグに示されたようにすべてのクラウド Web セキュリティ接続を表示します。
show scansafe server	サーバーが現在のアクティブ サーバー、バックアップ サーバー、または到達不能のいずれであるか、サーバーのステータスを表示します。
show scansafe statistics	合計と現在の http 接続を表示します。
user-identity monitor	AD エージェントから指定したユーザーまたはグループ情報をダウンロードします。
whitelist	トラフィックのクラスでホワイトリスト アクションを実行します。

http authentication-certificate

ASDM の HTTPS 接続による認証のために証明書を要求するには、グローバル コンフィギュレーション モードで **http authentication-certificate** 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** バージョンを使用します。

http authentication-certificate *interface name* [**match** *certificate_map_name*]
no http authentication-certificate [*interface* [**match** *certificate_map_name*]]

構文の説明

interface	証明書による認証を必要とする ASA でインターフェイスを指定します。
match *certificate_map_name*	証明書は証明書マップと一致する必要があります。マップを設定するには、**crypto ca certificate map** を使用します。

コマンド デフォルト

HTTP の証明書認証はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

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。
8.0(3)	このコマンドよりも **ssl certificate-authentication** コマンドを推奨します。
8.2.1	このコマンドは、再追加されました。グローバルな **ssl certificate-authentication** コマンドは、下位互換性のために保存されています。
8.4.7, 9.1.3	証明書のみの認証がイネーブルになりました。以前は、このコマンドは、**aaa authentication http console** コマンドをイネーブルにした場合にだけ証明書認証をユーザー認証に追加しました。
9.6(2)	**match** *certificate_map_name* オプションが追加されました。

使用上のガイドライン

AAA 認証の有無にかかわらず証明書認証を必須にできます。証明書認証はインターフェイスごとに設定できます。その結果、信頼できるインターフェイスまたは内部インターフェイス上

の接続については証明書の提示が不要になります。コマンドを複数回使用すれば、複数のインターフェイス上で証明書認証をイネーブルにできます。

ASA は、PKI トラストポイントと比較して証明書を検証します。証明書が検証に合格しない場合、ASA は SSL 接続を終了します。

例

次に、outside および external というインターフェイスに接続するクライアントに対して、証明書による認証を要求する例を示します。

```
ciscoasa(config)# http authentication-certificate inside
ciscoasa(config)# http authentication-certificate external
```

関連コマンド

コマンド	説明
clear configure http	HTTP コンフィギュレーションを削除します。HTTP サーバーをディセーブルにし、HTTP サーバーにアクセスできるホストを削除します。
http	IP アドレスとサブネット マスクによって、HTTP サーバーにアクセスできるホストを指定します。ホストが HTTP サーバーへのアクセスで経由する ASA のインターフェイスを指定します。
http redirect	ASA が HTTP 接続を HTTPS にリダイレクトすることを指定します。
http server enable	HTTP サーバーをイネーブルにします。
show running-config http	HTTP サーバーにアクセスできるホストを表示し、さらに HTTP サーバーがイネーブルであるかどうかを表示します。
ssl authentication-certificate	SSL 接続に証明書を要求します。

http-comp

特定のグループまたはユーザーの WebVPN 接続上で 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 モードおよびユーザー名 webvpn コンフィギュレーション モードで http-comp 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。

http-comp { **gzip** | **none** }
no http-comp { **gzip** | **none** }

構文の説明

gzip	グループまたはユーザーに対して圧縮をイネーブルにすることを指定します。
none	そのグループまたはユーザーに対し圧縮がディセーブルにされるよう指示します。

コマンド デフォルト

デフォルトでは、圧縮はイネ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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザー名 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。

使用上のガイドライン

WebVPN 接続の場合、グローバル 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 コンフィギュレーション モードおよびユーザー名 webvpn コンフィギュレーション モードで設定された **http-comp** コマンドが上書きされます。

例

次の例では、グループ ポリシー sales の圧縮をディセーブルにします。

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# http-comp none
```

関連コマンド

コマンド	説明
圧縮	すべての SVC、WebVPN、および IPsec VPN 接続で、圧縮をイネーブルにします。

http connection idle-timeout

ASDM、クライアントレス VPN、AnyConnect クライアント、およびその他のクライアントなど、ASA への HTTPS 接続のアイドルタイムアウトを設定するには、グローバル コンフィギュレーション モードで **http connection idle-timeout** コマンドを使用します。タイムアウ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。

http connection idle-timeout *seconds*
no http connection idle-timeout

構文の説明

seconds アイドルタイムアウト（10 ー 86400 秒）。

コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.14(1)	このコマンドが追加されました。

使用上のガイドライン

ASA は、設定した期間アイドル状態の接続を切断します。**http server idle-timeout** コマンドと **http connection idle-timeout** コマンドの両方を設定した場合、**http connection idle-timeout** コマンドが優先されます。

例

次の例では、HTTPS セッションのアイドルタイムアウトを 600 秒に設定します。

```
ciscoasa(config)# http connection idle-timeout 600
```

関連コマンド

コマンド	説明
clear configure http	HTTP コンフィギュレーションを削除します。HTTP サーバーをディセーブルにし、HTTP サーバーにアクセスできるホストを削除します。

コマンド	説明
http	IP アドレスおよびサブネット マスクにより HTTP サーバーにアクセスできるホストと、そのホストの HTTP サーバーへのアクセスで経由するインターフェイスを指定します。
http authentication-certificate	ASA への HTTPS 接続を確立するユーザーの証明書による認証を要求します。
http server enable	ASDM セッション用に HTTP サーバーをイネーブルにします。
http server idle-timeout	ASDM アイドルタイムアウトを設定します。
http server session-timeout	ASA に対する ASDM セッションのセッション時間を制限します。
http redirect	ASA が HTTP 接続を HTTPS にリダイレクトすることを指定します。
show running-config http	HTTP サーバーにアクセスできるホストを表示し、さらに HTTP サーバーがイネーブルであるかどうかを表示します。

http-only-cookie

クライアントレス SSL VPN セッションクッキーの httponly フラグ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 **http-only-cookie** コマンドを使用します。このフラグ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。

http-only-cookie
no http-only-cookie

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

httponly フラグはデフォルトでディセーブルです。

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。

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
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
9.2(3)	このコマンドが導入されました。

使用上のガイドライン

Flash アプリケーションや Java アプレットなどの組み込みオブジェクト、および外部アプリケーションは、通常は既存のセッションのクッキーに依存してサーバーと連携しています。これらの組み込みオブジェクトは、初期化時にいくつかの Javascript を使用してブラウザからクッキーを取得します。クライアントレス SSL VPN セッション クッキーに httponly フラグを追加すると、セッションクッキーがブラウザのみで認識され、クライアント側のスクリプトでは認識されなくなり、セッションの共有は不可能になります。

VPN セッションクッキー設定の変更は、アクティブなクライアントレス SSL VPN セッションが存在しない場合のみ実行してください。**show vpn-sessiondb webvpn** コマンドを使用して、クライアントレス SSL VPN セッションのステータスを確認します。**vpn-sessiondb logoff webvpn** コマンドを使用して、すべてのクライアントレス SSL VPN セッションからログアウトします。

次のクライアントレス SSL VPN 機能は、**http-only-cookie** コマンドがイネーブルの場合に動作しません。

- Java プラグイン

- Java リライタ
- ポートフォワーディング。
- ファイルブラウザ
- デスクトップ アプリケーション（Microsoft Office アプリケーションなど）を必要とする Sharepoint 機能
- AnyConnect Web 起動
- Citrix Receiver、XenDesktop、および Xenon
- その他の非ブラウザ ベース アプリケーションおよびブラウザプラグインベースのアプリケーション

（注） このコマンドは、Cisco TAC から使用を推奨された場合のみ使用してください。このコマンドをイネーブルにすると、セキュリティ上のリスクが発生します。

例

次に、クライアントレス SSL VPN セッション クッキーの httponly フラグをイネーブルにする例を示します。

```
ciscoasa
(config)#
 webvpn
ciscoasa(config-webvpn)# http-only-cookie
ciscoasa(config-webvpn)
```

関連コマンド

コマンド	説明
show running-config webvpn	クライアントレス SSL VPN の実行コンフィギュレーションを表示します。

http-only-cookie

クライアントレス SSL VPN セッションクッキーの httponly フラグ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 **http-only-cookie** コマンドを使用します。このフラグ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。

http-only-cookie
no http-only-cookie

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

httponly フラグはデフォルトでディセーブルです。

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。

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
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
9.2(3)	このコマンドが導入されました。

使用上のガイドライン

Flash アプリケーションや Java アプレットなどの組み込みオブジェクト、および外部アプリケーションは、通常は既存のセッションのクッキーに依存してサーバーと連携しています。これらの組み込みオブジェクトは、初期化時にいくつかの Javascript を使用してブラウザからクッキーを取得します。クライアントレス SSL VPN セッション クッキーに httponly フラグを追加すると、セッションクッキーがブラウザのみで認識され、クライアント側のスクリプトでは認識されなくなり、セッションの共有は不可能になります。

VPN セッションクッキー設定の変更は、アクティブなクライアントレス SSL VPN セッションが存在しない場合のみ実行してください。**show vpn-sessiondb webvpn** コマンドを使用して、クライアントレス SSL VPN セッションのステータスを確認します。**vpn-sessiondb logoff webvpn** コマンドを使用して、すべてのクライアントレス SSL VPN セッションからログアウトします。

次のクライアントレス SSL VPN 機能は、**http-only-cookie** コマンドがイネーブルの場合に動作しません。

- Java プラグイン

- Java リライタ
- ポートフォワーディング。
- ファイルブラウザ
- デスクトップ アプリケーション（Microsoft Office アプリケーションなど）を必要とする Sharepoint 機能
- AnyConnect Web 起動
- Citrix Receiver、XenDesktop、および Xenon
- その他の非ブラウザ ベース アプリケーションおよびブラウザプラグインベースのアプリケーション

（注） このコマンドは、Cisco TAC から使用を推奨された場合のみ使用してください。このコマンドをイネーブルにすると、セキュリティ上のリスクが発生します。

例

次に、クライアントレス SSL VPN セッション クッキーの httponly フラグをイネーブルにする例を示します。

```
ciscoasa
(config)#
 webvpn
ciscoasa(config-webvpn)# http-only-cookie
ciscoasa(config-webvpn)
```

関連コマンド

コマンド	説明
show running-config webvpn	クライアントレス SSL VPN の実行コンフィギュレーションを表示します。

http-proxy（call-home）

スマートライセンスおよびSmart Call Home 用にHTTP(S) プロキシを設定するには、Call Home コンフィギュレーション モードで **http-proxy** コマンドを使用します。プロキシを削除するには、このコマンドの **no** 形式を使用します。

http-proxy*ip_address***port***port*
no http-proxy *ip_address* **port** *port*

構文の説明

ip_address	HTTP プロキシ サーバーの IP アドレスを設定します。
port *port*	HTTP プロキシのポート番号を設定します。たとえば、HTTPS サーバーに 443 を使用します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	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
Call Home コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Smart Call Home およびスマート ライセンスに対して HTTP または HTTPS プロキシをグローバルに設定します。

例

次に、HTTP プロキシを設定する例を示します。

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# http-proxy 10.1.1.1 port 443
```

関連コマンド

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

http-proxy（dap）

HTTP プロキシ ポート フォワーディングをイネーブルまたはディセーブルにするには、DAP webvpn コンフィギュレーション モードで **http-proxy** 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。

http-proxy { **enable** | **disable** | **auto-start** }
no http-proxy

構文の説明

auto-start	DAP レコードの HTTP プロキシ ポート フォワーディングをイネーブルにし、自動的に開始します。
enable/disable	DAP レコードの HTTP プロキシ ポート フォワーディングをイネーブルまたはディセーブルにします。

コマンド 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。

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
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

ASAは、さまざまなソースからの属性値を適用できます。次の階層に従って、属性値を適用します。

1. DAP レコード
2. ユーザー名
3. グループ ポリシー
4. トンネル グループのグループ ポリシー
5. デフォルトのグループ ポリシー

したがって、属性の DAP 値は、ユーザー、グループ ポリシー、またはトンネル グループに設定されたものよりも優先順位が高くなります。

DAP レコードの属性をイネーブルまたはディセーブルにすると、ASA はその値を適用して実行します。たとえば、DAP-webvpn コンフィギュレーション モードで HTTP プロキシをディセーブルにすると、ASA はそれ以上値を検索しません。ディセーブルにする代わりに**http-proxy** コマンドで **no** の値を設定した場合、属性は DAP レコードには存在しないため、ASA はユーザー名の AAA 属性に移動し、必要に応じてグループポリシーにも移動して、適用する値を検索します。

例

次に、Finance という名前の DAP レコードに対して HTTP プロキシ ポート フォワーディングをイネーブルにする例を示します。

```
ciscoasa
 (config)#
dynamic-access-policy-record
Finance
ciscoasa
(config-dynamic-access-policy-record)#
 webvpn
ciscoasa
(config-dap-webvpn)#
 http-proxy enable
ciscoasa
(config-dap-webvpn)#
```

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。

http-proxy（webvpn）

外部プロキシ サーバーを使用して HTTP 要求を処理するように ASA を設定するには、webvpn コンフィギュレーション モードで **http-proxy** コマンドを使用します。HTTP プロキシサーバー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。

http-proxy { **host** [*port*] [**exclude** *url*] | **pac** *pacfile* } [**username** *username* { **password** *password* }]
no http-proxy

構文の説明

ホスト	外部 HTTP プロキシ サーバーのホスト名または IP アドレス。
pac pacfile	1 つ以上のプロキシを指定する JavaScript 関数を含む PAC ファイルを指定します。
password	（オプション。username を指定した場合に限り使用可能）各 HTTP プロキシ要求にパスワードを付加して基本的なプロキシ認証を提供するには、このキーワードを入力します。
password	各 HTTP 要求とともにプロキシ サーバーに送信されるパスワード。
port	（任意）HTTP プロキシサーバーによって使用されるポート番号。デフォルトポートは 80 です。値を指定しなかった場合、ASA はこのポートを使用します。範囲は 1 ～ 65535 です。
url	プロキシ サーバーへの送信が可能な URL から除外する URL を 1 つ、または複数の URL のカンマ区切りのリストを入力します。このストリングには文字数の制限はありませんが、コマンド全体で 512 文字以下となるようにする必要があります。リテラル URL を指定するか、次のワイルドカードを使用できます。 • ***** は、スラッシュ（/）とピリオド（.）を含む任意の文字列と一致します。このワイルドカードは、英数字ストリングとともに使用する必要があります。 • **?** は、スラッシュおよびピリオドを含む、任意の 1 文字に一致します。 • [*x*-*y*] は、*x* から *y* までの範囲の任意の 1 文字と一致します。*x* は ANSI 文字セット内のある 1 文字を表し、*y* は別の 1 文字を表します。 • [**!***x*-*y*] は、範囲外の任意の 1 文字と一致します。
username	（任意）各 HTTP プロキシ要求にユーザー名を付加して基本的なプロキシ認証を提供するには、このキーワードを入力します。
username	各 HTTP 要求とともにプロキシ サーバーに送信されるユーザー名。

コマンド デフォルト

デフォルトでは、HTTP プロキシ サーバーは設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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
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
7.0(1)	このコマンドが追加されました。
8.0(2)	**exclude**、**username**、および**password**キーワードが追加されました。

使用上のガイドライン

組織が管理するサーバーを経由したインターネットへのアクセスを必須にすると、セキュアなインターネットアクセスを確保して管理面の制御を保証するためのフィルタリング導入の別のきっかけにもなります。

ASA でサポートされるのは、**http-proxy** コマンドの 1 つのインスタンスだけです。このコマンドのインスタンスが実行コンフィギュレーションにすでに 1 つ存在する場合、もう 1 つインスタンスを入力すると、CLI は以前のインスタンスを上書きします。**show running-config webvpn** コマンドを入力すると、CLI によって実行コンフィギュレーション内のすべての **http-proxy** コマンドがリストされます。応答に **http -proxy** コマンドがリストされていない場合、このコマンドは存在しません。

（注） プロキシ NTLM 認証は **http-proxy** ではサポートされていません。認証なしのプロキシと基本認証だけがサポートされています。

例

次の例は、次の設定の HTTP プロキシ サーバーの使用を設定する方法を示しています。IP アドレスが 209.165. 201.2 で、デフォルト ポートの 443 を使用しています。

```
ciscoasa
(config)#
 webvpn
ciscoasa(config-webvpn)# http-proxy 209.165.201.2
ciscoasa(config-webvpn)
```

次に、同じプロキシ サーバーを使用して、各 HTTP 要求とともにユーザー名およびパスワードを送信するように設定する例を示します。

```
ciscoasa(config-webvpn)# http-proxy 209.165.201.2 jsmith password mysecretdonttell
ciscoasa(config-webvpn)
```

次も、同じコマンドの例を示しますが、前の例とは異なり、この例では、ASAがHTTP要求でwww.example.comという特定のURLを受信した場合には、プロキシサーバーに渡すのではなく自分自身で要求を解決します。

```
ciscoasa(config-webvpn)# http-proxy 209.165.201.2 exclude www.example.com username jsmith
 password mysecretdonttell
ciscoasa(config-webvpn)
```

次の例は、**exclude**オプションの使い方を示しています。

```
ciscoasa(config-webvpn)# http-proxy 10.1.1.1 port 8080 exclude *.com username John pasword
 12345678
ciscoasa(config-webvpn)
```

次の例は、**pac**オプションの使い方を示しています。

```
ciscoasa(config-webvpn)# http-proxy pac http://10.1.1.1/pac.js
ciscoasa(config-webvpn)
```

関連コマンド

コマンド	説明
https-proxy	外部プロキシ サーバーを使用してHTTPS要求を処理するように設定します。
show running-config webvpn	SSL VPNの実行コンフィギュレーションを、HTTPおよびHTTPSのプロキシ サーバーをすべて含めて表示します。

http redirect

ASA による HTTP 接続の HTTPS へのリダイレクトを指定するには、グローバル コンフィギュレーション モードで **http redirect** コマンドを使用します。コンフィギュレーションから指定した **http redirect** コマンドを削除するには、このコマンドの **no** 形式を使用します。すべての **http redirect** 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** 形式を引数なしで使用します。

http redirect *interface* [*port*]
no http redirect [*interface*]

構文の説明

interface	ASA で HTTP 要求を HTTPS にリダイレクトする必要があるインターフェイスを識別します。
port	ASA が HTTP 要求をリッスンするポートを識別します。HTTP 要求はリッスン後 HTTPS にリダイレクトされます。デフォルトでは、ポート 80 でリッスンします。

コマンド デフォルト

HTTP リダイレクトはディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

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

インターフェイスには、HTTP を許可するアクセス リストが必要です。アクセス リストがない場合、ASA はポート 80 も HTTP 用に設定した他のどのポートもリッスンしません。

http redirect コマンドが失敗すると、次のメッセージが表示されます。

```
"TCP port <port_number> on interface <interface_name> is in use by another feature.
Please choose a different port for the HTTP redirect service"
```

HTTP リダイレクト サービス用に別のポートを使用してください。

例

次に、デフォルト ポート 80 のままで、内部インターフェイスの HTTP リダイレクトを設定する例を示します。

```
ciscoasa(config)# http redirect inside
```

関連コマンド

コマンド	説明
clear configure http	HTTP コンフィギュレーションを削除します。HTTP サーバーをディセーブルにし、HTTP サーバーにアクセスできるホストを削除します。
http	IP アドレスとサブネット マスクによって、HTTP サーバーにアクセスできるホストを指定します。ホストが HTTP サーバーへのアクセスで経由する ASA のインターフェイスを指定します。
http authentication-certificate	ASA への HTTPS 接続を確立するユーザーの証明書による認証を要求します。
http server enable	HTTP サーバーをイネーブルにします。
show running-config http	HTTP サーバーにアクセスできるホストを表示し、さらに HTTP サーバーがイネーブルであるかどうかを表示します。

http server basic-auth-client

ブラウザベース以外の HTTPS クライアントが ASA 上の HTTPS サービスにアクセスできるようにするには、グローバル コンフィギュレーション モードで **http server basic-auth-client** コマンドを使用します。クライアントのサポートを削除するには、このコマンドの **no** 形式を使用します。

http server basic-auth-client *user_agent*
no http server basic-auth-client *user_agent*

構文の説明

user_agent HTTP 要求の HTTP ヘッダーにあるクライアントの User-Agent 文字列を指定します。完全な文字列または部分文字列を指定できます。部分文字列については、User-Agent 文字列の先頭と一致している必要があります。セキュリティを強化するために完全な文字列をお勧めします。文字列では大文字と小文字が区別されることに注意してください。

たとえば、 **curl** は次の User-Agent 文字列と一致します。

```
curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1 Basic ECC
zlib/1.2.3 libidn/1.18 libssh2/1.4.2
```

curl は、次の User-Agent 文字列とは一致しません。

```
abcd curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1 Basic ECC
 zlib/1.2.3 libidn/1.18 libssh2/1.4.2
```

CURL は、次の User-Agent 文字列とは一致しません。

```
curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1 Basic ECC
zlib/1.2.3 libidn/1.18 libssh2/1.4.2
```

コマンド デフォルト

デフォルトでは、ASDM、CSM、および REST API が許可されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.12(1)	コマンドが追加されました。

使用上のガイドライン

個別のコマンドを使用して、各クライアント文字列を入力します。多くの専門クライアント（python ライブラリ、curl、wget など）は、クロスサイト要求の偽造（CSRF）トークンベースの認証をサポートしていないため、これらのクライアントが ASA 基本認証方式を使用することを明確に許可する必要があります。セキュリティ上の理由から、必要なクライアントのみを許可する必要があります。

例

次に、curl クライアントを許可する例を示します。

```
ciscoasa(config)# http server basic-auth-client curl
```

関連コマンド

コマンド	説明
http server enable	ASA で HTTPS サーバーを有効にします。

http server enable

ASA HTTP サーバー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 **http server enable** コマンドを使用します。HTTP サーバーを無効にするには、このコマンドの **no** 形式を使用します。

http server enable [*port*]

構文の説明

port	HTTP 接続に使用するポート。範囲は 1 ～ 65535 です。デフォルトのポートは 443 です。

コマンド デフォルト

HTTP サーバーはディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、HTTP サーバーをイネーブルにする例を示します。

```
ciscoasa(config)# http server enable
```

関連コマンド

コマンド	説明
clear configure http	HTTP コンフィギュレーションを削除します。HTTP サーバーをディセーブルにし、HTTPサーバーにアクセスできるホストを削除します。
http	IP アドレスとサブネット マスクによって、HTTP サーバーにアクセスできるホストを指定します。ホストが HTTP サーバーへのアクセスで経由する ASA のインターフェイスを指定します。

コマンド	説明
http authentication-certificate	ASA への HTTPS 接続を確立するユーザーの証明書による認証を要求します。
http redirect	ASA が HTTP 接続を HTTPS にリダイレクトすることを指定します。
show running-config http	HTTP サーバーにアクセスできるホストを表示し、さらに HTTP サーバーがイネーブルであるかどうかを表示します。

http server idle-timeout

ASA への ASDM 接続のアイドルタイムアウトを設定するには、グローバル コンフィギュレーション モードで **http server idle-timeout** コマンドを使用します。タイムアウ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。

http server idle-timeout [*minutes*]
no http server idle-timeout [*minutes*]

構文の説明

minutes アイドル タイムアウト（1 ～ 1440 分）。

コマンド デフォルト

デフォルトの設定は 20 分です。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

例

次に、ASDM セッションのアイドル タイムアウトを 500 分に設定する例を示します。

```
ciscoasa(config)# http server idle-timeout 500
```

関連コマンド

コマンド	説明
clear configure http	HTTP コンフィギュレーションを削除します。HTTP サーバーをディセーブルにし、HTTP サーバーにアクセスできるホストを削除します。
http	IP アドレスおよびサブネット マスクにより HTTP サーバーにアクセスできるホストと、そのホストの HTTP サーバーへのアクセスで経由するインターフェイスを指定します。

コマンド	説明
http authentication-certificate	ASA への HTTPS 接続を確立するユーザーの証明書による認証を要求します。
http server enable	ASDM セッション用に HTTP サーバーをイネーブルにします。
http server session-timeout	ASA に対する ASDM セッションのセッション時間を制限します。
http redirect	ASA が HTTP 接続を HTTPS にリダイレクトすることを指定します。
show running-config http	HTTP サーバーにアクセスできるホストを表示し、さらに HTTP サーバーがイネーブルであるかどうかを表示します。

http server session-timeout

ASA への ASDM 接続のセッションタイムアウトを設定するには、グローバル コンフィギュレーション モードで **http server session-timeout** コマンドを使用します。タイムアウ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。

http server session-timeout [*minutes*]
no http server session-timeout [*minutes*]

構文の説明

minutes セッション タイムアウト（1 ～ 1440 分）。

コマンド デフォルト

セッション タイムアウトはディセーブルです。ASDM 接続にセッション時間の制限はありません。

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
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

例

次に、ASDM 接続のセッション タイムアウトを 1000 分に設定する例を示します。

```
ciscoasa(config)# http server session-timeout 1000
```

関連コマンド

コマンド	説明
clear configure http	HTTP コンフィギュレーションを削除します。HTTP サーバーをディセーブルにし、HTTP サーバーにアクセスできるホストを削除します。
http	IP アドレスおよびサブネット マスクにより HTTP サーバーにアクセスできるホストと、そのホストの HTTP サーバーへのアクセスで経由するインターフェイスを指定します。

コマンド	説明
http authentication-certificate	ASA への HTTPS 接続を確立するユーザーの証明書による認証を要求します。
http server enable	ASDM セッション用に HTTP サーバーをイネーブルにします。
http server idle-timeout	ASA に対する ASDM セッションのアイドル時間を制限します。
http redirect	ASA が HTTP 接続を HTTPS にリダイレクトすることを指定します。
show running-config http	HTTP サーバーにアクセスできるホストを表示し、さらに HTTP サーバーがイネーブルであるかどうかを表示します。

https-proxy

外部プロキシサーバーを使用してHTTPS要求を処理するようにASAを設定するには、webvpnコンフィギュレーション モードで **https-proxy** コマンドを使用します。HTTPS プロキシサーバー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。

https-proxy { *host* [*port*] [**exclude** *url*] | [**username** *username* { **password** *password* }]
no https-proxy

構文の説明

ホスト	外部 HTTPS プロキシ サーバーのホスト名または IP アドレス。
password	（オプション。username を指定した場合に限り使用可能）各 HTTPS プロキシ要求にパスワードを付加して基本的なプロキシ認証を提供するには、このキーワードを入力します。
password	各 HTTPS 要求とともにプロキシ サーバーに送信されるパスワード。
port	（任意）HTTPSプロキシサーバーによって使用されるポート番号。デフォルトポートは443です。値を指定しなかった場合、ASAはこのポートを使用します。範囲は 1 ～ 65535 です。
url	プロキシ サーバーへの送信が可能な URL から除外する URL を 1 つ、または複数の URL のカンマ区切りのリストを入力します。このストリングには文字数の制限はありませんが、コマンド全体で 512 文字以下となるようにする必要があります。リテラル URL を指定するか、次のワイルドカードを使用できます。 • ***** は、スラッシュ（/）とピリオド（.）を含む任意の文字列と一致します。このワイルドカードは、英数字ストリングとともに使用する必要があります。 • **?** は、スラッシュおよびピリオドを含む、任意の 1 文字に一致します。 • [*x*-*y*] は、*x* から *y* までの範囲の任意の 1 文字と一致します。*x* は ANSI 文字セット内のある 1 文字を表し、*y* は別の 1 文字を表します。 • [**!***x*-*y*] は、範囲外の任意の 1 文字と一致します。
username	（任意）各 HTTPS プロキシ要求にユーザー名を付加して基本的なプロキシ認証を提供するには、このキーワードを入力します。
username	各 HTTPS 要求とともにプロキシ サーバーに送信されるユーザー名。

コマンド デフォルト

デフォルトでは、HTTPS プロキシ サーバーは設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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
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
7.0(1)	このコマンドが追加されました。
8.0(2)	**exclude**、**username**、および**password**キーワードが追加されました。

使用上のガイドライン

組織が管理するサーバーを経由したインターネットへのアクセスを必須にすると、セキュアなインターネットアクセスを確保して管理面の制御を保証するためのフィルタリング導入の別のきっかけにもなります。

ASA でサポートされるのは、**https-proxy** コマンドの 1 つのインスタンスだけです。このコマンドのインスタンスが実行コンフィギュレーションにすでに 1 つ存在する場合、もう 1 つインスタンスを入力すると、CLI は以前のインスタンスを上書きします。**show running-config webvpn** コマンドを入力すると、CLI によって実行コンフィギュレーション内のすべての **https-proxy** コマンドがリストされます。応答に **https-proxy** コマンドがリストされていない場合、このコマンドは存在しません。

例

次の例は、次の設定の HTTPS プロキシ サーバーの使用を設定する方法を示しています：IP アドレスが 209.165. 201.2 で、デフォルト ポートの 443 を使用しています。

```
ciscoasa
(config)#
 webvpn
ciscoasa(config-webvpn)# https-proxy 209.165.201.2
ciscoasa(config-webvpn)
```

次に、同じプロキシ サーバーを使用して、各 HTTPS 要求とともにユーザー名およびパスワードを送信するように設定する例を示します。

```
ciscoasa(config-webvpn)# https-proxy 209.165.201.2 jsmith password mysecretdonttell
ciscoasa(config-webvpn)
```

次も、同じコマンドの例を示しますが、前の例とは異なり、この例では、ASA が HTTPS 要求で www.example.com という特定の URL を受信した場合には、プロキシサーバーに渡すのではなく自分自身で要求を解決します。

```
ciscoasa(config-webvpn)# https-proxy 209.165.201.2 exclude www.example.com username
```

```
jsmith password mysecretdonttell
ciscoasa(config-webvpn)
```

次の例は、**exclude** オプションの使い方を示しています。

```
ciscoasa(config-webvpn)# https-proxy 10.1.1.1 port 8080 exclude *.com username John
pasword 12345678
ciscoasa(config-webvpn)
```

次の例は、**pac**オプションの使い方を示しています。

```
ciscoasa(config-webvpn)# https-proxy pac http://10.1.1.1/pac.js
ciscoasa(config-webvpn)
```

関連コマンド

コマンド	説明
http-proxy	外部プロキシ サーバーを使用して HTTP 要求を処理するように設定します。
show running-config webvpn	SSL VPN の実行コンフィギュレーションを、HTTP および HTTPS のプロキシ サーバーをすべて含めて表示します。

http username-from-certificate

ASDM の承認または認証を取得する証明書またはルールのフィールドを指定するには、 **http username-from-certificate** コマンドを使用します。

http username-from-certificate { < **primary-attr** > [< **secondary-attr** >] | **use-entire-name** | **use-script** } | **pre-fill-username**

構文の説明

pre-fill-username	VPN接続の場合に同じ目的で機能するトンネルグループ一般属性モードの既存の username-from-certificate コマンドを使用できるようにします。イネーブルの場合、このユーザー名は、ユーザーが入力したパスワードとともに認証に使用されます。
primary-attr	ユーザー名の取得に使用する属性を指定します。
secondary-attr	ユーザー名を取得するために、プライマリ属性とともに使用する追加の属性を指定します。
use-entire-name	DN 名全体を使用します。セカンダリ属性としては使用できません。
use-script	ASDM によって生成された LUA スクリプトを使用します。

コマンド デフォルト

このコマンドのデフォルトは、http username-from-certificate CN OU 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		
	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
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
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

次に、プライマリ属性およびセカンダリ属性の有効値と関連するキーワードの意味を示します。

属性/キーワード	定義
C	Country（国名）：2 文字の国名略語。国名コードは、ISE 3166 国名略語に準拠しています。
CN	Common Name（一般名）：人、システム、その他のエンティティの名前。セカンダリ属性としては使用できません。
DNQ	ドメイン名修飾子。
EA	電子メール アドレス
GENQ	世代修飾子
GN	名
I	Initials（イニシャル）。
L	Locality（地名）：組織が置かれている市または町。
N	名前
O	Organization（組織）：会社、団体、機関、連合、その他のエンティティの名前。
OU	組織ユニット：組織内のサブグループ（0）。
SER	Serial Number（シリアル番号）。
SN	Surname（姓）。
SP	州または都道府県：組織が置かれている州または都道府県。
T	Title（タイトル）。
UID	User Identifier（ユーザー ID）。
UPN	User Principal Name（ユーザー プリンシパル名）。

このコマンドは、webvpn をサポートしないプラットフォーム（ASA 1000v）や No Payload Encryption（NPE）がイネーブルになっているプラットフォームでは使用できません。

例

```
100/act(config)# http ?
configure mode commands/options:
  Hostname or A.B.C.D         The IP address of the host and/or network
                              authorized to access the HTTP server
  X:X:X:X::X/<0-128>          IPv6 address/prefix authorized to access the HTTP
                              server
  authentication-certificate  Request a certificate from the HTTPS client when
                              a management connection is being established
  redirect                    Redirect HTTP connections to the security gateway
```

```
                              to use HTTPS
  server                      Enable the http server required to run Device
                              Manager
  username-from-certificate   Specify fields from certificate DN to be used for
                              authorization/authentication
100/act(config)# help http
USAGE:
        [no] http {<local_ip>|<hostname>} <mask> <if_name>
        [no] http authentication-certificate <if_name>
        [no] http redirect <if_name> [<port>]
        [no] http server enable [<port>]
        [no] http username-from-certificate {<primary-attr> [<secondary-attr>] | use-
entire-name | use-script } [pre-fill-username]
        show running-config [all] http
        clear configure http
DESCRIPTION:
http            Configure HTTP server
SYNTAX:
<local_ip>      The ip address of the host and/or network authorized to
                access the device HTTP server.
<hostname>      Hostname of the host authorized to access the device
                HTTP server.
<mask>          The IP netmask to apply to <local_ip>.
                Default is 255.255.255.255.
<if_name>       Network interface name.
<port>          The decimal number or name of a TCP or UDP port.
                Default is "http" (80).
<primary-attr>  The DN from the certificate to be used as the username

<secondary-attr> Optional Secondary DN from the certificate to be used in the username
```

hw-module module allow-ip

ASA 5505 の AIP SSC に対して、管理 IP アドレスにアクセスが許可されたホストを設定するには、特権 EXEC モードで **hw-module module allow-ip** コマンドを使用します。

hw-module module 1 allow-ip *ip_address netmask*

構文の説明

1	スロット番号を指定します。これは常に 1 です。
ip_address	ホスト IP アドレスを指定します。
netmask	サブネット マスクを指定します。

コマンド デフォルト

出荷時のデフォルトのコンフィギュレーションでは、192.168.1.5 ～ 192.168.1.254 のホストが IPS モジュールの管理を許可されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

このコマンドは、SSC のステータスがアップ状態にある場合だけ有効です。

これらの設定は、ASA コンフィギュレーションではなく IPS アプリケーション コンフィギュレーションに書き込まれます。これらの設定は、**show module details** コマンドを使用して ASA から表示できます。

または、IPS アプリケーションの **setup** コマンドを使用して、この設定を IPS CLI から設定することもできます。

例

次に、SSC のホスト パラメータを設定する例を示します。

```
ciscoasa# hw-module module 1 allow-ip 209.165.201.29 255.255.255.0
```

関連コマンド

コマンド	説明
hw-module module ip	AIP SSC 管理アドレスを設定します。
show module	モジュールのステータス情報を表示します。

hw-module module ip

ASA 5505 の AIP SSC に対して、管理 IP アドレスを設定するには、特権 EXEC モードで **hw-module module ip** コマンドを使用します。

hw-module module 1 ip *ip_address netmask gateway*

構文の説明

1	スロット番号を指定します。これは常に 1 です。
gateway	ゲートウェイ IP アドレスを指定します。
ip_address	管理 IP アドレスを指定します。
netmask	サブネット マスクを指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	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
特権 EXEC	• 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

このアドレスが ASA VLAN IP アドレスと同じサブネット上にあることを確認します。たとえば、10.1.1.1 を ASA の VLAN に割り当てた場合は、そのネットワーク上の別のアドレス（10.1.1.2 など）を IPS 管理アドレスに割り当てます。

管理ステーションが、直接接続されている ASA ネットワーク上にある場合は、ゲートウェイを、IPS 管理 VLAN に割り当てられた ASA IP アドレスに設定します。上記の例では、10.1.1.1 にゲートウェイを設定します。管理ステーションがリモート ネットワーク上にある場合は、ゲートウェイを、IPS 管理 VLAN のアップストリーム ルータのアドレスに設定します。

（注） これらの設定は、ASA コンフィギュレーションではなく IPS アプリケーション コンフィギュレーションに書き込まれます。これらの設定は、**show module details** コマンドを使用して ASA から表示できます。または、IPS アプリケーションの **setup** コマンドを使用して、この設定を IPS CLI から設定することもできます。

例

次に、IPS モジュールの管理アドレスを設定する例を示します。

```
ciscoasa# hw-module module 1 ip 209.165.200.254
 255.255.255.224 209.165.200.225
```

関連コマンド

コマンド	説明
hw-module module allow-ip	AIP SSC 管理ホストのアドレスを設定します。
show module	モジュールのステータス情報を表示します。

hw-module module password-reset

ハードウェアモジュールのデフォルト管理ユーザーのパスワードをデフォルト値にリセットするには、特権 EXEC モードで **hw-module module password-reset** コマンドを使用します。

hw-module module 1 password-reset

構文の説明

1スロット番号を指定します。これは常に1です。

コマンド デフォルト

デフォルトのユーザー名とパスワードはモジュールによって異なります。

- IPS モジュール：ユーザー名：**cisco**、パスワード：**cisco**
- CSC モジュール：ユーザー名：**cisco**、パスワード：**cisco**
- ASA CX モジュール：ユーザー名：**admin**、パスワード：**Admin123**

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
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(2)	このコマンドが追加されました。
8.4(4.1)	ASA CX モジュールのサポートが追加されました。

使用上のガイドライン

このコマンドは、ハードウェア モジュールがアップ状態で、パスワード リセットがサポートされている場合にのみ有効です。IPS の場合、パスワードのリセットは、モジュールが IPS バージョン 6.0 以降を実行している場合にのみサポートされます。パスワードをリセットした後は、モジュール アプリケーションを使用してパスワードを独自の値に変更する必要があります。モジュールのパスワードをリセットすると、モジュールがリブートします。モジュールのリブート中はサービスを使用できません。リブートには数分を要する場合があります。**show module** コマンドを実行すると、モジュールの状態をモニターできます。

コマンドは、必ずプロンプトで確認を要求します。コマンドが成功した場合は、それ以上何も出力されません。コマンドが失敗した場合は、障害が発生した理由を示すエラー メッセージが表示されます。表示される可能性のあるエラー メッセージは、次のとおりです。

```
Unable to reset the password on the module in slot 1
Unable to reset the password on the module in slot 1 - unknown module state
Unable to reset the password on the module in slot 1 - no module installed
Failed to reset the password on the module in slot 1 - module not in Up state
Unable to reset the password on the module in slot 1 - unknown module type
The module in slot 1 does not support password reset
Unable to reset the password on the module in slot 1 - no application found
The SSM application version does not support password reset
Failed to reset the password on the module in slot 1
```

例

次に、スロット 1 のハードウェア モジュールのパスワードをリセットする例を示します。

```
ciscoasa(config)# hw-module module 1 password-reset
Reset the password on module in slot 1? [confirm] y
```

関連コマンド

コマンド	説明
hw-module module recover	TFTP サーバーからリカバリ イメージをロードしてモジュールを回復します。
hw-module module reload	モジュール ソフトウェアをリロードします。
hw-module module reset	モジュールハードウェアをシャットダウンしてリセットします。
hw-module module shutdown	コンフィギュレーション データを失わずに電源を切る準備をして、モジュール ソフトウェアをシャットダウンします。
show module	モジュール情報を表示します。

hw-module module recover

TFTP サーバーから取り付けモジュールにリカバリ ソフトウェア イメージをロードしたり、TFTP サーバーにアクセスするためのネットワーク設定を行ったりするには、特権 EXEC モードで **hw-module module recover** コマンドを使用します。たとえば、モジュールがローカル イメージをロードできない場合などは、このコマンドを使用したモジュールの回復が必要となる場合があります。

hw-module module 1 recover { **boot** | **stop** | **configure** [**url** *tfp_url* | **ip** *module_address* | **gateway** *gateway_ip_address* | **vlan** *vlan_id*] }

構文の説明

1	スロット番号を指定します。これは常に 1 です。
boot	このモジュールの回復を開始し、**configure** キーワード設定に従ってリカバリイメージをダウンロードします。ダウンロード後、モジュールは新しいイメージからリブートします。
configure	リカバリ イメージをダウンロードするためのネットワーク パラメータを設定します。**configure** キーワードの後にネットワークパラメータを入力しなかった場合、すべてのパラメータの入力を求めるプロンプトが表示されます。このコマンドを実行すると、TFTP サーバーの URL、管理インターフェイスの IP アドレスとネットマスク、ゲートウェイ アドレス、および VLAN ID の入力を求めるプロンプトが表示されます。これらのネットワーク パラメータは ROMMON で設定されます。モジュール アプリケーション コンフィギュレーションで設定したネットワーク パラメータは ROMMON には使用できないため、ここで別個に設定する必要があります。
gateway *gateway_ip_address*	（任意）SSM 管理インターフェイスを介して TFTP サーバーにアクセスするためのゲートウェイ IP アドレス。
ip *module_address*	（オプション）モジュール管理インターフェイスの IP アドレス。
stop	リカバリ アクションを停止し、リカバリ イメージのダウンロードを停止します。モジュールは、元のイメージからブートします。このコマンドは、**hw-module module recover boot** コマンドを使用して回復を開始してから 30 ～ 45 秒以内に入力する必要があります。この期間が経過した後で **stop** コマンドを入力すると、モジュールが無応答になるなど、予期しない結果になることがあります。
url *tfp_url*	（任意）TFTP サーバー上のイメージの URL。次の形式で指定します。 **tftp:**//*server*/[*path*/]*filename*
vlan *vlan_id*	（オプション）管理インターフェイスの VLAN ID を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	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
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
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

モジュールに障害が発生して、モジュールアプリケーションイメージを実行できない場合は、TFTP サーバーからモジュール上に新しいイメージを再インストールできます。

（注） モジュールソフトウェア内部では、イメージをインストールするために **upgrade** コマンドを使用しないでください。

指定する TFTP サーバーが、最大 60 MB のサイズのファイルを転送できることを確認してください。ネットワークとイメージのサイズに応じて、このプロセスは完了までに約 15 分間かかることがあります。

このコマンドは、モジュールがアップ、ダウン、無応答、または回復のいずれかの状態である場合にのみ使用可能です。ステート情報については、**show module** コマンドを参照してください。

show module 1 recover コマンドを使用してリカバリ コンフィギュレーションを表示できます。

（注） このコマンドは、ASA CX、ASA FirePOWER モジュールではサポートされていません。

例

次に、TFTP サーバーからイメージをダウンロードするようにモジュールを設定する例を示します。

```
ciscoasa# hw-module module 1 recover configure
Image URL [tftp://127.0.0.1/myimage]: tftp://10.1.1.1/ids-newimg
Port IP Address [127.0.0.2]: 10.1.2.10
Port Mask [255.255.255.254]: 255.255.255.0
Gateway IP Address [1.1.2.10]: 10.1.2.254
VLAN ID [0]: 100
```

次に、モジュールを回復する例を示します。

```
ciscoasa# hw-module module 1 recover boot
The module in slot 1 will be recovered.  This may
erase all configuration and all data on that device and
attempt to download a new image for it.
Recover module in slot 1? [confirm]
```

関連コマンド

コマンド	説明
debug module-boot	モジュールのブート プロセスに関するデバッグ メッセージを表示します。
hw-module module reset	モジュールをシャットダウンし、ハードウェア リセットを実行します。
hw-module module reload	モジュール ソフトウェアをリロードします。
hw-module module shutdown	コンフィギュレーション データを失わずに電源を切る準備をして、モジュール ソフトウェアをシャットダウンします。
show module	モジュール情報を表示します。

hw-module module recover（ASA 5506W-X）

デフォルト設定をロードまたは回復する、あるいはROMMONにアクセスして新しいイメージを ASA 5506W-X のワイヤレスアクセスポイントにロードするには、特権 EXEC モードで **hw-module module recover** コマンドを使用します。

hw-module module wlan recover [**configuration** | **image**]

構文の説明

configuration	ワイヤレス アクセス ポイントを工場出荷時のデフォルト設定にリセットします。
image	ROMMON にアクセスし、TFTP アップグレード プロシージャを実行できるモジュール コンソールへのセッション。

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		
	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
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

バックプレーン上のアクセスポイント CLI に対する **image** キーワードセッション。アクセスポイントをリロードします。アクセスポイントが起動している場合は、起動プロセスをエスケープして ROMMON にアクセスし、TFTP イメージをダウンロードできます。詳しい手順については、[アクセスポイントのイメージのリロード（Reloading the Access Point Image）] > [CLIの使用（Using the CLI）] を参照してください。

例

次に、アクセス ポイント上でイメージを回復する例を示します。

```
ciscoasa# hw-module module wlan recover image
WARNING: Image recovery cannot be carried out via CLI command on this module.
Do you want to reset the module and session into the module console to carry out the
image recovery?[confirm]
Resetting the module and sessioning into the module console
```

関連コマンド

コマンド	説明
hw-module module wlan reset	モジュールをシャットダウンし、ハードウェア リセットを実行します。

hw-module module reload

物理モジュールのモジュールソフトウェアをリロードするには、特権EXECモードで**hw-module module reload** コマンドを使用します。

hw-module module 1 reload

構文の説明

1スロット番号を指定します。これは常に1です。

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		
	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
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.4(4.1)	ASA CX モジュールのサポートが追加されました。
9.2(1)	ASA FirePOWER モジュールのサポートが追加されました。

使用上のガイドライン

このコマンドは、モジュールをリロードする前にハードウェアリセットを実行する **hw-module module reset** コマンドとは異なります。

このコマンドは、モジュールのステータスがアップ状態にある場合だけ有効です。ステート情報については、 **show module** コマンドを参照してください。

例

次に、スロット 1 のモジュールをリロードする例を示します。

```
ciscoasa# hw-module module 1 reload
Reload module in slot 1? [confirm] y
Reload issued for module in slot 1
%XXX-5-505002: Module in slot 1 is reloading. Please wait...
%XXX-5-505006: Module in slot 1 is Up.
```

関連コマンド

コマンド	説明
debug module-boot	モジュールのブート プロセスに関するデバッグ メッセージを表示します。
hw-module module recover	TFTP サーバーからリカバリ イメージをロードしてモジュールを回復します。
hw-module module reset	モジュールをシャットダウンし、ハードウェア リセットを実行します。
hw-module module shutdown	コンフィギュレーション データを失わずに電源を切る準備をして、モジュール ソフトウェアをシャットダウンします。
show module	モジュール情報を表示します。

hw-module module reset

モジュールをリセットしてからモジュールソフトウェアをリロードするには、特権EXECモードで **hw-module module reset** コマンドを使用します。

hw-module module { **1** | **wlan** } **reset**

構文の説明

1	スロット番号を指定します。これは常に 1 です。
wlan	ASA 5506W-X の場合は、ワイヤレス アクセス ポイントを指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	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
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.4(4.1)	ASA CX モジュールのサポートが追加されました。
9.2(1)	ASA FirePOWER モジュールのサポートが追加されました。
9.4(1)	**wlan** キーワードが追加されました。

使用上のガイドライン

モジュールがアップ状態の場合、**hw-module module reset** コマンドによって、リセットの前にソフトウェアをシャットダウンするように要求されます。

hw-module module recover コマンドを使用してモジュールを回復できます（サポートされている場合）。モジュールが回復状態になっているときに **hw-module module reset** コマンドを入力しても、モジュールは回復プロセスを中断しません。**hw-module module reset** コマンドによって、モジュールのハードウェアリセットが実行され、ハードウェアのリセット後にモジュールのリカバリが続行されます。モジュールがハングした場合は、回復中にモジュールをリセットできます。ハードウェア リセットによって、問題が解決することもあります。

このコマンドは、ソフトウェアのリロードのみを行いハードウェアリセットは行わない **hw-module module reload** コマンドとは異なります。

このコマンドは、モジュールのステータスがアップ、ダウン、無応答、または回復のいずれかの場合にのみ有効です。ステート情報については、**show module** コマンドを参照してください。

例

次に、アップ状態になっているスロット1のモジュールをリセットする例を示します。

```
ciscoasa# hw-module module 1 reset
The module in slot 1 should be shut down before
resetting it or loss of configuration may occur.
Reset module in slot 1? [confirm] y
Reset issued for module in slot 1
%XXX-5-505001: Module in slot 1 is shutting down.  Please wait...
%XXX-5-505004: Module in slot 1 shutdown is complete.
%XXX-5-505003: Module in slot 1 is resetting. Please wait...
%XXX-5-505006: Module in slot 1 is Up.
```

関連コマンド

コマンド	説明
debug module-boot	モジュールのブート プロセスに関するデバッグ メッセージを表示します。
hw-module module recover	TFTP サーバーからリカバリ イメージをロードしてモジュールを回復します。
hw-module module reload	モジュール ソフトウェアをリロードします。
hw-module module shutdown	コンフィギュレーション データを失わずに電源を切る準備をして、モジュール ソフトウェアをシャットダウンします。
show module	モジュール情報を表示します。

hw-module module shutdown

モジュールソフトウェアをシャットダウンするには、特権 EXEC モードで **hw-module module shutdown** コマンドを使用します。

hw-module module 1 shutdown

構文の説明

1	スロット番号を指定します。これは常に 1 です。

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		
	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
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.4(4.1)	ASA CX モジュールのサポートが追加されました。
9.2(1)	ASA FirePOWER モジュールのサポートが追加されました。

使用上のガイドライン

モジュール ソフトウェアをシャットダウンするのは、コンフィギュレーション データを失うことなく安全にモジュールの電源をオフにできるように準備するためです。

このコマンドは、モジュール ステータスがアップまたは無応答である場合にのみ有効です。ステート情報については、**show module** コマンドを参照してください。

例

次に、スロット 1 のモジュールをシャットダウンする例を示します。

```
ciscoasa# hw-module module 1 shutdown
Shutdown module in slot 1? [confirm] y
Shutdown issued for module in slot 1
ciscoasa#
%XXX-5-505001: Module in slot 1 is shutting down.  Please wait...
%XXX-5-505004: Module in slot 1 shutdown is complete.
```

関連コマンド

コマンド	説明
debug module-boot	モジュールのブート プロセスに関するデバッグ メッセージを表示します。
hw-module module recover	TFTP サーバーからリカバリ イメージをロードしてモジュールを回復します。
hw-module module reload	モジュール ソフトウェアをリロードします。
hw-module module reset	モジュールをシャットダウンし、ハードウェア リセットを実行します。
show module	モジュール情報を表示します。

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