fe – fz

feature

スマートライセンス機能権限付与を要求するには、ライセンス スマート コンフィギュレーション モードで **feature** コマンドを使用します。この機能を削除するには、このコマンドの **no** 形式を使用します。

（注） このコマンドは、ASA 仮想 およびシャーシでのみサポートされています。

feature { **tier standard** | **strong-encryption** | **context** *number* | **mobile-sp** | **carrier** }
no feature { **tier standard** | **strong-encryption** | **context** *number* | **mobile-sp** | **carrier** }

構文の説明

carrier	キャリア（GTP/GPRS、Diameter、SCTP、M3UA）ライセンスを要求します。このライセンスは、モバイル SP ライセンスを置き換えます。
context *number*	（シャーシのみ）セキュリティコンテキストのライセンスを要求します。標準ライセンスに含まれるデフォルトのコンテキストの数は差し引いてください。たとえば、ご使用のモデルが 250 のコンテキストをサポートしており、デフォルトのコンテキストの数が 10 の場合、要求するコンテキストの数は 240 までにする必要があります。
mobile-sp	（FirePOWER 9300/4100 のみ）モバイル SP（GTP/GPRS）ライセンスを要求します。このライセンスは、Version 9.5(2) のキャリア ライセンスに置き換えられて廃止されました。
strong-encryption	（シャーシのみ）高度暗号化（3DES）ライセンスを要求します。FXOS 1.1.3 以降では、対象となるお客様がデバイスを登録すると、高度暗号化ライセンスが自動的に有効になります。このコマンドを使用する必要があるのは、2.3.0 より前のスマート ソフトウェア マネージャ サテライトのユーザーだけです。
tier standard	使用可能なオプションは標準層だけです。

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
ライセンス スマート 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
9.3(2)	このコマンドが追加されました。
9.4(1.152)	Firepower 9300 ASA セキュリティモジュールのサポートと、キーワード **strong-encryption**、**mobile-sp**、および **context** が追加されました。
9.5(2)	**mobile-sp** キーワードが **carrier** キーワードに置き換えられています。**strong-encryption** キーワードが廃止されました（2.3.0 より前のスマート ソフトウェア マネージャ サテライトのユーザーを除く）。
9.6(1)	Firepower 4100 シリーズのサポートが追加されました。
9.8(2)	Firepower 2100 シリーズのサポートが追加されました。
9.18(1)	Cisco Secure Firewall 3100 のサポート（キャリアライセンスを含む）が追加されました。

使用上のガイドライン

ASA仮想の場合、初めて機能層を要求するときに、変更を有効にするためにライセンス スマート コンフィギュレーション モードを終了する必要があります。シスコ ライセンス認証局で認可された後で機能層を変更した場合、変更を有効にするために ASA 仮想 をリロードする必要があります。

例

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

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

関連コマンド

コマンド	説明
call-home	Smart Call Home を設定します。スマート ライセンスでは、Smart Call Home インフラストラクチャが使用されます。

コマンド	説明
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。

fec

25 Gbps 以上のインターフェイスに前方誤り訂正（FEC）を設定するには、インターフェイス コンフィギュレーション モードで **fec** コマンドを使用します。FEC 設定をデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

（注） このコマンドは、Cisco Secure Firewall 3100 でのみサポートされています。

fec { **auto** | **cl108-rs** | **cl74-fc** | **disable** }
no fec { **auto** | **cl108-rs** | **cl74-fc** | **disable** }

構文の説明

auto	SFP タイプに基づいて FEC 設定を自動検出します。
cl108-rs	FEC モードを Clause 108 RS-FEC に設定します。
cl74-fc	FEC モードを Clause 74 FC-FEC に設定します。
disable	FEC を無効にします。

コマンド デフォルト

デフォルト設定は**auto**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	—	• 対応

コマンド履歴

リリース	変更内容
9.17(1)	このコマンドは、Cisco Secure Firewall 3100 に導入されました。

使用上のガイドライン

FEC は物理インターフェイスでのみ設定します。FEC は EtherChannel メンバーインターフェイスに設定してから、EtherChannel に追加する必要があります。

例

次に、FEC を cl74-fc に設定する例を示します。

```
ciscoasa(config)# interface ethernet1/5
ciscoasa(config-if)# fec cl74-fc
```

関連コマンド

コマンド	説明
clear configure interface	インターフェイスのコンフィギュレーションをすべてクリアします。
duplex	デュプレックス モードを設定します。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。
show running-config interface	インターフェイス コンフィギュレーションを表示します。
speed	インターフェイスの速度を設定します。

file-bookmarks

認証された WebVPN ユーザーに表示される WebVPN ホームページの [ファイルブックマーク（File Bookmarks）] タイトルまたは [ファイルブックマーク（File Bookmarks）] リンク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 **file-bookmarks** 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。

file-bookmarks { **link** { **style** *value* } | **title** { **style** *value* | **text** *value* } }
no file-bookmarks { **link** { **style** *value* } | **title** { **style** *value* | **text** *value* } }

構文の説明

link	リンクへの変更を指定します。
title	タイトルへの変更を指定します。
style	HTML スタイルへの変更を指定します。
text	テキストへの変更を指定します。
value	表示する実際のテキストまたは CSS パラメータ（最大 256 文字）。

コマンド デフォルト

デフォルトのリンクのスタイルは color:#669999;border-bottom: 1px solid #669999;text-decoration:none です。

デフォルトのタイトルのスタイルは color:#669999;background-color:#99CCCC;font-weight:bold です。

デフォルトのタイトル テキストは「File Folder Bookmarks」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、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、[File Bookmarks] タイトルを「Corporate File Bookmarks」にカスタマイズする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# file-bookmarks title text Corporate File Bookmarks
```

関連コマンド

コマンド	説明
application-access	WebVPN ホームページの [Application Access] ボックスをカスタマイズします。
browse-networks	WebVPN ホームページの [Browse Networks] ボックスをカスタマイズします。
web-applications	WebVPN ホームページの [Web Application] ボックスをカスタマイズします。
web-bookmarks	WebVPN ホームページの [Web Bookmarks] タイトルまたはリンクをカスタマイズします。

file-browsing

ファイルサーバーまたは共有の CIFS または FTP によるファイルブラウジ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 **file-browsing** コマンドを使用します。

file-browsing enable | **disable**

構文の説明

enable | **disable**	ファイル サーバーまたは共有のブラウズ機能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

ファイル ブラウジングには、次の使用上の注意事項があります。

- ファイル ブラウジングでは、国際化はサポートされていません。
- ブラウズには、NBNS（マスター ブラウザまたは WINS）が必要です。NBNS に障害が発生した場合や、NBNS が設定されていない場合は、DNS を使用します。

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 モードでファイルブラウジングをディセーブルにした場合、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 **file-browsing** 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 DAP レコードでファイル ブラウジングをイネーブルにする例を示します。

```
ciscoasa
 (config)# config-dynamic-access-policy-record
Finance
ciscoasa
(config-dynamic-access-policy-record)#
 webvpn
ciscoasa
(config-dap-webvpn)#
 file-browsing 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。
file-entry	アクセス先のファイル サーバーの名前を入力する機能をイ ネーブルまたはディセーブルにします。

file-encoding

Common Internet File System サーバーからのページの文字エンコーディングを指定するには、webvpn コンフィギュレーション モードで **file-encoding** コマンドを使用します。file-encoding 属性の値を削除するには、このコマンドの **no** 形式を使用します。

file-encoding { **server-name** | **server-ip-addr** } *charset*
no file-encoding { **server-name** | **server-ip-addr** }

構文の説明

charset	最大 40 文字から成るストリングで、http://www.iana.org/assignments/character-sets で特定されている有効な文字セットのいずれかに相当するもの。このページに示されている文字セットの名前またはエイリアスのいずれかを使用できます。たとえば、iso-8859-1、shift_jis、ibm850 などです。 この文字列は、大文字と小文字が区別されません。ASA 設定内では、コマンド インタープリタによって大文字が小文字に変換されます。
server-ip-addr	文字エンコーディングを指定する CIFS サーバーの IP アドレス（ドット付き 10 進表記）。
server-name	文字エンコーディングを指定する CIFS サーバーの名前。 ASA では、指定した大文字と小文字の区別が保持されますが、名前をサーバーと照合するときには大文字と小文字は区別されません。

コマンド デフォルト

WebVPN コンフィギュレーションに明示的な file-encoding エントリがないすべての CIFS サーバーからのページでは、character-encoding 属性の文字エンコーディング値が継承されます。

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
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 文字エンコーディング属性の値とは異なる文字エンコーディング エントリが必要なすべての CIFS サーバーに対して、ファイル エンコーディング エントリを入力します。

CIFS サーバーから WebVPN ユーザーにダウンロードされた WebVPN ポータル ページは、サーバーを識別する WebVPN ファイル エンコーディング属性の値を符号化します。符号化が行われなかった場合は、文字エンコーディング属性の値を継承します。リモートユーザーのブラウザでは、ブラウザの文字エンコードセットのエントリにこの値がマップされ、使用する正しい文字セットが決定されます。WebVPN コンフィギュレーションで CIFS サーバー用の file-encoding エントリが指定されず、character-encoding 属性も設定されていない場合、WebVPN ポータル ページは値を指定しません。WebVPN ポータル ページが文字エンコーディングを指定しない場合、またはブラウザがサポートしていない文字エンコーディング値を指定した場合、リモート ブラウザはブラウザ自体のデフォルト エンコーディングを使用します。

CIFS サーバーに適切な文字エンコーディングを、広域的には webvpn 文字エンコーディング属性によって、個別的にはファイルエンコーディングの上書きによってマッピングすることで、ページと同様にファイル名やディレクトリ パスを正しくレンダリングすることが必要な場合には、CIFS ページの正確な処理と表示が可能になります。

（注） 文字エンコーディングおよびファイル エンコーディングの値は、ブラウザによって使用されるフォント ファミリを排除するものではありません。次の例に示すように日本語の Shift_JIS 文字エンコーディングを使用する場合などは、webvpn カスタマイゼーション コマンド モードで **page style** コマンドを使用してフォントファミリを置換し、これらの値の設定を補足するか、または webvpn カスタマイゼーション コマンド モードで **no page style** コマンドを入力してフォントファミリを削除する必要があります。

例

次の例では、「CISCO-server-jp」という名前の CIFS サーバーが日本語の Shift_JIS 文字をサポートするようにファイルエンコーディング属性を設定し、フォントファミリを削除して、デフォルトの背景色を保持しています。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# file-encoding CISCO-server-jp shift_jis
ciscoasa(config-webvpn)# customization DfltCustomization
ciscoasa(config-webvpn-custom)# page style background-color:white
ciscoasa(config-webvpn-custom)#
```

次に、CIFS サーバー 10.86.5.174 のファイルエンコーディング属性を設定して、IBM860（エイリアス「CP860」）文字をサポートする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# file-encoding 10.86.5.174 cp860
ciscoasa(config-webvpn)
```

関連コマンド

コマンド	説明
character-encoding	WebVPN コンフィギュレーションのファイル エンコーディング エントリに指定されたサーバーのページを除き、すべての WebVPN ポータル ページで使用されるグローバルな文字エンコーディングを指定します。
show running-config webvpn	WebVPN の実行コンフィギュレーションを表示します。デフォルト コンフィギュレーションを組み込むには **all** キーワードを使用します。
debug webvpn cifs	Common Internet File System についてのデバッグ メッセージを表示します。

file-entry

アクセスするファイルサーバー名をユーザーが入力できる機能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 **file-entry** コマンドを使用します。

file-entry enable | **disable**

構文の説明

enable | **disable**	アクセス先のファイルサーバーの名前を入力する機能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、次の階層に従って、さまざまなソースから属性値を適用できます。

1. DAP レコード
2. ユーザー名
3. グループ ポリシー
4. 接続プロファイル（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

属性の DAP 値には、ユーザー、グループ ポリシー、または接続プロファイルよりも高いプライオリティが設定されています。

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 モードでファイル入力をディセー

ブルにした場合、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 **file-entry** 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 DAP レコードでファイル サーバー名の入力をイネーブルにする例を示します。

```
ciscoasa
 (config)#
config-dynamic-access-policy-record
Finance
ciscoasa
(config-dynamic-access-policy-record)#
 webvpn
ciscoasa
(config-dap-webvpn)#
 file-entry 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。
file-browsing	ファイル サーバーまたは共有のブラウズ機能をイネーブルまたはディセーブルにします。

filter

特定のグループポリシーまたはユーザー名の WebVPN 接続で使用するアクセスリストの名前を指定するには、webvpn コンフィギュレーション モードで **filter** コマンドを使用します。アクセス リ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。

filter { **value** *ACLname* | **none** }
no filter

構文の説明

none	WebVPN タイプのアクセス リストがないことを示します。ヌル値を設定して、アクセス リストを使用できないようにします。アクセス リストを他のグループ ポリシーから継承しないようにします。
value *ACLname*	事前に設定済みのアクセス リストの名前を指定します。

コマンド デフォルト

WebVPN アクセスリストは、**filter** コマンドを使用してアクセスリストを指定するまでは適用されません。

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	—	—	• 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

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。値が継承されないようにするには、**filter value none** コマンドを使用します。

このユーザーまたはグループポリシーに対する、さまざまなタイプのトラフィックを許可または拒否するには、ACL を設定します。その後、**filter** コマンドを使用して、これらの WebVPN トラフィック用の ACL を適用します。

WebVPN では、**vpn-filter** コマンドで定義された ACL は使用されません。

例

次に、FirstGroup という名前のグループ ポリシーで *acl_in* という名前のアクセス リストを呼び出すフィルタ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)# filter acl_in
```

関連コマンド

コマンド	説明
access-list	アクセス リストを作成するか、ダウンロード可能なアクセス リストを使用します。
webvpn	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 モードで使用します。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。

filter activex

ASA を通過する HTTP トラフィック内の ActiveX オブジェクトを削除するには、グローバル コンフィギュレーション モードで filter activex 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。

filter activex *port*［ *-port* ］| **except** *local_ip* **mask** *foreign_ip foreign_mask*
no filter activex *port*［ *-port* ］| **except** *local_ip* **mask** *foreign_ip foreign_mask*

構文の説明

except	先行の filter 条件に対する例外を作成します。
foreign_ip	セキュリティ レベルが最も低い、アクセスが要求されているインターフェイスの IP アドレス。0.0.0.0（短縮形は 0）を使用すると、すべてのホストを指定できます。
foreign_mask	foreign_ip 引数のネットワーク マスク。常に特定のマスク値を指定します。0.0.0.0（短縮形は 0）を使用すると、すべてのホストを指定できます。
local_ip	セキュリティ レベルが最も高い、アクセスが要求されているインターフェイスの IP アドレス。このアドレスに 0.0.0.0（短縮形は 0）を設定すると、すべてのホストを指定できます。
mask	*local_ip* 引数のネットワーク マスク。0.0.0.0（短縮形は 0）を使用すると、すべてのホストを指定できます。
port	フィルタリングが適用される TCP ポート。一般的に、これはポート 21 ですが、他の値も受け入れられます。ポート 21 の代わりに、http または url リテラルを使用できます。指定できる値の範囲は、0 ～ 65535 です。
-port	（任意）ポート範囲を指定します。

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
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)	このコマンドが追加されました。

使用上のガイドライン

ActiveX オブジェクトには、保護されているネットワーク上のホストやサーバーを攻撃することを目的とするコードが含まれている場合があるため、セキュリティのリスクが発生する可能性があります。**activex** コマンドを使用して、ActiveX オブジェクトをディセーブルにできます。

ActiveX コントロール（旧称：OLE コントロールまたは OCX コントロール）は、Web ページやその他のアプリケーションに挿入できるコンポーネントです。これらのコントロールにはカスタム フォームやカレンダーなど、情報の収集と表示に使用されるサードパーティ製の多様なフォームが含まれています。ActiveX は、技術的に、ネットワーク クライアントに対して多くの問題を発生させる可能性があります。たとえば、ワークステーションの障害の原因となる、ネットワーク セキュリティ問題を引き起こす、またはサーバーへの攻撃に利用される、などのおそれがあります。

filter **activex**コマンドは、HTML Web ページ内でコメントアウトすることで、HTML**object** コマンドをブロックします。HTML ファイルの ActiveX フィルタリングは、<applet> および </applet> タグと <object classid> および </object> タグを選択的にコメントに置換することによって実行されます。ネストされたタグのフィルタリングは、最上位タグをコメントに変換することによってサポートされています。

⚠

注意 事前定義済みの <object> タグは、Java アプレット、画像ファイル、およびマルチメディア オブジェクトにも使用されます。この場合、これらもこのコマンドによってブロックされます。

[システム名（System Name）] が空白の場合は、 <object> または </object> HTML タグが複数のネットワークパケットに分割されている場合や、タグ内のコードが MTU のバイト数よりも長い場合は、ASA でタグをブロックできません。

alias コマンドによって参照されている IP アドレスにユーザーがアクセスした場合、または WebVPN トラフィックでは、ActiveX ブロッキングは行われません。

例

次に、すべての発信接続で ActiveX オブジェクトをブロックする例を示します。

```
ciscoasa(config)# filter activex 80 0 0 0 0
```

このコマンドは、任意のローカル ホストから任意の外部ホストへの接続において、ポート 80 で Web トラフィックに対して ActiveX オブジェクト ブロッキングを適用することを指定します。

関連コマンド

コマンド	説明
filter url	トラフィックを URL フィルタリング サーバーに送ります。
filter java	ASA を通過する HTTP トラフィックから Java アプレットを削除します。
show running-config filter	フィルタリング コンフィギュレーションを表示します。
url-block	フィルタリング サーバーからのフィルタリング決定を待っている間、Web サーバーの応答に使用される URL バッファを管理します。
url-server	filter コマンドで使用する N2H2 サーバーまたは Websense サーバーを指定します。

filter ftp

Websense サーバーまたは N2H2 サーバーでフィルタリングする FTP トラフィックを指定するには、グローバル コンフィギュレーション モードで filter **ftp** 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。

filter ftp *port*［ *-port* ］**except** *local_ip mask foreign_ip foreign_mask*［ **allow** ］［ **interact-block** ］
no filter ftp *port*［ *-port* ］**except** *local_ip mask foreign_ip foreign_mask*［ **allow** ］［ **interact-block** ］

構文の説明

allow	（任意）サーバーが利用できない場合に、フィルタリングなしで発信接続が ASA を通過します。このオプションを省略した場合、および N2H2 サーバーまたは Websense サーバーがオフラインの場合、ASA は、N2H2 サーバーまたは Websense サーバーがオンラインに戻るまで、発信ポート 80（Web）トラフィックを停止します。
except	先行の filter 条件に対する例外を作成します。
foreign_ip	セキュリティ レベルが最も低い、アクセスが要求されているインターフェイスの IP アドレス。0.0.0.0（短縮形は 0）を使用すると、すべてのホストを指定できます。
foreign_mask	foreign_ip 引数のネットワーク マスク。常に特定のマスク値を指定します。0.0.0.0（短縮形は 0）を使用すると、すべてのホストを指定できます。
interact-block	（任意）ユーザーが対話形式の FTP プログラムを使用して FTP サーバーに接続することを禁止します。
local_ip	セキュリティ レベルが最も高い、アクセスが要求されているインターフェイスの IP アドレス。このアドレスに 0.0.0.0（短縮形は 0）を設定すると、すべてのホストを指定できます。
mask	*local_ip* 引数のネットワーク マスク。0.0.0.0（短縮形は 0）を使用すると、すべてのホストを指定できます。
port	フィルタリングが適用される TCP ポート。一般的に、これはポート 21 ですが、他の値も受け入れられます。ポート 80 の代わりに、ftp リテラルを使用できます。
-port	（任意）ポート範囲を指定します。

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
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)	このコマンドが追加されました。

使用上のガイドライン

filter ftp コマンドを使用すると、Websense サーバーまたは N2H2 サーバーでフィルタリングする FTP トラフィックを指定できます。

この機能をイネーブルにした後、ユーザーがサーバーに対して FTP GET 要求を発行すると、ASA は、FTP サーバー、および Websense サーバーまたは N2H2 サーバーに対して同時に要求を送信します。Websense サーバーまたは N2H2 サーバーによって接続が許可されると、ASA は成功の FTP リターンコードを変更しないでそのままユーザーに返します。たとえば、成功の戻りコードは「250: CWD command successful.」です。

Websense サーバーまたは N2H2 サーバーによって接続が拒否されると、ASA は FTP リターンコードを変更して、接続が拒否されたことを示します。たとえば、ASA はコード 250 を「550 Requested file is prohibited by URL filtering policy」に変更します。Websense は FTP PUT コマンドのみをフィルタリングし、PUT コマンドのフィルタリングは行いません。

完全なディレクトリ パスを指定しない対話形式の FTP セッションを禁止するには、interactive-block オプションを使用します。対話形式の FTP クライアントを使用すると、ユーザーは、完全なパスを入力しないでディレクトリを変更できます。たとえば、ユーザーは、cd /public/files ではなく、cd ./files と入力できます。これらのコマンドを使用する前に、URL フィルタリング サーバーを指定してイネーブルにする必要があります。

例

次に、FTP フィルタリングをイネーブルにする例を示します。

```
ciscoasa(config)# url-server (perimeter) host 10.0.1.1
ciscoasa(config)# filter ftp 21 0 0 0 0
ciscoasa(config)# filter ftp except 10.0.2.54 255.255.255.255 0 0
```

関連コマンド

コマンド	説明
filter https	Websense サーバーまたは N2H2 サーバーによってフィルタリングされる HTTPS トラフィックを指定します。

コマンド	説明
filter java	ASA を通過する HTTP トラフィックから Java アプレットを削除します。
filter url	トラフィックを URL フィルタリング サーバーに送ります。
show running-config filter	フィルタリング コンフィギュレーションを表示します。
url-block	フィルタリング サーバーからのフィルタリング決定を待っている間、Web サーバーの応答に使用される URL バッファを管理します。
url-server	filter コマンドで使用する N2H2 サーバーまたは Websense サーバーを指定します。

filter https

N2H2 サーバーまたは Websense サーバーでフィルタリングする HTTPS トラフィックを指定するには、グローバル コンフィギュレーション モードで filter **https** 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。

filter https *port* [*-port*] | **except** *local_ip* **mask** *foreign_ip* [**allow**]
no filter https *port* [*-port*] | **except** *local_ip* **mask** *foreign_ip* [**allow**]

構文の説明

allow	（任意）サーバーが利用できない場合に、フィルタリングなしで発信接続が ASA を通過します。このオプションを省略した場合に、N2H2 サーバーまたは Websense サーバーがオフラインになると、ASA は、N2H2 サーバーまたは Websense サーバーが再度オンラインになるまで、ポート 443 への発信トラフィックを停止します。
except	（オプション）先行の filter 条件に対する例外を作成します。
foreign_ip	セキュリティ レベルが最も低い、アクセスが要求されているインターフェイスの IP アドレス。0.0.0.0（短縮形は 0）を使用すると、すべてのホストを指定できます。
foreign_mask	foreign_ip 引数のネットワーク マスク。常に特定のマスク値を指定します。0.0.0.0（短縮形は 0）を使用すると、すべてのホストを指定できます。
local_ip	セキュリティ レベルが最も高い、アクセスが要求されているインターフェイスの IP アドレス。このアドレスに 0.0.0.0（短縮形は 0）を設定すると、すべてのホストを指定できます。
mask	*local_ip* 引数のネットワーク マスク。0.0.0.0（短縮形は 0）を使用すると、すべてのホストを指定できます。
port	フィルタリングが適用される TCP ポート。一般的に、これはポート 443 ですが、他の値でも受け入れられます。ポート 443 の代わりに、https リテラルを使用できます。
-port	（任意）ポート範囲を指定します。

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
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)	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、外部の Websense または N2H2 フィルタリングサーバーを使用した HTTPS サイトおよび FTP サイトのフィルタリングをサポートしています。

サイトが許可されない場合、SSL 接続ネゴシエーションを完了させないことによって、HTTPS フィルタリングが行われます。ブラウザに、「The Page or the content cannot be displayed.」のようなエラー メッセージが表示されます。

HTTPS コンテンツは暗号化されているため、ASA は、ディレクトリおよびファイル名の情報を付けずに URL ルックアップを送信します。

例

次に、10.0.2.54 ホストからの接続を除く、すべての発信 HTTPS 接続をフィルタリングする例を示します。

```
ciscoasa(config)# url-server (perimeter) host 10.0.1.1
ciscoasa(config)# filter https 443 0 0 0 0
ciscoasa(config)# filter https except 10.0.2.54 255.255.255.255 0 0
```

関連コマンド

コマンド	説明
filter activex	ASA を通過する HTTP トラフィックから ActiveX オブジェクトを削除します。
filter java	ASA を通過する HTTP トラフィックから Java アプレットを削除します。
filter url	トラフィックを URL フィルタリング サーバーに送ります。
show running-config filter	フィルタリング コンフィギュレーションを表示します。
url-block	フィルタリング サーバーからのフィルタリング決定を待っている間、Web サーバーの応答に使用される URL バッファを管理します。

コマンド	説明
url-server	filter コマンドで使用する N2H2 サーバーまたは Websense サーバーを指定します。

filter java

ASA を通過する HTTP トラフィックから Java アプレットを削除するには、グローバル コンフィギュレーション モードで filter **java** 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。

filter java { [*port* [- *port*] | **except** } *local_ip local_mask foreign_ip foreign_mask*]
no filter java { [*port* [- *port*] | **except** } *local_ip local_mask foreign_ip foreign_mask*]

構文の説明

except	（オプション）先行の filter 条件に対する例外を作成します。
foreign_ip	セキュリティ レベルが最も低い、アクセスが要求されているインターフェイスの IP アドレス。0.0.0.0（短縮形は 0）を使用すると、すべてのホストを指定できます。
foreign_mask	foreign_ip 引数のネットワーク マスク。常に特定のマスク値を指定します。0.0.0.0（短縮形は 0）を使用すると、すべてのホストを指定できます。
local_ip	セキュリティ レベルが最も高い、アクセスが要求されているインターフェイスの IP アドレス。このアドレスに 0.0.0.0（短縮形は 0）を設定すると、すべてのホストを指定できます。
local_mask	*local_ip* 引数のネットワーク マスク。0.0.0.0（短縮形は 0）を使用すると、すべてのホストを指定できます。
port	フィルタリングが適用される TCP ポート。一般的に、これはポート 80 ですが、他の値でも受け入れられます。ポート 80 には http または url リテラルを使用できます。
port-port	（任意）ポート範囲を指定します。

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
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)	このコマンドが追加されました。

使用上のガイドライン

Javaアプレットは、保護されたネットワーク上のホストとサーバーを攻撃するコードを含むことがあるため、セキュリティリスクを引き起こす可能性があります。Javaアプレットは、filter java コマンドで取り除くことができます。

filter java コマンドは、発信接続から ASA に返される Java アプレットをフィルタリングします。フィルタリングされてもユーザーは HTML ページを受信できますが、アプレットの Web ページ ソースはコメントアウトされているため、アプレットは実行できません。**filter java** コマンドでは、WebVPN トラフィックはフィルタリングされません。

<applet> または </applet> HTML タグが複数のネットワークパケットに分割されている場合や、タグ内のコードが MTU のバイト数よりも長い場合は、ASA でタグをブロックできません。Java アプレットが <object> タグにあることがわかっている場合、 **filter activex** コマンドを使用して削除します。

例

次の例では、すべての発信接続で Java アプレットをブロックすることを指定しています。

```
ciscoasa(config)# filter java 80 0 0 0 0
```

次に、Java アプレット ブロックを、すべてのローカル ホストからポート 80 への Web トラフィック、および外部ホストへの接続の Web トラフィックに適用することを指定する例を示します。

次の例では、保護されたネットワーク上のホストへの Java アプレットのダウンロードをブロックしています。

```
ciscoasa(config)# filter java http 192.168.3.3 255.255.255.255 0 0
```

関連コマンド

filter activex	ASA を通過する HTTP トラフィックから ActiveX オブジェクトを削除します。
filter url	トラフィックを URL フィルタリング サーバーに送ります。
show running-config filter	フィルタリング コンフィギュレーションを表示します。
url-server	filter コマンドで使用する N2H2 サーバーまたは Websense サーバーを指定します。

filter url

トラフィックを URL フィルタリングサーバーに転送するには、グローバル コンフィギュレーション モードで filter **url** 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。

filter url *port* [- *port*] | **except** *local_ip local_mask foreign_ip foreign_mask* [**allow**] [**cgi-truncate**] [**longurl-truncate** | **longurl-deny**] [**proxy-block**]
no filter url *port* [- *port*] | **except** *local_ip local_mask foreign_ip foreign_mask* [**allow**] [**cgi-truncate**] [**longurl-truncate** | **longurl-deny**] [**proxy-block**]

構文の説明

allow	サーバーが利用できない場合、発信接続はフィルタリングなしで ASA を通過します。このオプションを省略した場合、および N2H2 サーバーまたは Websense サーバーがオフラインの場合、ASA は、N2H2 サーバーまたは Websense サーバーがオンラインに戻るまで、発信ポート 80（Web）トラフィックを停止します。
cgi_truncate	CGI スクリプトのように、URL に疑問符（?）から始まるパラメータ リストがある場合は、フィルタリング サーバーに送信する URL から、疑問符を含む疑問符以降のすべての文字を削除します。
except	先行の filter 条件に対する例外を作成します。
foreign_ip	セキュリティ レベルが最も低い、アクセスが要求されているインターフェイスの IP アドレス。0.0.0.0（短縮形は 0）を使用すると、すべてのホストを指定できます。
foreign_mask	foreign_ip 引数のネットワーク マスク。常に特定のマスク値を指定します。0.0.0.0（短縮形は 0）を使用すると、すべてのホストを指定できます。
http	ポート 80 を指定します。80 の代わりに http または www と入力してポート 80 を指定することもできます。
local_ip	セキュリティ レベルが最も高い、アクセスが要求されているインターフェイスの IP アドレス。このアドレスに 0.0.0.0（短縮形は 0）を設定すると、すべてのホストを指定できます。
local_mask	*local_ip* 引数のネットワーク マスク。0.0.0.0（短縮形は 0）を使用すると、すべてのホストを指定できます。
longurl-deny	URL が URL バッファ サイズの制限を超える場合や、URL バッファが使用できない場合に URL 要求を拒否します。
longurl-truncate	URL が URL バッファの制限を超える場合は、N2H2 サーバーまたは Websense サーバーに対して元のホスト名または IP アドレスのみを送信します。

-port	（任意）フィルタリングの適用対象となる TCP ポート。一般的に、これはポート 80 ですが、他の値でも受け入れられます。ポート 80 には http または url リテラルを使用できます。ハイフンの後にもう 1 つポートを追加すると、ポートの範囲を指定できます。
proxy-block	ユーザーの HTTP プロキシ サーバーへの接続を禁止します。
url	ASA 経由で伝送されるデータから URL をフィルタリングします。

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
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)	このコマンドが追加されました。

使用上のガイドライン

filter url コマンドを使用すると、N2H2 または Websense フィルタリング アプリケーションを使用して指定した WWW 上の URL への発信ユーザーのアクセスを禁止できます。

（注） **url-server** コマンドを発行するには、事前に **filter url** コマンドを設定する必要があります。

filter **url** コマンドの allow オプションは、N2H2 サーバーまたは Websense サーバーがオフラインになった場合の ASA の動作を決定します。filter **url** コマンドで allow オプションを使用し、N2H2 サーバーまたは Websense サーバーがオフラインになった場合、ポート 80 のトラフィックはフィルタリングなしで ASA を通過します。allow オプションを指定しないでこのコマンドを使用し、サーバーがオフラインになった場合、ASA では、サーバーが再度オンラインになるまでポート 80（Web）への発信トラフィックが停止されるか、または別の URL サーバーを使用できる場合は次の URL サーバーに制御が渡されます。

（注） allow オプションを設定した場合、ASA では、N2H2 サーバーまたは Websense サーバーがオフラインになると代替サーバーに制御が渡されます。

N2H2 サーバーまたは Websense サーバーは、ASA と連携して動作し、会社のセキュリティポリシーに基づいてユーザーの Web サイトへのアクセスを拒否します。

フィルタリング サーバーの使用方法

Websense プロトコルバージョン 4 では、ホストと ASA との間でのグループおよびユーザー名認証が可能です。ASA は、ユーザー名ルックアップを実行し、その後 Websense サーバーが URL フィルタリングおよびユーザー名のロギングを処理します。

N2H2 サーバーは、IFP サーバーを実行する Windows ワークステーション（2000、NT、または XP）である必要があります。512 MB 以上の RAM を推奨します。また、N2H2 サービスにおける長い URL のサポートは最大 3 KB までとなっており、Websense における制限よりも短くなっています。

Websense プロトコル バージョン 4 では、次の機能が拡張されました。

- URL フィルタリングによって、ASA では、Websense サーバーに定義されているポリシーを使用して発信 URL 要求をチェックできます。
- ユーザー名のロギングによって、Websense サーバーでユーザー名、グループ、およびドメイン名が追跡されます。
- ユーザー名ルックアップによって、ASA では、ユーザー認証テーブルを使用して、ホストの IP アドレスをユーザー名にマッピングできます。

Websense についての情報は、次の Web サイトで入手できます。

http://www.websense.com/

設定手順

次の手順を実行して、URL フィルタリングを行います。

1. ベンダー固有の適切な形式の url-server コマンドを使用して、N2H2 サーバーまたは Websense サーバーを指定します。
2. filter コマンドを使用して、フィルタリングをイネーブルにします。
3. 必要に応じて url-cache コマンドを使用して、スループットを向上させます。ただし、このコマンドは Websense ログを更新しないため、Websense アカウンティング レポートに影響がある可能性があります。url-cache コマンドを使用する前に、Websense の実行ログを蓄積します。
4. show url-cache statistics コマンドおよび show perfmon コマンドを使用して、実行情報を表示します。

長い URL の使用

Websense フィルタリング サーバーでは 4 KB まで、N2H2 フィルタリング サーバーでは 3 KB までの URL のフィルタリングがサポートされています。

許可されている最大サイズよりも長い URL 要求の処理を許可するには、**longurl-truncate** オプションおよび **cgi-truncate** オプションを使用します。

URL が最大長よりも長く、longurl-truncate オプションまたは longurl-deny オプションをイネーブルにしない場合、ASA ではパケットがドロップされます。

longurl-truncate オプションを指定すると、ASA は URL が最大許容長よりも長い場合に、URL のホスト名または IP アドレス部分だけを、評価のためにフィルタリングサーバーに送信します。longurl-deny オプションは、URL が最大許容長よりも長い場合、発信 URL トラフィックを拒否します。

パラメータは含まずに CGI スクリプトの場所とスクリプト名だけを含むよう CGI URL を切り捨てるには、cgi-truncate オプションを使用します。長い HTTP 要求のほとんどは、CGI 要求です。パラメータリストが非常に長い場合、パラメータリストを含む完全な CGI 要求を待機したり送信したりすると、大量のメモリリソースが使用され、ASA のパフォーマンスに影響を与える可能性があります。

HTTP 応答のバッファリング

デフォルトで、ユーザーが特定の Web サイトに対する接続要求を発行すると、ASA はその要求を Web サーバーとフィルタリングサーバーに同時に送信します。Web コンテンツ サーバーよりも前にフィルタリング サーバーが応答しない場合、Web サーバーからの応答はドロップされます。このような場合、Web クライアントの観点からは、Web サーバーの応答が遅延することになります。

HTTP 応答バッファをイネーブルにすることによって、Web コンテンツ サーバーからの応答がバッファリングされ、フィルタリング サーバーによって接続が許可された場合にその応答が要求元ユーザーに転送されます。これにより、応答バッファをイネーブルにしない場合に発生する遅延を防止できます。

HTTP 応答バッファをイネーブルにするには、次のコマンドを入力します。

```
ciscoasa(config)# url-block block
 block-buffer-limit
```

block-buffer-limit 引数を、バッファリングする最大ブロック数で置き換えます。1 ～ 128 の値を指定できます。この値は、一度にバッファリング可能な 1550 バイトのブロック数を指定します。

例

次に、10.0.2.54 ホストからの接続を除く、すべての発信 HTTP 接続をフィルタリングする例を示します。

```
ciscoasa(config)# url-server (perimeter) host 10.0.1.1
ciscoasa(config)# filter url 80 0 0 0 0
ciscoasa(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

次に、ポート 8080 でリッスンするプロキシ サーバー宛てのすべての発信 HTTP 接続をブロックする例を示します。

```
ciscoasa(config)# filter url 8080 0 0 0 0 proxy-block
```

関連コマンド

コマンド	説明
filter activex	ASA を通過する HTTP トラフィックから ActiveX オブジェクトを削除します。
filter java	ASA を通過する HTTP トラフィックから Java アプレットを削除します。
url-block	フィルタリング サーバーからのフィルタリング決定を待っている間、Web サーバーの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバーまたは Websense サーバーからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	filter コマンドで使用する N2H2 サーバーまたは Websense サーバーを指定します。

fips enable

FIPS 準拠を強制するためのポリシー チェック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 fips enable コマンドを使用します。ポリシー 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。

fips enable
no fips enable

構文の説明

enable	FIPS 準拠を強制するためのポリシー チェック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

このコマンドには、デフォルト設定がありません。

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(4)	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。
9.8(2)	FIPS モードを有効にするには、設定の保存とリロードが必要になりました。また、フェールオーバー ペアの両方のユニットは、同じ FIPS 設定が必要です。

使用上のガイドライン

FIPS 準拠動作モードで実行するには、fips enable コマンドを適用し、セキュリティ ポリシーに指定されている正しいコンフィギュレーションを適用する必要があります。内部 API によって、実行時に正しいコンフィギュレーションが適用されるようにデバイスを移行できます。

スタートアップ コンフィギュレーションに FIPS 準拠モードが存在する場合、FIPS POST が実行され、次のコンソール メッセージが出力されます。

```
Copyright (c) 1996-2005 by Cisco Systems, Inc.
Restricted Rights Legend
Use, duplication, or disclosure by the Government is subject to restrictions as set forth
 in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at
```

```
FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and
Computer Software clause at DFARS sec. 252.227-7013.

               Cisco Systems, Inc.
               170 West Tasman Drive
               San Jose, California 95134-1706

....
Cryptochecksum (unchanged): 6c6d2f77 ef13898e 682c9f94 9c2d5ba9

INFO: FIPS Power-On Self-Test in process.  Estimated completion in 90 seconds.
.................................................
INFO: FIPS Power-On Self-Test complete.
Type help or '?' for a list of available commands.
sw8-5520>
```

（注） FIPS モードは、クラスタリングモードではサポートされていません。

（注） すべてのインターフェイスがポートチャネルのメンバーとして設定されている場合、FIPS セルフテストは起動時に失敗します。FIPS セルフテストが起動時に成功するには、少なくとも 1 つのインターフェイスを有効にして、ポートチャネルのメンバーとしては設定しないようにする必要があります。

例

次に、システムで FIPS 準拠を強制するためのポリシー チェックを示します。

```
ciscoasa(config)# fips enable
WARNING: FIPS mode change will not take effect until you save configuration and reboot
the device
```

関連コマンド

コマンド	説明
clear configure fips	NVRAM に保存されているシステムまたはモジュールの FIPS コンフィギュレーション情報をクリアします。
crashinfo console disable	フラッシュに対するクラッシュ書き込みの読み取り、書き込み、およびコンフィギュレーションをディセーブルにします。
fips self-test poweron	電源投入時自己診断テストを実行します。
show crashinfo console	フラッシュに対するクラッシュ書き込みの読み取り、書き込み、および設定を行います。
show running-config fips	ASA で実行されている FIPS コンフィギュレーションを表示します。
show fips	FIPS の現在の動作状態を ASA に表示します。

fips self-test poweron

電源投入時自己診断テストを実行するには、特権 EXEC モードで fips self-test powereon コマンドを使用します。

fips self-test poweron

構文の説明

poweron	電源投入時自己診断テストを実行します。

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
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(4)	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

このコマンドを入力すると、デバイスでFIPS 140-2 準拠に必要なすべてのセルフテストが実行されます。テストには、暗号化アルゴリズムテスト、ソフトウェア完全性テスト、および重要機能のテストがあります。

例

次に、システムで電源投入時自己診断テストを実行する例を示します。

```
ciscoasa(config)# fips self-test poweron
```

関連コマンド

コマンド	説明
clear configure fips	NVRAM に保存されているシステムまたはモジュールの FIPS コンフィギュレーション情報をクリアします。
crashinfo console disable	フラッシュに対するクラッシュ書き込み情報の読み取り、書き込み、およびコンフィギュレーションをディセーブルにします。

コマンド	説明
fips enable	システムまたはモジュールで FIPS 準拠を強制するためのポリシーチェックをイネーブルまたはディセーブルにします。
show crashinfo console	フラッシュに対するクラッシュ書き込みの読み取り、書き込み、および設定を行います。
show running-config fips	ASA で実行されている FIPS コンフィギュレーションを表示します。

firewall transparent

ファイアウォールモードをトランスペアレントモードに設定するには、グローバル コンフィギュレーション モードで **firewall transparent** コマンドを使用します。ルーテッドモードに戻すには、このコマンドの **no** 形式を使用します。

firewall transparent
no firewall transparent

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、ASA はルーテッドモードになっています。

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
7.0(1)	このコマンドが追加されました。
8.5(1)/9.0(1)	マルチ コンテキスト モードでは、コンテキストごとにこれを設定できます。

使用上のガイドライン

トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルス ファイアウォール」のように動作するレイヤ2ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。

マルチ コンテキスト モードでは、コンテキストごとにこのコマンドを設定できます。

多くのコマンドは両方のモードではサポートされていないため、モードを変更した場合は、ASAによってコンフィギュレーションがクリアされます。設定済みのコンフィギュレーションがある場合は、モードを変更する前にコンフィギュレーションをバックアップしてください。このバックアップは、新しいコンフィギュレーション作成時の参照として使用できます。

firewall transparent コマンドでモードを使用して変更するテキスト コンフィギュレーションを ASA にダウンロードする場合、コマンドをコンフィギュレーションの先頭に配置してください。このコマンドが読み込まれるとすぐに ASA がモードを変更し、その後ダウンロードされたコンフィギュレーションを引き続き読み込みます。コマンドをコンフィギュレーションの後

の方に配置すると、コンフィギュレーション内のその位置よりも前にあるすべての行が ASA によってクリアされます。

例

次に、ファイアウォール モードをトランスペアレントに変更する例を示します。

```
ciscoasa(config)# firewall transparent
```

関連コマンド

コマンド	説明
arp-inspection	ARP パケットとスタティック ARP エントリを比較する ARP インスペクションをイネーブルにします。
mac-address-table static	MAC アドレス テーブルにスタティック MAC アドレス エントリを追加します。
mac-learn	MAC アドレス ラーニングをディセーブルにします。
show firewall	ファイアウォール モードを表示します。
show mac-address-table	ダイナミック エントリおよびスタティック エントリを含む MAC アドレス テーブルを表示します。

flow-export active refresh-interval

flow-update イベント間の間隔を指定するには、グローバル コンフィギュレーション モードで **flow-export active refresh-interval** コマンドを使用します。

flow-export active refresh-interval *value*

構文の説明

value	flow-update イベント間の間隔を分単位で指定します。有効な値は 1 ～ 60 分です。

コマンド デフォルト

デフォルト値は 1 分です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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
9.1(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

flow-export delay flow-create コマンドを設定した後で、遅延値より 5 秒以上長くはない間隔値を使用して flow-export active refresh-interval コマンドを設定した場合、コンソールに次の警告メッセージが表示されます。

```
WARNING: The current delay flow-create value configuration may cause flow-update events
 to appear before flow-creation events.
```

flow-export active refresh-interval コマンドを設定した後で、間隔値より 5 秒以上短くはない遅延値を使用して **flow-export delay flow-create** コマンドを設定した場合、コンソールに次の警告メッセージが表示されます。

```
WARNING: The current delay flow-create value configuration may cause flow-update events
 to appear before flow-creation events.
```

例

次に、30 分の時間間隔を設定する例を示します。

```
ciscoasa(config)# flow-export active refresh-interval 30
```

関連コマンド

コマンド	説明
clear flow-export counters	NetFlow のランタイム カウンタをすべてゼロにリセットします。
flow-export destination	NetFlow コレクタの IP アドレスまたはホスト名と、NetFlow コレクタがリッスンする UDP ポートを指定します。
flow-export template timeout-rate	テンプレート情報が NetFlow コレクタに送信される間隔を制御します。
logging flow-export-syslogs enable	**logging flow-export-syslogs disable** コマンドを入力した後に、syslog メッセージをイネーブルにし、さらに NetFlow データに関連付けられた syslog メッセージをイネーブルにします。
show flow-export counters	NetFlow のランタイム カウンタのセットを表示します。

flow-export delay flow-create

フロー作成イベントのエクスポートを遅延するには、グローバル コンフィギュレーション モードで **flow-export delay flow-create** コマンドを使用します。遅延なしでフロー作成イベントをエクスポートするには、このコマンドの **no** 形式を使用します。

flow-export delay flow-create *seconds*
no flow-export delay flow-create *seconds*

構文の説明

seconds	フロー作成イベントのエクスポートを遅延する秒数を指定します。有効な値は、1 ～ 180 秒です。

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

次の表は、このコマンドを入力できるモードを示しています。

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
8.1(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

flow-export delay flow-create コマンドが設定されていない場合、フロー作成イベントは遅延なしでエクスポートされます。

設定されている遅延よりも前にフローが切断された場合は、flow-create イベントは送信されません。その代わりに拡張フロー ティアダウン イベントが送信されます。

例

次に、フロー作成イベントのエクスポートを 10 秒間遅延する例を示します。

```
ciscoasa(config)# flow-export delay flow-create 10
```

関連コマンド

コマンド	説明
clear flow-export counters	NetFlow のランタイム カウンタをすべてゼロにリセットします。
flow-export destination	NetFlow コレクタの IP アドレスまたはホスト名と、NetFlow コレクタがリッスンする UDP ポートを指定します。
flow-export template timeout-rate	テンプレート情報が NetFlow コレクタに送信される間隔を制御します。
logging flow-export-syslogs enable	**logging flow-export-syslogs disable** コマンドを入力した後に、syslog メッセージをイネーブルにし、さらに NetFlow データに関連付けられた syslog メッセージをイネーブルにします。
show flow-export counters	NetFlow のランタイム カウンタのセットを表示します。

flow-export destination

NetFlow パケットの送信先のコレクタを設定するには、グローバル コンフィギュレーション モードで **flow-export destination** コマンドを使用します。NetFlow パケットのコレクタを削除するには、このコマンドの **no** 形式を使用します。

flow-export destination *interface-name ipv4-address | hostname udp-port*
no flow-export destination *interface-name ipv4-address | hostname udp-port*

構文の説明

hostname	NetFlow コレクタのホスト名を指定します。
interface-name	宛先に到達可能なインターフェイス名を指定します。
ipv4-address	NetFlow コレクタの IP アドレスを指定します。IPv4 だけがサポートされます。
udp-port	NetFlow コレクタがリッスンしている UDP ポートを指定します。有効な値は、1 ～ 65535 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

次の表は、このコマンドを入力できるモードを示しています。

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
8.1(1)	このコマンドが追加されました。
8.1(2)	フローエクスポートの宛先の最大数が 5 に増やされました。

使用上のガイドライン

flow-export destination コマンドを使用すると、NetFlow コレクタに NetFlow データをエクスポートするように ASA を設定できます。

（注） セキュリティ コンテキストごとに最大で 5 つのエクスポートの宛先（コレクタ）を入力できます。新しい宛先を入力すると、新たに追加されたコレクタにテンプレート レコードが送信されます。宛先を 6 つ以上追加しようとすると、次のエラーメッセージが表示されます。「ERROR: A maximum of 5 flow-export destinations can be configured.」

ASA が NetFlow データをエクスポートするように設定されている場合、パフォーマンス向上のため、**logging flow-export-syslogs disable** コマンドを入力して（NetFlow でキャプチャされた）冗長な syslog メッセージをディセーブルにすることを推奨します。

例

次に、NetFlow データのコレクタを設定する例を示します。

```
ciscoasa(config)# flow-export destination inside 209.165.200.224 2055
```

関連コマンド

コマンド	説明
clear flow-export counters	NetFlow のランタイム カウンタをすべてゼロにリセットします。
low-export delay flow-create	指定した時間だけ、フロー作成イベントのエクスポートを遅延します。
flow-export template timeout-rate	テンプレート情報が NetFlow コレクタに送信される間隔を制御します。
logging flow-export-syslogs enable	**logging flow-export-syslogs disable** コマンドを入力した後に、syslog メッセージをイネーブルにし、さらに NetFlow データに関連付けられた syslog メッセージをイネーブルにします。
show flow-export counters	NetFlow のランタイム カウンタのセットを表示します。

flow-export event-type destination

各コレクタにどの NetFlow レコードを送信するかを決定するために NetFlow コレクタおよびフィルタのアドレスを設定するには、ポリシー マップ クラス コンフィギュレーション モードで **flow-export event-type destination** コマンドを使用します。NetFlow コレクタおよびフィルタのアドレスを削除するには、このコマンドの **no** 形式を使用します。

flow-export event-type { **all** | **flow-create** | **flow-denied** | **flow-update** | **flow-teardown** } **destination**
no flow-export event-type { **all** | **flow-create** | **flow-denied** | **flow-update** | **flow-teardown** } **destination**

構文の説明

all	4 つのイベント タイプをすべて指定します。
flow-create	flow-create イベントを指定します。
flow-denied	flow-denied イベントを指定します。
flow-teardown	flow-teardown イベントを指定します。
flow-update	flow-update イベントを指定します。

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

次の表は、このコマンドを入力できるモードを示しています。

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
ポリシー マップ クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.1(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

NetFlow イベントは、Modular Policy Framework を使用して設定されます。Modular Policy Framework が NetFlow 用に設定されていない場合、イベントはログに記録されません。トラフィックはクラスが設定される順序に基づいて照合されます。一致が検出されると、その他のクラスはチェックされません。NetFlow イベントの場合、コンフィギュレーションの要件は次のとおりです。

- flow-export destination（NetFlow コレクタ）は、その IP アドレスによって一意に識別されます。
- サポートされるイベント タイプは、flow-create、flow-teardown、flow-denied、および all です（前述の 4 つのイベント タイプを含みます）。
- flow-export アクションは、インターフェイス ポリシーでサポートされません。
- flow-export アクションがサポートされるのは、**class-default** コマンド、および **match any** コマンドまたは **match access-list** コマンドで使用されるクラスに限られます。
- NetFlow コレクタが定義されていない場合は、コンフィギュレーション アクションは発生しません。
- NetFlow セキュア イベント ロギングのフィルタリングは、順序に関係なく実行されます。

（注） 有効な NetFlow コンフィギュレーションを作成するには、flow-export destination コンフィギュレーションと flow-export event-type コンフィギュレーションの両方が必要です。flow-export destination コンフィギュレーション単独では何も実行されません。また、flow-export event-type コンフィギュレーションのクラス マップも設定する必要があります。これは、デフォルト クラス マップにすることも、自分で作成したクラス マップにすることもできます。

例

次に、ホスト 10.1.1.1 と 20.1.1.1 の間のすべての NetFlow イベントを送信先 15.1.1.1 にエクスポートする例を示します。

```
ciscoasa(config)# access-list
 flow_export_acl
 permit ip host 10.1.1.1 host 20.1.1.1
ciscoasa(config)# class-map flow_export_classciscoasa(config-cmap)# match access-list
flow_export_aclciscoasa(config)# policy-map global_policyciscoasa(config-pmap)# class
flow_export_classciscoasa(config-pmap-c)# flow-export event-type all destination
15.1.1.1
```

関連コマンド

コマンド	説明
clear flow-export counters	NetFlow のランタイム カウンタをすべてゼロにリセットします。
flow-export delay flow-create	指定した時間だけ、フロー作成イベントのエクスポートを遅延します。
flow-export template timeout-rate	テンプレート情報が NetFlow コレクタに送信される間隔を制御します。

コマンド	説明
logging flow-export-syslogs enable	**logging flow-export-syslogs disable** コマンドを入力した後に、syslog メッセージをイネーブルにし、さらに NetFlow データに関連付けられた syslog メッセージをイネーブルにします。
show flow-export counters	NetFlow のランタイム カウンタのセットを表示します。

flow-export template timeout-rate

テンプレート情報がNetFlowコレクタに送信される間隔を制御するには、グローバル コンフィギュレーション モードで**flow-export template timeout-rate** コマンドを使用します。テンプレートタイムアウトをデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

flow-export template timeout-rate *minutes*
no flow-export template timeout-rate *minutes*

構文の説明

minutes	間隔を分単位で指定します。有効な値は、1 ～ 3600 分です。
template	テンプレートのエクスポートを設定するための **timeout-rate** キーワードをイネーブルにします。
timeout-rate	テンプレートを最初に送信してから再送信するまでの時間（間隔）を指定します。

コマンド デフォルト

間隔のデフォルト値は 30 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
8.1(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

使用するコレクタ、およびコレクタにおいて必要となるテンプレートリフレッシュ頻度に基づいて、タイムアウト レートを設定する必要があります。

セキュリティアプライアンスが NetFlow データをエクスポートするように設定されている場合、パフォーマンス向上のため、**logging flow-export-syslogs disable** コマンドを入力して（NetFlow でキャプチャされた）冗長な syslog メッセージをディセーブルにすることを推奨します。

例

次に、すべてのコレクタに対してテンプレート レコードを 60 分ごとに送信するように NetFlow を設定する例を示します。

```
ciscoasa(config)# flow-export template timeout-rate 60
```

関連コマンド

コマンド	説明
clear flow-export counters	NetFlow データに関連付けられているすべてのランタイム カウンタをリセットします。
flow-export destination	NetFlow コレクタの IP アドレスまたはホスト名と、NetFlow コレクタがリッスンする UDP ポートを指定します。
logging flow-export-syslogs enable	**logging flow-export-syslogs disable** コマンドを入力した後に、syslog メッセージをイネーブルにし、さらに NetFlow データに関連付けられた syslog メッセージをイネーブルにします。
show flow-export counters	NetFlow のランタイム カウンタのセットを表示します。

flow-offload enable

フローオフロードを有効にするには、グローバル コンフィギュレーション モードで **flow-offload enable** コマンドを使用します。オフロード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。

flow-offloadenable
no flow-offload 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

フローのオフロー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
9.5(2.1)	このコマンドが導入されました。このコマンドは FXOS 1.1.3+ を実行している Firepower 9300 シリーズのみで使用できます。
9.6(1)	FXOS 1.1.4+ を実行している Firepower 4100 シリーズのサポートが追加されました。
9.6(2)	トランスペアレント モードのマルチキャスト接続のサポートが追加されました。ただし、ブリッジ グループに 2 つのインターフェイスだけが含まれる場合に限ります。
9.15(1)	機能を有効または無効にするときにシステムをリロードする必要がなくなりました。

使用上のガイドライン

データセンターにアプライアンスと ASA セキュリティモジュールを展開した場合、超高速パスにオフロードするために選択されたトラフィックを識別して、フローがNIC自体でスイッチングされるようにできます。オフロードを行うと、大容量ファイルの転送など、データ集約型アプリケーションのパフォーマンスを向上させることができます。

オフロードを行う前に、ASA は接続確立時に通常のセキュリティ処理（アクセス ルールやインスペクションなど）を適用します。ASAはまた、セッションの切断を行います。しかし、接

続が確立され、フローがオフロード対象として識別されると、以降の処理はASA ではなく NIC で発生します。

オフロード中、フローはセキュリティ ポリシー チェックなどのサービスを受け取らないため、システム全体を可能な限り高速に移動できます。オフロードされたフローに対しては、インスペクション、TCP 正規化（設定した場合はチェックサム検証を除く）、QoS、シーケンス番号チェックが行われません。

オフロードできるフローを識別するには、フロー オフロード サービスを適用するサービス ポリシー ルールを作成します。次の条件を満たす場合、一致したフローがオフロードされます。

- IPv4 アドレスのみ。
- TCP、UDP、GRE のみ。
- 標準または 802.1q タグ付きイーサネット フレームのみ。
- （トランスペアレント モードのみ。）インターフェイスを 2 つだけ含むブリッジ グループのマルチキャスト フロー。
- オフロードされるフローに適用できないサービス（インスペクション、復号化、IPSec および VPN フロー、サービス モジュールに送信されるフロー）を受け取らない。

オフロードされるフローのリバース フローもオフロードされます。

マルチコンテキスト モードでは、フロー オフロードを有効または無効にすると、すべてのコンテキストのフロー オフロードが有効または無効になります。コンテキストごとに異なる設定を使用することはできません。

9.15(1) より前のバージョンでは、フロー オフロードを有効または無効にするたびにシステムをリロードする必要があります。バージョン 9.15(1) 以降では、リロードは不要になり、次の特別な考慮事項は適用されません。

9.15(1) より前のバージョンでは、クラスタまたはフェールオーバーペアの場合、ヒットレスなモード変更を行うには、次の事項を考慮する必要があります。

- クラスタリング：最初にマスター ユニット上でコマンドを入力しますが、マスター ユニットをすぐにリブートしないでください。代わりに、クラスタの各メンバーを最初にリブートしてから、マスターに戻ってリブートします。その後、マスター ユニットでオフロード サービス ポリシーを設定できます。
- フェールオーバー：最初にアクティブ ユニット上でコマンドを入力しますが、アクティブ ユニットをすぐにリブートしないでください。代わりに、スタンバイ ユニットをリブートしてから、アクティブ ユニットをリブートします。次に、アクティブ ユニット上でオフロード サービス ポリシーを設定します。

（注） デバイス サポートの詳細については、http://www.cisco.com/c/en/us/td/docs/security/firepower/9300/compatibility/fxos-compatibility.html を参照してください。

例

次に、フローのオフロードをイネーブルにし、設定を保存してシステムをリブートする例を示します。

```
ciscoasa(config)# flow-offload enable

WARNING: This command will take effect after the running-config is
saved and the system has been rebooted.
ciscoasa(config)# write memory

ciscoasa(config)# reload
```

関連コマンド

コマンド	説明
set-connection advanced-options flow-offload	オフロードの対象としてトラフィック フローを指定します。
show flow-offload	オフロードするフローに関する情報を表示します。

flow-offload-ipsec

IPsec フローオフロードを有効にするには、グローバル コンフィギュレーション モードで **flow-offload-ipsec** コマンドを使用します。オフロード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。

flow-offload-ipsec ［ **egress-optimization** ］
no flow-offload-ipsec ［ **egress-optimization** ］

構文の説明

egress-optimization	（オプション）データパスを最適化して、単一トンネルフローのパフォーマンスを向上させます。

コマンド デフォルト

IPsec フローオフロードは、サポートされるデフォルトのプラットフォームで有効になっていますが、出力の最適化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
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
9.18(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

IPsec フローのオフロードを使用するように、サポートするデバイスモデルを設定できます。IPsec サイト間 VPN またはリモートアクセス VPN セキュリティ アソシエーション (SA) の初期設定後、IPsec 接続はデバイスのフィールド プログラマブル ゲート アレイ (FPGA) にオフロードされるため、デバイスのパフォーマンスが向上します。

オフロード操作は、特に、入力の事前復号および復号処理と出力の事前暗号化および暗号化処理に関連しています。システムソフトウェアは、セキュリティポリシーを適用するための内部フローを処理します。

IPsec フローのオフロードはデフォルトで有効になっており、次のデバイスタイプに適用されます。

- Cisco Secure Firewall 3100

次の IPsec フローはオフロードされません。

- IKEv1 トンネル。IKEv2 トンネルのみがオフロードされます。IKEv2 は、より強力な暗号をサポートしています。
- ボリュームベースのキー再生成が設定されているフロー。
- 圧縮が設定されているフロー。
- トランスポートモードのフロー。トンネルモードのフローのみがオフロードされます。
- AH 形式。ESP/NAT-T 形式のみがサポートされます。
- ポストフラグメンテーションが設定されているフロー。
- 64 ビット以外のアンチリプレイ ウィンドウ サイズを持ち、アンチリプレイが無効になっていないフロー。
- ファイアウォールフィルタが有効になっているフロー。

例

次に、IPsec フローオフロードと出力最適化の両方を有効にする例を示します。

```
ciscoasa# flow-offload-ipsec
ciscoasa# flow-offload-ipsec egress-optimization
```

関連コマンド

コマンド	説明
clear flow-offload-ipsec	IPsec フローオフロードの統計をクリアします。
show flow-offload-ipsec	IPsec フローオフロード統計および情報を表示します。

flowcontrol

フロー制御用のポーズ（XOFF）フレームをイネーブルにするには、インターフェイス コンフィギュレーション モードで **flowcontrol** コマンドを使用します。ポーズフレーム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。

Secure Firewall 3100：

flowcontrol send on
no flowcontrol send on

ASA ハードウェア：

flowcontrol send on ［ *low_water high_water pause_time* ］［ **noconfirm** ］
no flowcontrol send on ［ *low_water high_water pause_time* ］［ **noconfirm** ］

構文の説明

high_water	10 GigabitEthernet の最高水準点を 0 ～ 511 KB の範囲で設定し、1 GigabitEthernet の最高水準点を 0 ～ 47 KB の範囲で（4GE-SSM では GigabitEthernet の最高水準点を 0 ～ 11 KB の範囲で）設定します。バッファの使用量が高基準値を超えると、NIC からポーズ フレームが送信されます。
low_water	10 GigabitEthernet の最低水準点を 0 ～ 511 KB の範囲で設定し、1 GigabitEthernet の最低水準点を 0 ～ 47 KB の範囲で（4GE-SSM では GigabitEthernet の最低水準点を 0 ～ 11 KB の範囲で）設定します。Network Interface Controller（NIC; ネットワーク インターフェイス コントローラ）からポーズ フレームが送信された後、バッファの使用量が低基準値を下回ると、NIC から XON フレームが送信されます。リンク パートナーは、XON フレームを受信するとトラフィックを再開できます。
noconfirm	確認なしでコマンドを適用します。このコマンドでは、インターフェイスがリセットされるため、このオプションを指定しない場合は、コンフィギュレーションの変更の確認を求められます。
pause_time	ポーズ リフレッシュのしきい値を 0 ～ 65535 スロットの範囲で設定します。各スロットは 64 バイトを転送するために必要な時間なので、ユニットあたりの時間はリンク速度によって異なります。リンク パートナーは、XON を受信した後、または XOFF の期限が切れた後、トラフィックを再開できます。XOFF の期限は、ポーズ フレーム内のこのタイマー値によって制御されます。バッファの使用量が継続的に最高水準点を超えている場合は、ポーズ リフレッシュのしきい値に指定された間隔でポーズ フレームが繰り返し送信されます。デフォルトは 26624 です。

コマンド デフォルト

ポーズ フレームは、デフォルトではディセーブルになっています。

10 GigabitEthernet の場合は、次のデフォルト設定を参照してください。

- デフォルトの最高水準点は 128 KB です。
- デフォルトの最低水準点は 64 KB です。

- デフォルトのポーズ リフレッシュのしきい値は 26624 スロットです。

1 GigabitEthernet の場合は、次のデフォルト設定を参照してください。

- デフォルトの最高水準点は 24 KB です。
- デフォルトの最低水準点は 16 KB です。
- デフォルトのポーズ リフレッシュのしきい値は 26624 スロットです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.2(2)	ASA 5580 上の 10-GigabitEthernet インターフェイスに対して、このコマンドが追加されました。
8.2(3)	ASA 5585-X のサポートが追加されました。
8.2(5)/8.4(2)	すべてのモードで 1-GigabitEthernet インターフェイスのサポートが追加されました。
9.18(1)	Cisco Secure Firewall 3100 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、1-GigabitEthernet 以上のインターフェイスでサポートされています。このコマンドでは、管理インターフェイスをサポートしていません。

このコマンドは、物理インターフェイスに対して入力します。

トラフィック バーストが発生している場合、バーストが NIC の FIFO バッファまたは受信リングバッファのバッファリング容量を超えると、パケットがドロップされる可能性があります。フロー制御用のポーズ フレームをイネーブルにすると、このような問題の発生を抑制できます。

このコマンドをイネーブルにすると、FIFO バッファの使用量に基づいて、NIC ハードウェアによってポーズ（XOFF）フレームおよび XON フレームが自動的に生成されます。

1. バッファの使用量が最高水準点を超えると、NIC からポーズ フレームが送信されます。

2. ポーズが送信された後、バッファの使用量が最低水準点を下回ると、NICからXONフレームが送信されます。
3. リンク パートナーは、XON を受信した後、または XOFF の期限が切れた後、トラフィックを再開できます。XOFF の期限は、ポーズ フレーム内のタイマー値によって制御されます。
4. バッファの使用量が継続的に最高水準点を超えている場合は、ポーズリフレッシュのしきい値に指定された間隔でポーズ フレームが繰り返し送信されます。

ASA モデルでこのコマンドを使用すると、次の警告メッセージが表示されます。

```
Changing flow-control parameters will reset the interface. Packets may be lost during
the reset.
Proceed with flow-control changes?
```

プロンプトを表示しないでパラメータを変更するには、**noconfirm** キーワードを使用します。

（注） 802.3x に定義されているフロー制御フレームのみがサポートされています。プライオリティベースのフロー制御はサポートされていません。

例

次に、デフォルト設定を使用してポーズ フレームをイネーブルにする例を示します。

```
ciscoasa(config)# interface tengigabitethernet 1/0
ciscoasa(config-if)# flowcontrol send on
Changing flow-control parameters will reset the interface. Packets may be lost during
the reset.
Proceed with flow-control changes?
ciscoasa(config-if)# y
```

関連コマンド

コマンド	説明
interface	インターフェイス コンフィギュレーション モードを開始します。

flow-mobility lisp

クラスタのフローモビリティをイネーブルにするには、クラス コンフィギュレーション モードで **flow-mobility lisp** コマンドを使用します。フローモビリティ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。

flow-mobility lisp
no flow-mobility lisp

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
クラスタ構成	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(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

このオン/オフ トグルを使用すると、特定のクラスのトラフィックまたはアプリケーションに対してフロー モビリティを簡単にイネーブルまたはディセーブルにできます。

クラスタ フロー モビリティの LISP インスペクションについて

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

クラスタ フロー モビリティには複数の相互に関連する設定が含まれています。

1. （オプション）ホストまたはサーバーの IP アドレスに基づく検査される EID の限定：最初のホップ ルータは、ASA クラスタが関与していないホストまたはネットワークに関する EID 通知メッセージを送信することがあるため、EID をクラスタに関連するサーバーまたはネットワークのみに限定することができます。たとえば、クラスタが 2 つのサイトのみに関連しているが、LISP は 3 つのサイトで稼働している場合は、クラスタに関連する 2 つのサイトの EID のみを含めます。**policy-map type inspect lisp**、**allowed-eid,** および **validate-key** コマンドを参照してください。

2. LISP トラフィックのインスペクション：ASA は、最初のホップ ルータと ITR または ETR 間で送信された EID 通知メッセージに関して LISP トラフィックを検査します。ASA は EID とサイト ID を相関付ける EID テーブルを維持します。たとえば、最初のホップ ルータの送信元 IP アドレスと ITR または ETR の宛先アドレスをもつ LISP トラフィックを検査する必要があります。**inspect lisp** コマンドを参照してください。
3. 指定されたトラフィックでのフロー モビリティを有効にするサービス ポリシー：ビジネスクリティカルなトラフィックでフローモビリティを有効にする必要があります。たとえば、フロー モビリティを、HTTPS トラフィックのみに制限したり、特定のサーバとの間でやり取りされるトラフィックのみに制限したりできます。**cluster flow-mobility lisp** コマンドを参照してください。
4. サイト ID：ASA は各クラスタ ユニットのサイト ID を使用して、新しい所有者を判別します。**site-id** コマンドを参照してください。
5. フロー モビリティを有効にするクラスタレベルの設定：クラスタ レベルでもフロー モビリティを有効にする必要があります。このオン/オフの切り替えを使用することで、特定のクラスのトラフィックまたはアプリケーションに対してフローモビリティを簡単に有効または無効にできます。**flow-mobility lisp** コマンドを参照してください。

例

次に、cluster1 のフロー モビリティをイネーブルにする例を示します。

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# flow-mobility lisp
```

関連コマンド

コマンド	説明
allowed-eids	IP アドレスに基づいて検査される EID を限定します。
clear cluster info flow-mobility counters	フロー モビリティ カウンタをクリアします。
clear lisp eid	ASA EID テーブルから EID を削除します。
cluster flow-mobility lisp	サービス ポリシーのフローモビリティを有効にします。
flow-mobility lisp	クラスタのフロー モビリティを有効にします。
inspect lisp	LISP トラフィックを検査します。
policy-map type inspect lisp	LISP 検査をカスタマイズします。
site-id	クラスタ シャーシのサイト ID を設定します。
show asp table classify domain inspect-lisp	LISP 検査用の ASP テーブルを表示します。
show cluster info flow-mobility counters	フロー モビリティ カウンタを表示します。

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

format

すべてのファイルを消去してファイルシステムをフォーマットするには、特権EXECモードで **format** コマンドを使用します。

format { **disk0:** | **disk1:** | **flash:** }

構文の説明

disk0：	内部フラッシュメモリを指定し、続けてコロンを入力します。
disk1:	外部フラッシュメモリカードを指定し、続けてコロンを入力します。
flash:	内部フラッシュメモリを指定し、続けてコロンを入力します。ASA 5500 シリーズでは、**flash** キーワードは **disk0** のエイリアスです。

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。

使用上のガイドライン

format コマンドは、指定したファイルシステム上のすべてのデータを消去して、デバイスに FAT 情報を再書き込みします。

⚠

注意 **format** コマンドを使用するのは、必要な場合に、破損したフラッシュメモリをクリーンアップするためにのみ、慎重に使用してください。

（非表示のシステムファイルを除く）表示されているすべてのファイルを削除する場合は、**format** コマンドではなく **delete /recursive** コマンドを入力します。

（注） ASA 5500 シリーズでは、**erase** コマンドを実行すると、ディスク上のすべてのユーザーデータが 0xFF パターンを使用して破棄されます。一方、**format** コマンドはファイルシステムの制御構造をリセットするだけです。raw ディスク読み取りツールを使用すると、この情報はまだ参照できる可能性があります。破損したファイルシステムを修復する場合は、**format** コマンドを入力する前に **fsck** コマンドを入力します。

例

次に、フラッシュ メモリをフォーマットする例を示します。

```
ciscoasa# format flash:
```

関連コマンド

コマンド	説明
delete	ユーザーに表示されるすべてのファイルを削除します。
erase	すべてのファイルを削除し、フラッシュ メモリをフォーマットします。
fsck	破損したファイル システムを修復します。

forward interface

ASA 5505 など、組み込みスイッチを搭載したモデルの場合、特定の VLAN で他の特定の VLAN への接続の開始を可能にするには、インターフェイス コンフィギュレーション モードで**forward interface** コマンドを使用します。特定の VLAN で他の特定の VLAN への接続が開始されないよう制限するには、このコマンドの **no** 形式を使用します。

forward interface vlan *number*
no forward interface vlan *number*

（注） Firepower 1010 および ASA 5505 でのみサポートされています。

構文の説明

vlan *number*	この VLAN インターフェイスでトラフィックの開始を禁止する先の VLAN ID を指定します。

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から他のすべてのインターフェイスにトラフィックを開始できます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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
7.2(1)	このコマンドが追加されました。
9.13(1)	Firepower 1010 のサポートが追加されました。

使用上のガイドライン

ライセンスでサポートされている VLAN 数に応じて、特定の VLAN の制限が必要となることがあります。

ルーテッド モードでは、ASA 5505 の基本ライセンスで最大 3 つのアクティブ VLAN と Security Plus ライセンスで最大 5 つのアクティブ VLAN を設定できます。アクティブな VLAN とは、

nameif コマンドが設定された VLAN のことです。いずれのライセンスでも、ASA 5505 では最大 5 つの非アクティブな VLAN を設定できますが、これらをアクティブにする場合は、ライセンスのガイドラインに従う必要があります。

基本ライセンスでは、3 つめの VLAN は **no forward interface** コマンドを使用して設定し、この VLAN から他の特定の VLAN への接続の開始を制限する必要があります。

たとえば、1 つめの VLAN がインターネットアクセス用の外部ネットワークに、2 つめの VLAN が内部の業務用ネットワークに、3 つめの VLAN が家庭用ネットワークにそれぞれ割り当てられているとします。家庭用ネットワークから業務用ネットワークにアクセスする必要はないため、家庭用 VLAN に対して **no forward interface** コマンドを使用できます。業務用ネットワークから家庭用ネットワークにはアクセスできますが、家庭用ネットワークから業務用ネットワークにはアクセスできません。

すでに 2 つの VLAN インターフェイスを **nameif** コマンドで設定している場合は、3 つ目のインターフェイスに対して **nameif** コマンドを使用する前に **no forward interface** コマンドを入力してください。ASA では、ASA 5505 の基本ライセンスで 3 つのフル機能 VLAN インターフェイスを持つことは許可されていません。

例

次の例では、3 つの VLAN インターフェイスを設定します。3 つめの家庭用インターフェイスは、業務用インターフェイスにトラフィックを転送できません。

```
ciscoasa(config)# interface vlan 100
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address dhcp
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 200
ciscoasa(config-if)# nameif work
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 300
ciscoasa(config-if)# no forward interface vlan 200
ciscoasa(config-if)# nameif home
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.2.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/2
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/3
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/4
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# no shutdown
...
```

関連コマンド

コマンド	説明
backup interface	たとえば、ISP へのバックアップ リンクとしてインターフェイスを割り当てます。
clear interface	**show interface** コマンドのカウンタをクリアします。
interface vlan	VLANインターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。
switchport	インターフェイスをスイッチポートモードに設定します。
switchport access vlan	スイッチ ポートを VLAN に割り当てます。

forward-reference （廃止）

まだ存在しない ACL およびオブジェクトを参照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 **forward-reference** コマンドを使用します。

forward-reference enable
no forward-reference enable

構文の説明

enable （アクセス グループ内の）ACL の前方参照と（オブジェクトおよび ACL 内の）オブジェクトの前方参照をイネーブルにします。

コマンド デフォルト

（9.18 より前）デフォルトでは、前方参照は無効になっています。アクセス リスト ルール、別のオブジェクト、またはアクセス グループ内で ACL またはオブジェクトを参照するためには、その ACL またはオブジェクトが存在している必要があります。

9.18以降では、このコマンドはデフォルトで有効になり、設定できなくなりました。前方参照は常に有効になります。

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

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。
9.18(1)	このコマンドは削除されました。常に有効になるようにデフォルトが変更されました。この動作を変更することはできません。

使用上のガイドライン

このコマンドは、ACLおよびそのオブジェクトを編集するための隔離されたセッションを作成する **configure session** コマンドと組み合わせて使用すると最も役立ちます。たとえば、セッション内で、**access-group** コマンドによって現在参照されている ACL を削除して、同じ名前の新しい ACL を作成できます。セッションをコミットすると、ACL の新しいバージョンがコンパイルされて、コンパイル後にアクセス グループのアクティブ バージョンとなります。

同様に、アクティブなアクセス ルールで使用されているオブジェクトを削除して再作成することもできます。

前方参照は、アクセス ルール ACL で使用できるように設計されています。他の機能（NAT や VPN など）で現在使用されているオブジェクトは削除できません。

前方参照をイネーブルにする際は、慎重に行ってください。デフォルトの動作では、オブジェクト、アクセス リスト、およびアクセス グループの設定時に単純な入力ミスを回避できます。前方参照では、ASA は、入力ミスと、将来作成する何かに対する意図的な参照を区別することはできません。

存在しないオブジェクトまたは ACL を指すルール、アクセス グループ、またはオブジェクトは、処理中に無視されます。欠落している項目を作成するまでは、処理できません。

例

次に、前方参照をイネーブルにする例を示します。

```
ciscoasa(config)# forward-reference enable
```

関連コマンド

コマンド	説明
access-group	ACL をインターフェイスに、またはグローバルに割り当てます。
access-list	ACL ルールを作成します。
configure session	セッションを作成するか、開きます。
object	オブジェクトを作成します。
object-group	オブジェクト グループを作成します。

fqdn（クリプト CA トラストポイント）

登録時に、指定した FQDN を証明書のサブジェクト代替名の拡張に含めるには、クリプト CA トラストポイント コンフィギュレーション モードで **fqdn** コマンドを使用します。FQDN のデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

fqdn [*fqdn* | **none**]
no fqdn

構文の説明

fqdn	FQDN を指定します。最大長は、64 文字です。
none	完全修飾ドメイン名を指定しません。

コマンド デフォルト

デフォルトの設定には、FQDN は含まれていません。

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
クリプト CA トラストポイント コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

証明書を使用した Nokia VPN クライアントの認証をサポートするように ASA を設定する場合は、**none** キーワードを使用します。Nokia VPN クライアントの証明書認証のサポートの詳細については、**crypto isakmp identity** コマンドまたは **isakmp identity** コマンドを参照してください。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、トラストポイント central の登録要求に FQDN engineering を含める例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
```

```
ciscoasa(config-ca-trustpoint)# fqdn engineering
ciscoasa(config-ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	クリプトCAトラストポイントコンフィギュレーションモードを開始します。
default enrollment	登録パラメータをデフォルト値に戻します。
enrollment retry count	登録要求の送信を再試行する回数を指定します。
enrollment retry period	登録要求の送信を試行するまでの待機時間を分単位で指定します。
enrollment terminal	このトラストポイントを使用したカットアンドペースト登録を指定します。

fqdn（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 FQDN を設定するには、オブジェクト コンフィギュレーション モードで **fqdn** コマンドを使用します。このオブジェクト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。

fqdn [**v4** | **v6**] *fqdn*
no fqdn [**v4** | **v6**] *fqdn*

構文の説明

fqdn	ホスト名とドメインを含む FQDN を指定します。FQDN は、数字または文字で始まって終わる必要があります。内部文字として使用できるのは、文字、数字、およびハイフンだけです。ラベルは（www.cisco.com のように）ドットで区切ります。
v4	（オプション）IPv4 ドメイン名を指定します。
v6	（任意）IPv6 ドメイン名を指定します。

コマンド デフォルト

デフォルトでは、ドメイン名は IPv4 ドメインです。

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
オブジェクトネットワークコンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(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

別の値を使用して既存のネットワーク オブジェクトを設定すると、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を置き換えます。

例

次に、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 FQDN_1
ciscoasa (config-network-object)# fqdn example.cisco.com
```

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。
description	ネットワーク オブジェクトに説明を追加します。
fqdn	完全修飾ドメイン名のネットワーク オブジェクトを指定します。
host	ホスト ネットワーク オブジェクトを指定します。
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。
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。
range	ネットワーク オブジェクトのアドレス範囲を指定します。
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。
subnet	サブネット ネットワーク オブジェクトを指定します。

fragment

パケット フラグメンテーションの付加的な管理を提供して、NFS との互換性を向上させるには、グローバル コンフィギュレーション モードで fragment 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。

fragment reassembly { **full** | **virtual** } { **size** | **chain** | **timeout** *limit* } [*interface*]
no fragment reassembly { **full** | **virtual** } { **size** | **chain** | **timeout** *limit* } [*interface*]

構文の説明

chain limit	完全な IP パケットをフラグメント化できる最大フラグメント数を指定します。
interface	（任意）ASA のインターフェイスを指定します。interface が指定されていない場合、このコマンドはすべてのインターフェイスに適用されます。
reassembly full | **virtual**	ASA 経由でルーティングされた IP フラグメントに対して完全再構成または仮想再構成を指定します。ASA で終端する IP フラグメントは、常に完全に再構成されます。
size limit	IP 再構築データベース内で再構築を待機可能な最大フラグメント数を設定します。 （注） ASA では、キューのサイズが 2/3 までいっぱいになると、既存のファブリックチェーンの一部ではないすべてのフラグメントが受け入れられなくなります。キューの残りの 1/3 は、すでに部分的にキューイングされている不完全なフラグメント チェーンと送信元 IP アドレス、宛先 IP アドレス、および IP ID 番号が同じであるフラグメントを受け入れるために使用されます。この制限は、フラグメント フラッディング攻撃が行われた場合でも、正規のフラグメント チェーンの再構築を可能にするための DoS 保護メカニズムです。
timeout limit	フラグメント化されたパケット全体が到着するまで待機する最大秒数を指定します。タイマーは、パケットの最初のフラグメントの到着後に開始されます。指定した秒数までに到着しなかったパケット フラグメントがある場合、到着済みのすべてのパケット フラグメントが廃棄されます。

コマンド デフォルト

デフォルトの設定は次のとおりです。

- **chain** は 24 パケットです。
- *interface* はすべてのインターフェイスです。
- **size** は 200 です。
- **timeout** は 5 秒です。
- 仮想再構成がイネーブルです。

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
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)	このコマンドが変更され、**chain**、 **size**、または **timeout** のいずれかのキーワードを選択することが必要になりました。ソフトウェアの以前のリリースでは、これらのキーワードのいずれかを入力しなくても **fragment** コマンドを入力できましたが、これらのキーワードなしでは入力できなくなりました。
8.0(4)	**reassembly full** | **virtual** オプションが追加されました。

使用上のガイドライン

デフォルトで、ASA では、完全な IP パケットを再構築するために最大で 24 のフラグメントを受け入れます。ネットワーク セキュリティ ポリシーに基づいて、各インターフェイスで **fragment chain 1***interface* コマンドを入力して、フラグメント化されたパケットが ASA を通過しないように ASA を設定することを検討する必要があります。limit を 1 に設定すると、すべてのパケットは完全なものである必要があります。つまり、フラグメント化されていない必要があります。

ASA を通過するネットワークトラフィックの多くが NFS である場合は、データベースのオーバーフローを回避するために追加の調整が必要となることがあります。

WAN インターフェイスなど、NFS サーバーとクライアントとの間の MTU サイズが小さい環境では、chain キーワードに追加の調整が必要となる場合があります。この場合、効率性を向上させるために、NFS over TCP を使用することを推奨します。

size limit を大きな値に設定すると、ASA がフラグメントフラッディングによる DoS 攻撃を受けやすくなります。**size** の値は、1550 または 16384 プールの合計ブロック数以上には設定しないでください。

デフォルト値を使用すると、フラグメント フラッディングによる DoS 攻撃が抑制されます。

次のプロセスは、**reassembly** オプションの設定に関係なく実行されます。

- IP フラグメントは、フラグメントセットが作成されるまで、またはタイムアウト間隔が経過するまで収集されます（**timeout** オプションを参照）。
- フラグメントセットが作成されると、セットに対して整合性チェックが実行されます。これらのチェックには、重複、テールオーバーフロー、チェーンオーバーフローはいずれも含まれません（**chain** オプションを参照）。

fragment reassembly virtual コマンドを設定した場合、フラグメントセットはさらなる処理のためにトランスポート層に転送されます。

fragment reassembly full コマンドを設定した場合、フラグメントセットはまず単一の IP パケットに結合されます。この単一の IP パケットは、さらなる処理のためにトランスポート層に転送されます。

例

次に、外部インターフェイスおよび内部インターフェイスにおいてフラグメント化されたパケットの通過を禁止する例を示します。

```
ciscoasa(config)# fragment chain 1 outside
ciscoasa(config)# fragment chain 1 inside
```

引き続き、フラグメント化されたパケットの通過を禁止する追加の各インターフェイスに対して、fragment chain 1 interface コマンドを入力します。

次に、外部インターフェイスのフラグメントデータベースを、最大サイズ 2000、最大チェーン長 45、待機時間 10 秒に設定する例を示します。

```
ciscoasa(config)# fragment size 2000 outside
ciscoasa(config)# fragment chain 45 outside
ciscoasa(config)# fragment timeout 10 outside
```

次に、**reassembly virtual** オプションを含む **show fragment** コマンドの出力例を示します。

```
ciscoasa(config)# show fragment
Interface: outside
    Size: 200, Chain: 24, Timeout: 5, Reassembly: virtual
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: inside
    Size: 200, Chain: 24, Timeout: 5, Reassembly: virtual
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
```

関連コマンド

コマンド	説明
clear configure fragment	すべての IP フラグメント再構成コンフィギュレーションを、デフォルトにリセットします。
clear fragment	IP フラグメント再構成モジュールの動作データをクリアします。
show fragment	IP フラグメント再構成モジュールの動作データを表示します。
show running-config fragment	IP フラグメント再構成コンフィギュレーションを表示します。

frequency

選択した SLA 動作の反復間隔を設定するには、SLA モニター プロトコル コンフィギュレーション モードで **frequency** 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。

frequency*seconds*
no frequency

構文の説明

seconds	SLA プローブ間の秒数。有効な値は、1 ～ 604800 秒です。この値は、**timeout** 値より小さくすることはできません。

コマンド デフォルト

デフォルトの頻度は、60 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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
SLA モニター プロトコル 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
7.2(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

SLA動作は、動作のライフタイム中、指定された頻度で繰り返し実行されます。次に例を示します。

- 60 秒の頻度に設定された **ipIcmpEcho** 動作は、動作のライフタイム中 60 秒ごとにエコー要求パケットを繰り返し送信します。
- エコー動作のデフォルトのパケット数は1です。動作が開始されるとこのパケットが送信され、60 秒後に再度送信されます。

個別の SLA 動作において、指定された頻度の値よりも実行に時間がかかる場合は、動作がすぐに繰り返されるのではなく、「busy」という統計情報カウンタが増加します。

frequency コマンドに指定された値は、**timeout** コマンドに指定された値より小さくすることはできません。

例

次の例では、ID が 123 の SLA 動作を設定し、ID が 1 のトラッキング エントリを作成して、SLA の到達可能性を追跡しています。SLA 動作の頻度が 3 秒に、タイムアウト値が 1000 ミリ秒に設定されています。

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# timeout 1000
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
sla monitor	SLA モニタリング動作を定義します。
timeout	SLA動作が応答を待機する期間を定義します。

fsck

ファイルシステムのチェックを実行して、破損を修復するには、特権 EXEC モードで **fsck** コマンドを使用します。

fsck [**/noconfirm**] { **disk0:** | **disk1:** \ | **flash:** }

構文の説明

/noconfirm	（任意）修復時に確認を求めません。
disk0:	内部フラッシュメモリを指定し、続けてコロンを入力します。
disk1:	外部フラッシュメモリカードを指定し、続けてコロンを入力します。
flash:	内部フラッシュメモリを指定し、続けてコロンを入力します。**flash** キーワードにエイリアス **disk0:** が使用されます。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	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

fsck コマンドは、ファイルシステムに破損がないかどうかをチェックし、破損があった場合には修復を試みます。より恒久的な手順を試みる前に、このコマンドを使用します。

FSCK ユーティリティで（電源障害や異常なシャットダウンなどによる）ディスクの破損箇所が修復されると、FSCK*xxx*.REC という名前のリカバリファイルが作成されます。これらのファイルには、FSCK 実行時に回復されたファイルの一部またはファイル全体が含まれています。まれに、データを回復するためにこれらのファイルを調べる必要がある場合があります。通常、これらのファイルは必要なく、安全に削除できます。

（注） FSCK ユーティリティは起動時に自動的に実行されるため、手動で **fsck** コマンドを入力していない場合でもこれらのリカバリファイルが存在する場合があります。

例

次に、フラッシュ メモリのファイル システムをチェックする例を示します。

```
ciscoasa# fsck disk0:
```

関連コマンド

コマンド	説明
delete	ユーザーに表示されるすべてのファイルを削除します。
erase	すべてのファイルを削除し、フラッシュ メモリをフォーマットします。
format	非表示のシステム ファイルを含むファイル システム上のすべてのファイルを消去して、ファイル システムを再インストールします。

ftp mode passive

FTP モードをパッシブに設定するには、グローバル コンフィギュレーション モードで コマンドを使用します。FTP クライアントをアクティブモードに設定するには、このコマンドの **no** 形式を使用します。

ftp mode passive
no ftp mode passive

コマンド デフォルト

このコマンドは、デフォルトでイネーブルになっています。

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。

使用上のガイドライン

ftp mode passive コマンドは、FTP モードをデフォルトであるパッシブに設定します。ASA では、FTP サーバーとの間で、イメージ ファイルやコンフィギュレーション ファイルのアップロードおよびダウンロードを実行できます。**ftp mode passive** コマンドは、ASA 上の FTP クライアントの FTP サーバーとの通信方法を制御します。

パッシブ FTP では、クライアントは制御接続およびデータ接続の両方を開始します。パッシブ モードとはサーバーの状態を指しており、クライアントが開始する制御接続およびデータ接続の両方をサーバーが受動的に受け入れることを意味しています。

パッシブ モードでは、送信元ポートおよび宛先ポートの両方が 1023 よりも大きい一時ポートです。モードはクライアントによって設定されます。クライアントは、**passive** コマンドを発行して、パッシブデータ接続の設定を開始します。パッシブ モードではデータ接続の受け入れ側となるサーバーは、今回の特定の接続においてリッスンするポート番号を応答として返します。

例

次に、パッシブ モードを無効にする例を示します。

```
ciscoasa(config)# no ftp mode passive
```

関連コマンド

copy	イメージ ファイルやコンフィギュレーション ファイルを FTP サーバーとの間でアップロードまたはダウンロードします。
debug ftp client	FTP クライアントのアクティビティに関する詳細な情報を表示します。
show running-config ftp mode	FTP クライアントのコンフィギュレーションを表示します。

functions（廃止）

（注） このコマンドをサポートする最後のリリースは、Version 8.0(1) でした。

functions コマンドは、リリース 8.0(2) では使用できません。このコマンドは廃止されており、下位互換性の目的でのみこのコマンド リファレンスに記載されています。Web サイトの URL リストの作成、ファイルアクセス、プラグイン、カスタマイゼーション、言語変換には、**import** コマンドおよび **export** コマンドを使用します。

特定のユーザーまたはグループポリシーに対して、ポートフォワーディング Java アプレットの自動ダウンロード、ファイルアクセス、ファイルブラウジング、ファイルサーバー名の入力、Web タイプ ACL の適用、HTTP プロキシ、ポートフォワーディング、または WebVPN 上での URL 入力を設定するには、webvpn コンフィギュレーション モードで **functions** コマンドを入力します。設定済みの機能を削除するには、このコマンドの **no** 形式を使用します。

functions { **auto-download** | **citrix** | **file-access** | **file-browsing** | **file-entry** | **filter** | **http-proxy** | **url-entry** | **port-forward** | **none** }
no functions { **auto-download** | **citrix** | **file-access** | **file-browsing** | **file-entry** | **filter** | **http-proxy** | **url-entry** | **port-forward** | **none** }

構文の説明

auto-download	WebVPN ログイン後のポート フォワーディング Java アプレットの自動ダウンロードをイネーブルまたはディセーブルにします。最初に、ポート フォワーディング、Outlook/Exchange プロキシ、または HTTP プロキシをイネーブルにする必要があります。
citrix	リモート ユーザーに対して、MetaFrame Application Server からのターミナル サービスのサポートをイネーブルまたはディセーブルにします。このキーワードを指定すると、セキュアな Citrix コンフィギュレーション内で ASA をセキュアゲートウェイとして使用できます。これらのサービスでは、ユーザーは、標準的な Web ブラウザから MetaFrame アプリケーションにアクセスできます。
file-access	ファイルアクセスをイネーブルまたはディセーブルにします。イネーブルの場合、WebVPN ホームページには、サーバー リスト内のファイル サーバーが一覧表示されます。ファイル ブラウジングまたはファイル サーバー名の入力をイネーブルにするには、ファイル アクセスをイネーブルにする必要があります。
file-browsing	ファイルサーバーおよび共有のブラウジングをイネーブルまたはディセーブルにします。ユーザーによるファイルサーバー名の入力を許可するには、ファイル ブラウジングをイネーブルにする必要があります。
file-entry	ユーザーによるファイルサーバーの名前の入力をイネーブルまたはディセーブルにします。

filter	Web タイプ ACL を適用します。イネーブルの場合、ASA は、WebVPN の **filter** コマンドで定義された Web タイプ ACL を適用します。
http-proxy	リモート ユーザーへの HTTP アプレット プロキシの転送をイネーブルまたはディセーブルにします。このプロキシは、Java、ActiveX、フラッシュなどの、適切なマングリングに干渉するテクノロジーに対して有用です。これによって、ASA の使用を継続しながらマングリングを回避できます。転送されたプロキシは、自動的にブラウザの古いプロキシ コンフィギュレーションを変更して、すべての HTTP および HTTPS 要求を新しいプロキシ コンフィギュレーションにリダイレクトします。HTTP アプレット プロキシでは、HTML、CSS、JavaScript、VBScript、ActiveX、Java など、ほとんどすべてのクライアント側テクノロジーがサポートされています。サポートされているブラウザは、Microsoft Internet Explorer だけです。
none	すべての WebVPN functions に対してヌル値を設定します。デフォルトまたは指定したグループ ポリシーから機能を継承しません。
port-forward	ポート フォワーディングをイネーブルにします。イネーブルの場合、ASA は、WebVPN の **port-forward** コマンドで定義されたポート フォワーディング リストを使用します。
url-entry	ユーザーによる URL の入力をイネーブルまたはディセーブルにします。イネーブルの場合でも、ASA は引き続き設定されている URL またはネットワーク ACL に基づいて URL を制限します。URL 入力がディセーブルの場合、ASA では、WebVPN ユーザーは、ホームページ上の URL に制限されます。

コマンド デフォルト

機能は、デフォルトで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
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。
7.1(1)	**auto-download** および **citrix** キーワードが追加されました。

リリース	変更内容
8.0(2)	このコマンドは廃止されました。

使用上のガイドライン

functions none コマンドを発行することによって作成されたヌル値を含め、設定されているすべての機能を削除するには、引数を指定しないでこのコマンドの **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。機能の値が継承されないようにするには、**functions none** コマンドを使用します。

例

次に、FirstGroup という名前のグループ ポリシーに対して、ファイル アクセスおよびファイル ブラウジ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)# functions file-access file-browsing
```

関連コマンド

コマンド	説明
webvpn	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 モードで使用します。webvpn 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。

fxos mode appliance

Firepower 2100 をアプライアンスモードに設定するには、グローバル コンフィギュレーション モードで**fxos mode appliance** コマンドを使用します。このモードをプラットフォームモードに設定するには、このコマンドの **no** 形式を使用します。

fxos mode appliance
no fxos mode appliance

（注） このコマンドは Firepower 2100 のみでサポートされています。

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトでは、モードはアプライアンスモードに設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.13(1)	コマンドが追加されました。

使用上のガイドライン

Firepower 2100 は、FXOS と呼ばれる基盤となるオペレーティングシステムを実行します。Firepower 2100 は、次のモードで実行できます。

- アプライアンスモード（デフォルト）：アプライアンスモードでは、ASA のすべての設定を行うことができます。FXOS CLI からは、高度なトラブルシューティング コマンドのみ使用できます。
- プラットフォーム モード：プラットフォーム モードでは、FXOS で、基本的な動作パラメータとハードウェア インターフェイスの設定を行う必要があります。これらの設定には、インターフェイスの有効化、EtherChannels の確立、NTP、イメージ管理などが含まれます。シャーシマネージャ Web インターフェイスまたは FXOS CLI を使用できます。そ

の後、ASDM または ASA CLI を使用して ASA オペレーティング システムにセキュリティ ポリシーを設定できます。

モードを変更すると、設定がクリアされ、現在の設定を保存してシステムをリロードする必要があります。デフォルト設定は、リロード時に適用されます。リロードする前に、中断することなく、モードを元の値に戻すことができます。**clear configure all** および **configure factory-default** コマンドは、現在のモードをクリアしません。

現在のモードを表示するには、**show fxos mode** を使用します。

例

次に、モードをプラットフォームモードに設定する例を示します。

```
ciscoasa(config)# no fxos mode appliance
Mode set to platform mode
WARNING: This command will take effect after the running-config is saved and the system
 has been rebooted. Command accepted.
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: c0532471 648dc7c2 4f2b4175 1f162684
23736 bytes copied in 1.520 secs (23736 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload? [confirm]
```

関連コマンド

コマンド	説明
connect fxos	FXOS CLI に接続します。
show fxos mode	現在のモード、アプライアンス、またはプラットフォームを表示します。

fxos permit

ASA データインターフェイスから FirePOWER 2100 で FXOS SSH、HTTPS、または SNMP を使用するには、グローバル コンフィギュレーション モードで **fxos permit** コマンドを使用します。アクセスを無効にするには、このコマンドの **no** 形式を使用します。

fxos { **https** | **ssh** | **snmp** } **permit** { *ipv4_address netmask* | *ipv6_address* | *prefix_length* } *interface_name*
no fxos { **https** | **ssh** | **snmp** } **permit** { *ipv4_address netmask* | *ipv6_address* | *prefix_length* } *interface_name*

構文の説明

https	シャーシマネージャ の HTTPS アクセスを許可します。デフォルト ポートは 3443 です。
interface_name	アクセスが許可されている ASA データ インターフェイスを指定します。管理専用インターフェイスは指定できません。
ipv4_address netmask	IPv4 アドレスおよびサブネット マスクを指定します。
ipv6_address/prefix_length	IPv6 プレフィックスとプレフィックス長を指定します。
snmp	FXOS への SNMP アクセスを許可します。デフォルト ポートは 3061 です。デバイスからの SNMP トラフィックについては、**ip-client** コマンドも設定する必要があります。
ssh	FXOS への SSH アクセスを許可します。デフォルト ポートは 3022 です。

コマンド デフォルト

次のデフォルトを参照してください。

- HTTPS デフォルト ポート：3443
- SNMP デフォルト ポート：3061
- SSH デフォルト ポート：3022

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
9.8(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

データ インターフェイスから Firepower 2100 の FXOS を管理する場合、SSH、HTTPS、および SNMP アクセスを設定できます。この機能は、デバイスをリモート管理する場合、および管理 1/1 を隔離されたネットワークに維持する場合に役立ちます。継続してローカル アクセスで管理 1/1 を使用できます。1 つのゲートウェイしか指定できないため、ASA データ インターフェイスへのトラフィック転送用に同時に FXOS の管理 1/1 からのリモート アクセスを許可することはできません。デフォルトでは、FXOS 管理ゲートウェイは ASA への内部パスです。

ASA は、FXOS アクセスに非標準ポートを使用します。標準ポートは同じインタ フェースで ASA が使用するため予約されています。ポート値を変更するには、**fxos port** コマンドを使用します。ASA が FXOS にトラフィックを転送するときに、非標準の宛先ポートはプロトコルごとに FXOS ポートに変換されます（FXOS の HTTPS ポートは変更しません）。パケット宛先 IP アドレス（ASA インターフェイス IP アドレス）も、FXOS で使用する内部アドレスに変換されます。送信元アドレスは変更されません。トラフィックを返す場合、ASA は自身のデータ ルーティング テーブルを使用して正しい出力インターフェイスを決定します。管理アプリケーションの ASA データ IP アドレスにアクセスする場合、FXOS ユーザー名を使用してログインする必要があります。ASA ユーザー名は ASA 管理アクセスのみに適用されます。

ip-client コマンドを使用して、ASA データインターフェイスでの FXOS 管理トラフィックの開始を有効にすることもできます。これは、たとえば、SNMP トラップ、NTP と DNS のサーバー アクセスなどに必要です。

FXOS コンフィギュレーションでは、管理アドレスを許可するため、アクセスリストを設定する必要があります（**ip-block** コマンド）。**fxos permit** コマンドで指定されているすべてのアドレスを許可する必要があります。また、デフォルト ゲートウェイが 0.0.0.0 に設定されていることを確認してください。これにより、ASA がゲートウェイとして設定されます。FXOS **set out-of-band** コマンドを参照してください。

（注） ASA データ インターフェイスに VPN トンネルを使用して、FXOS に直接アクセスすることはできません。SSH の回避策として、ASA に VPN 接続し、ASA CLI にアクセスし、**connect fxos** コマンドを使用して FXOS CLI にアクセスします。SSH、HTTPS、および SNMPv3 は暗号化できるため、データ インターフェイスへの直接接続は安全です。

例

次に、192.168.1.0/24 ネットワークおよび 2001:DB8::34/64 ネットワーク用の内部インターフェイス上で、SSH アクセスおよび HTTPS アクセスを有効にする例を示します。

```
ciscoasa(config)# fxos https permit 192.168.1.0 255.255.155.0 inside
ciscoasa(config)# fxos https permit 2001:DB8::34/64 inside
ciscoasa(config)# fxos ssh permit 192.168.1.0 255.255.155.0 inside
ciscoasa(config)# fxos ssh permit 2001:DB8::34/64 inside
```

関連コマンド

コマンド	説明
connect fxos	ASA CLI から FXOS CLI に接続します。
fxos port	FXOS 管理アクセス ポートを設定します。
ip-client	FXOS 管理トラフィックを ASA データ インターフェイスに出力することを許可します。

fxos port

FirePOWER 2100 ASA データインターフェイスで FXOS にアクセスするときの SSH ポート、HTTPS ポート、または SNMP ポートを設定するには、グローバル コンフィギュレーション モードで **fxos port** コマンドを使用します。デフォルトポートを使用するには、このコマンドの **no** 形式を使用します。

fxos { **https** | **ssh** | **snmp** } **port** *port*
no fxos { **https** | **ssh** | **snmp** } **permit** { *ipv4_address netmask* | *ipv6_address* | *prefix_length* }

構文の説明

https	FXOS に対する HTTPS アクセスのためのポートを設定します。デフォルト ポートは 3443 です。
port	ポート番号を指定します。
snmp	FXOS に対する SNMP アクセスのためのポートを設定します。デフォルト ポートは 3061 です。
ssh	FXOS に対する SSH アクセスのためのポートを設定します。デフォルト ポートは 3022 です。

コマンド デフォルト

次のデフォルトを参照してください。

- HTTPS デフォルト ポート：3443
- SNMP デフォルト ポート：3061
- SSH デフォルト ポート：3022

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
9.8(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

fxos permit コマンドを使用して FirePOWER 2100 データインターフェイスでの FXOS アクセスを許可する場合、使用するポートをアプリケーションごとに設定することができます。ASA は、FXOS アクセスに非標準ポートを使用します。標準ポートは同じインタ フェースで ASA が使用するため予約されています。ASA が FXOS にトラフィックを転送するときに、非標準の宛先ポートはプロトコルごとに FXOS ポートに変換されます（FXOS の HTTPS ポートは変更しません）。

例

次に、SSH アクセスおよび HTTPS アクセスのためのポートを設定する例を示します。

```
ciscoasa(config)# fxos https port 6666
ciscoasa(config)# fxos ssh port 7777
```

関連コマンド

コマンド	説明
connect fxos	ASA CLI から FXOS CLI に接続します。
fxos permit	ASA データ インターフェイスでの FXOS 管理アクセスを許可します。
ip-client	FXOS 管理トラフィックを ASA データ インターフェイスに出力することを許可します。

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。