CHAPTER 7

clear conn コマンド～ clear xlate コマンド

clear conn

特定の接続または複数の接続をクリアするには、特権 EXEC モードで **clear conn** コマンドを使用します。このコマンドは IPv4 および IPv6 のアドレスをサポートします。

clear conn [**all**] [**protocol** {**tcp** | **udp**}] [**address** *src_ip*[**-***src_ip*] [**netmask** *mask*]]
[**port** *src_port*[**-***src_port*]] [**address** *dest_ip*[**-***dest_ip*] [**netmask** *mask*]]
[**port** *dest_port*[**-***dest_port*]]

構文の説明

address	（任意）指定された送信元または宛先の IP アドレスとの接続をクリアします。
all	（任意）デバイスを通過するトラフィックの接続に加えて、デバイスへの接続とデバイスからの接続を消去します。
dest_ip	（任意）宛先 IP アドレス（IPv4 または IPv6）を指定します。範囲を指定するには、次のように、IP アドレスをダッシュ（-）で区切ります。 `10.1.1.1-10.1.1.5`
dest_port	（任意）宛先ポート番号を指定します。範囲を指定するには、次のように、ポート番号をダッシュ（-）で区切ります。 `1000-2000`
netmask *mask*	（任意）指定された IP アドレスで使用するサブネット マスクを指定します。
port	（任意）指定された送信元または宛先のポートとの接続をクリアします。
protocol {tcp | udp}	（任意）プロトコル **tcp** または **udp** との接続をクリアします。
src_ip	（任意）送信元 IP アドレス（IPv4 または IPv6）を指定します。範囲を指定するには、次のように、IP アドレスをダッシュ（-）で区切ります。 `10.1.1.1-10.1.1.5`
src_port	（任意）送信元ポートの番号を指定します。範囲を指定するには、次のように、ポート番号をダッシュ（-）で区切ります。 `1000-2000`

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(8)/7.2(4)/8.0(4)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスで第 2 の接続を許すピンホールが作成された場合、このピンホールは、**show conn** コマンドでは不完全な接続として表示されます。この不完全な接続をクリアするには、**clear conn** コマンドを使用します。

例

次に、すべての接続を表示し、次に 10.10.10.108:4168 と 10.0.8.112:22 間の管理接続をクリアする例を示します。

```
hostname# show conn all
TCP mgmt 10.10.10.108:4168 NP Identity Ifc 10.0.8.112:22, idle 0:00:00, bytes 3084, flags
UOB

hostname# clear conn address 10.10.10.108 port 4168 address 10.0.8.112 port 22
```

関連コマンド

コマンド	説明
clear local-host	特定のローカル ホストまたはすべてのローカル ホストによるすべての接続をクリアします。
clear xlate	NAT セッション、または NAT を使用した任意の接続を消去します。
show conn	接続情報を表示します。
show local-host	ローカル ホストのネットワーク状態を表示します。
show xlate	NAT セッションを表示します。

clear console-output

現在キャプチャされているコンソール出力を削除するには、特権 EXEC モードで **clear console-output** コマンドを使用します。

clear console-output

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、現在キャプチャされているコンソール出力を削除する例を示します。

```
hostname# clear console-output
```

関連コマンド

コマンド	説明
console timeout	セキュリティ アプライアンスに対するコンソール接続のアイドル タイムアウトを設定します。
show console-output	キャプチャされているコンソール出力を表示します。
show running-config console timeout	セキュリティ アプライアンスに対するコンソール接続のアイドル タイムアウトを表示します。

clear counters

プロトコル スタック カウンタをクリアするには、グローバル コンフィギュレーション モードで **clear counters** コマンドを使用します。

clear counters [all | **context** *context-name* | **summary** | **top** *N*] [**detail**] [**protocol** *protocol_name* [**:***counter_name*]] [**threshold** *N*]

構文の説明

all	（任意）すべてのフィルタ詳細をクリアします。
context *context-name*	（任意）コンテキスト名を指定します。
:*counter_name*	（任意）名前でカウンタを指定します。
detail	（任意）カウンタの詳細情報をクリアします。
protocol *protocol_name*	（任意）指定したプロトコルのカウンタをクリアします。
summary	（任意）カウンタの要約をクリアします。
threshold *N*	（任意）指定されたしきい値以上になっているカウンタをクリアします。指定できる範囲は 1 ～ 4294967295 です。
top *N*	（任意）指定されたしきい値以上になっているカウンタをクリアします。指定できる範囲は 1 ～ 4294967295 です。

デフォルト

clear counters summary detail がデフォルトです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次に、プロトコル スタック カウンタをクリアする例を示します。

```
hostname(config)# clear counters
```

関連コマンド

コマンド	説明
show counters	プロトコル スタック カウンタを表示します。

clear crashinfo

フラッシュ メモリ内のクラッシュ ファイルの内容を削除するには、特権 EXEC モードで **clear crashinfo** コマンドを使用します。

clear crashinfo

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次のコマンドは、クラッシュ ファイルの削除方法を示しています。

```
hostname# clear crashinfo
```

関連コマンド

crashinfo force	セキュリティ アプライアンスを強制的にクラッシュさせます。
crashinfo save disable	フラッシュ メモリにクラッシュ情報を書き込めないようにします。
crashinfo test	セキュリティ アプライアンスでフラッシュ メモリ内のファイルにクラッシュ情報を保存できるかどうかをテストします。
show crashinfo	フラッシュ メモリに格納されているクラッシュ ファイルの内容を表示します。

clear crypto accelerator statistics

クリプト アクセラレータ MIB からグローバルな統計情報およびアクセラレータ固有の統計情報をクリアするには、特権 EXEC モードで **clear crypto accelerator statistics** コマンドを使用します。

clear crypto accelerator statistics

構文の説明

このコマンドには、キーワードや変数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、グローバル コンフィギュレーション モードで、クリプト アクセラレータの統計情報を表示する例を示します。

```
hostname(config)# clear crypto accelerator statistics
hostname(config)#
```

関連コマンド

コマンド	説明
clear crypto protocol statistics	暗号アクセラレータ MIB にあるプロトコル固有の統計情報をクリアします。
show crypto accelerator statistics	暗号アクセラレータ MIB にあるグローバルおよびアクセラレータ固有の統計情報を表示します。
show crypto protocol statistics	暗号アクセラレータ MIB からプロトコル固有の統計情報を表示します。

clear crypto ca crls

指定したトラストポイントに関連付けられているすべての CRL の CRL キャッシュ、またはすべての CRL の CRL キャッシュを削除するには、特権 EXEC モードで **clear crypto ca crls** コマンドを使用します。

clear crypto ca crls [*trustpointname*]

構文の説明

trustpointname	（任意）トラストポイントの名前。名前を指定しない場合、このコマンドはシステム上のキャッシュされた CRL をすべてクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、グローバル コンフィギュレーション モードで発行され、セキュリティ アプライアンスからすべての CRL のすべての CRL キャッシュを削除する例を示します。

```
hostname# clear crypto ca crls
hostname#
```

関連コマンド

コマンド	説明
crypto ca crl request	トラストポイントの CRL コンフィギュレーションに基づいて CRL をダウンロードします。
show crypto ca crls	キャッシュされたすべての CRL、または指定したトラストポイントのキャッシュされた CRL を表示します。

clear crypto ipsec sa

IPSec SA のカウンタ、エントリ、クリプト マップ、またはピア接続を削除するには、特権 EXEC モードで **clear crypto ipsec sa** コマンドを使用します。すべての IPSec SA をクリアするには、このコマンドを引数なしで使用します。

clear [crypto] ipsec sa [counters | entry {*hostname* | *ip_address*} **{esp | ah}** *spi* **| map** *map name* **| peer** {*hostname* | *ip_address*}**]**

このコマンドを使用するときは注意してください。

構文の説明

ah	認証ヘッダー。
counters	各 SA 統計情報のすべての IPSec をクリアします。
entry	指定した IP アドレス、ホスト名、プロトコル、および SPI 値に一致するトンネルを削除します。
esp	暗号化セキュリティ プロトコル。
hostname	IP アドレスに割り当てられたホスト名を指定します。
ip_address	IP アドレスを指定します。
map	マップ名で識別される、指定したクリプト マップに関連付けられているすべてのトンネルを削除します。
map name	クリプト マップを識別する英数字ストリング。最大 64 文字です。
peer	指定したホスト名または IP アドレスで識別されるピアへのすべての IPSec SA を削除します。
spi	セキュリティ パラメータ インデックス（16 進数）を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、グローバル コンフィギュレーション モードで、セキュリティ アプライアンスからすべての IPSec SA を削除する例を示します。

```
hostname# clear crypto ipsec sa
hostname#
```

次に、グローバル コンフィギュレーション モードで、10.86.1.1 のピア IP アドレスを持つ SA を削除する例を示します。

```
hostname# clear crypto ipsec peer 10.86.1.1
hostname#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべてまたは指定されたクリプト マップをコンフィギュレーションからクリアします。
clear configure isakmp	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
show ipsec sa	カウンタ、エントリ、マップ名、ピア IP アドレス、ホスト名などの IPSec SA に関する情報を表示します。
show running-config crypto	IPSec、クリプト マップ、ダイナミック クリプト マップ、ISAKMP など暗号コンフィギュレーション全体を表示します。

clear crypto protocol statistics

クリプト アクセラレータ MIB 内のプロトコル固有の統計情報をクリアするには、特権 EXEC モードで **clear crypto protocol statistics** コマンドを使用します。

clear crypto protocol statistics *protocol*

構文の説明

protocol	統計情報をクリアするプロトコルの名前を指定します。プロトコルの選択肢は次のとおりです。 • **ikev1**：インターネット キー交換バージョン 1。 • **ipsec**：IP セキュリティ フェーズ 2 プロトコル。 • **ssl**：Secure Socket Layer。 • **other**：新規プロトコル用に予約済み。 • **all**：現在サポートされているすべてのプロトコル。 このコマンドのオンライン ヘルプでは、今後のリリースでサポートされる他のプロトコルが表示される場合があります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、グローバル コンフィギュレーション モードで、すべてのクリプト アクセラレータの統計情報をクリアする例を示します。

```
hostname# clear crypto protocol statistics all
hostname#
```

関連コマンド

コマンド	説明
clear crypto accelerator statistics	暗号アクセラレータ MIB にあるグローバルおよびアクセラレータ固有の統計情報をクリアします。

コマンド	説明
show crypto accelerator statistics	暗号アクセラレータ MIB からグローバルおよびアクセラレータ固有の統計情報を表示します。
show crypto protocol statistics	クリプト アクセラレータ MIB のプロトコル固有の統計情報を表示します。

clear dhcpd

DHCP サーバのバインディングおよび統計情報をクリアするには、特権 EXEC モードで **clear dhcp** コマンドを使用します。

clear dhcpd {**binding** [*ip_address*] | **statistics**}

構文の説明

binding	クライアント アドレスのすべてのバインディングをクリアします。
ip_address	（任意）指定した IP アドレスのバインディングをクリアします。
statistics	統計情報カウンタをクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

オプションの IP アドレスを **clear dhcpd binding** コマンドに含めた場合は、その IP アドレスのバインディングだけがクリアされます。

すべての DHCP サーバ コマンドをクリアするには、**clear configure dhcpd** コマンドを使用します。

例

次に、**dhcpd** 統計情報をクリアする例を示します。

```
hostname# clear dhcpd statistics
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
show dhcpd	DHCP のバインディング、統計情報、または状態情報を表示します。

clear dhcprelay statistics

DHCP リレー統計情報カウンタをクリアするには、特権 EXEC モードで **clear dhcprelay statistics** コマンドを使用します。

clear dhcprelay statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

clear dhcprelay statistics コマンドは、DHCP リレー統計情報カウンタだけをクリアします。DHCP リレー コンフィギュレーション全体をクリアするには、**clear configure dhcprelay** コマンドを使用します。

例

次に、DHCP リレー統計情報をクリアする例を示します。

```
hostname# clear dhcprelay statistics
hostname#
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
debug dhcprelay	DHCP リレー エージェントのデバッグ情報を表示します。
show dhcprelay statistics	DHCP リレー エージェントの統計情報を表示します。
show running-config dhcprelay	DHCP リレー エージェントの現在のコンフィギュレーションを表示します。

clear dns-hosts cache

DNS キャッシュをクリアするには、特権 EXEC モードで **clear dns-hosts cache** コマンドを使用します。このコマンドは、**name** コマンドで追加したスタティック エントリをクリアしません。

clear dns-hosts cache

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、DNS キャッシュをクリアする例を示します。

```
hostname# clear dns-hosts cache
```

関連コマンド

コマンド	説明
dns domain-lookup	セキュリティ アプライアンスによるネーム ルックアップの実行をイネーブルにします。
dns name-server	DNS サーバ アドレスを設定します。
dns retries	セキュリティ アプライアンスが応答を受信しないときに、DNS サーバのリストを再試行する回数を指定します。
dns timeout	次の DNS サーバを試行するまでに待機する時間を指定します。
show dns-hosts	DNS キャッシュを表示します。

clear eigrp events

EIGRP イベント ログをクリアするには、特権 EXEC モードで **clear eigrp events** コマンドを使用します。

clear eigrp [*as-number*] **events**

構文の説明

as-number	（任意）イベント ログをクリアする EIGRP プロセスの自律システム番号を指定します。セキュリティ アプライアンスでサポートされる EIGRP ルーティング プロセスは 1 つだけであるため、自律システム番号（プロセス ID）を指定する必要はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(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

show eigrp events コマンドを使用して、EIGRP イベント ログを表示できます。

例

次に、EIGRP イベント ログをクリアする例を示します。

```
hostname# clear eigrp events
```

関連コマンド

コマンド	説明
show eigrp events	EIGRP イベント ログを表示します。

clear eigrp neighbors

EIGRP ネイバー テーブルからエントリを削除するには、特権 EXEC モードで **clear eigrp neighbors** コマンドを使用します。

clear eigrp [*as-number*] **neighbors** [*ip-addr* | *if-name*] [**soft**]

構文の説明

as-number	（任意）ネイバー エントリを削除する EIGRP プロセスの自律システム番号を指定します。セキュリティ アプライアンスでサポートされる EIGRP ルーティング プロセスは 1 つだけであるため、自律システム番号（プロセス ID）を指定する必要はありません。
if-name	（任意）**nameif** コマンドで指定されたインターフェイスの名前。インターフェイス名を指定すると、このインターフェイスを介して学習されたすべてのネイバー テーブル エントリが削除されます。
ip-addr	（任意）ネイバー テーブルから削除するネイバーの IP アドレス。
soft	セキュリティ アプライアンスは、隣接関係をリセットすることなくネイバーと再同期されます。

デフォルト

ネイバー IP アドレスまたはインターフェイス名を指定しない場合は、すべてのダイナミック エントリがネイバー テーブルから削除されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(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

clear eigrp neighbors コマンドは、**neighbor** コマンドを使用して定義されたネイバーをネイバー テーブルから削除しません。ダイナミックに検出されたネイバーだけが削除されます。

show eigrp neighbors コマンドを使用して、EIGRP ネイバー テーブルを表示できます。

例

次に、EIGRP ネイバー テーブルからすべてのエントリを削除する例を示します。

```
hostname# clear eigrp neighbors
```

次に、「outside」という名前のインターフェイスを介して学習されたすべてのエントリを EIGRP ネイバー テーブルから削除する例を示します。

```
hostname# clear eigrp neighbors outside
```

関連コマンド

コマンド	説明
debug eigrp neighbors	EIGRP ネイバーのデバッグ情報を表示します。
debug ip eigrp	EIGRP プロトコル パケットのデバッグ情報を表示します。
show eigrp neighbors	EIGRP ネイバー テーブルを表示します。

clear eigrp topology

EIGRP トポロジ テーブルからエントリを削除するには、特権 EXEC モードで **clear eigrp topology** コマンドを使用します。

clear eigrp [*as-number*] **topology** *ip-addr* [*mask*]

構文の説明

as-number	（任意）EIGRP プロセスの自律システム番号を指定します。セキュリティ アプライアンスでサポートされる EIGRP ルーティング プロセスは 1 つだけであるため、自律システム番号（プロセス ID）を指定する必要はありません。
ip-addr	トポロジ テーブルからクリアする IP アドレス。
mask	（任意）*ip-addr* 引数に適用するネットワーク マスク。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(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

このコマンドは、EIGRP トポロジ テーブルから既存の EIGRP エントリをクリアします。**show eigrp topology** コマンドを使用して、トポロジ テーブルのエントリを表示できます。

例

次に、EIGRP トポロジ テーブルから 192.168.1.0 ネットワークのエントリを削除する例を示します。

```
hostname# clear eigrp topology 192.168.1.0 255.255.255.0
```

関連コマンド

コマンド	説明
show eigrp topology	EIGRP トポロジ テーブルを表示します。

clear failover statistics

フェールオーバー統計情報カウンタをクリアするには、特権 EXEC モードで **clear failover statistics** コマンドを使用します。

clear failover statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、**show failover statistics** コマンドで表示される統計情報、および **show failover** コマンド出力の Stateful Failover Logical Update Statistics セクションのカウンタをクリアします。フェールオーバー コンフィギュレーションを削除するには、**clear configure failover** コマンドを使用します。

例

次に、フェールオーバー統計情報カウンタをクリアする例を示します。

```
hostname# clear failover statistics
hostname#
```

関連コマンド

コマンド	説明
debug fover	フェールオーバー デバッグ情報を表示します。
show failover	フェールオーバー コンフィギュレーションおよび動作統計に関する情報を表示します。

clear fragment

IP フラグメント再構築モジュールの動作データをクリアするには、特権 EXEC モードで **clear fragment** コマンドを入力します。このコマンドは、現在キューに入っている再構築待機中のフラグメント（**queue** キーワードが入力されている場合）、またはすべての IP フラグメント再構築統計情報（**statistics** キーワードが入力されている場合）のいずれかをクリアします。統計情報は、再構築に成功したフラグメント チェーンの数、再構築に失敗したチェーンの数、および最大サイズの超過によってバッファ オーバーフローが発生した回数を示すカウンタです。

clear fragment {**queue** | **statistics**} [*interface*]

構文の説明

interface	（任意）セキュリティ アプライアンスのインターフェイスを指定します。
queue	IP フラグメント再構築キューをクリアします。
statistics	IP フラグメント再構築統計情報をクリアします。

デフォルト

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。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、コンフィギュレーション データのクリアを動作データのクリアと区別するために、**clear fragment** および **clear configure fragment** という 2 つのコマンドに分けられました。

例

次に、IP フラグメント再構築モジュールの動作データをクリアする例を示します。

```
hostname# clear fragment queue
```

関連コマンド

コマンド	説明
clear configure fragment	IP フラグメント再構成コンフィギュレーションをクリアし、デフォルトにリセットします。
fragment	パケット フラグメンテーションを詳細に管理できるようにし、NFS との互換性を高めます。
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。

clear gc

ガーベッジ コレクション プロセスの統計情報を削除するには、特権 EXEC モードで **clear gc** コマンドを使用します。

clear gc

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、ガーベッジ コレクション プロセスの統計情報を削除する例を示します。

```
hostname# clear gc
```

関連コマンド

コマンド	説明
show gc	ガーベッジ コレクション プロセスの統計情報を表示します。

clear igmp counters

すべての IGMP カウンタをクリアするには、特権 EXEC モードで **clear igmp counters** コマンドを使用します。

clear igmp counters [*if_name*]

構文の説明

if_name	**nameif** コマンドで指定されたインターフェイス名。このコマンドにインターフェイス名を含めると、指定したインターフェイスのカウンタだけがクリアされます。

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、IGMP 統計情報カウンタをクリアする例を示します。

```
hostname# clear igmp counters
```

関連コマンド

コマンド	説明
clear igmp group	IGMP グループ キャッシュから、検出されたグループをクリアします。
clear igmp traffic	IGMP トラフィック カウンタをクリアします。

clear igmp group

検出されたグループを IGMP グループ キャッシュからクリアするには、特権 EXEC モードで **clear igmp** コマンドを使用します。

clear igmp group [*group* | **interface** *name*]

構文の説明

group	IGMP グループ アドレス。特定のグループを指定すると、そのグループがキャッシュから削除されます。
interface *name*	**namif** コマンドで指定されたインターフェイス名。指定した場合は、そのインターフェイスに関連付けられたすべてのグループが削除されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

グループまたはインターフェイスを指定しない場合は、すべてのインターフェイスからすべてのグループがクリアされます。グループを指定した場合は、そのグループのエントリだけがクリアされます。インターフェイスを指定した場合は、そのインターフェイスのすべてのグループがクリアされます。グループとインターフェイスの両方を指定した場合は、指定したインターフェイスの指定したグループだけがクリアされます。

このコマンドは、スタティックに設定されたグループをクリアしません。

例

次に、検出されたすべての IGMP グループを IGMP グループ キャッシュからクリアする例を示します。

```
hostname# clear igmp group
```

関連コマンド

コマンド	説明
clear igmp counters	すべての IGMP カウンタをクリアします。
clear igmp traffic	IGMP トラフィック カウンタをクリアします。

clear igmp traffic

IGMP トラフィック カウンタをクリアするには、特権 EXEC モードで **clear igmp traffic** コマンドを使用します。

clear igmp traffic

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、IGMP 統計情報トラフィック カウンタをクリアする例を示します。

```
hostname# clear igmp traffic
```

関連コマンド

コマンド	説明
clear igmp group	IGMP グループ キャッシュから、検出されたグループをクリアします。
clear igmp counters	すべての IGMP カウンタをクリアします。

clear interface

インターフェイス統計情報をクリアするには、特権 EXEC モードで **clear interface** コマンドを使用します。

clear interface [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*]

構文の説明

interface_name	（任意）**nameif** コマンド内にインターフェイス名のセットを指定します。
mapped_name	（任意）**allocate-interface** コマンドを使用してマッピング名を割り当てた場合、マルチ コンテキスト モードでその名前を指定します。
physical_interface	（任意）**gigabiternet0/1** などのインターフェイス ID を指定します。有効値については、**interface** コマンドを参照してください。
subinterface	（任意）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。

デフォルト

デフォルトでは、このコマンドはすべてのインターフェイス統計情報をクリアします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

インターフェイスがコンテキスト間で共有されている場合にコンテキスト内でこのコマンドを入力すると、セキュリティ アプライアンスは現在のコンテキストの統計情報だけをクリアします。システム実行スペースでこのコマンドを入力した場合、セキュリティ アプライアンスは結合された統計情報をクリアします。

インターフェイス名は、システム実行スペースでは使用できません。これは、**nameif** コマンドはコンテキスト内だけで使用できるためです。同様に、**allocate-interface** コマンドを使用してインターフェイス ID をマッピング名にマッピングした場合、そのマッピング名はコンテキスト内だけで使用できます。

例

次に、すべてのインターフェイス統計情報をクリアする例を示します。

```
hostname# clear interface
```

関連コマンド

コマンド	説明
clear configure interface	インターフェイス コンフィギュレーションをクリアします。
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	インターフェイスの設定を表示します。

clear ip audit count

監査ポリシーのシグニチャ一致の数をクリアするには、特権 EXEC モードで **clear ip audit count** コマンドを使用します。

clear ip audit count [**global** | **interface** *interface_name*]

構文の説明

global	（デフォルト）すべてのインターフェイスの一致数をクリアします。
interface *interface_name*	（任意）指定したインターフェイスの一致数をクリアします。

デフォルト

キーワードを指定しない場合、このコマンドはすべてのインターフェイスの一致をクリアします（**global**）。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、すべてのインターフェイスの数をクリアする例を示します。

```
hostname# clear ip audit count
```

関連コマンド

コマンド	説明
ip audit interface	監査ポリシーをインターフェイスに割り当てます。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
show ip audit count	監査ポリシーのシグニチャ一致の数を表示します。
show running-config ip audit attack	**ip audit attack** コマンドのコンフィギュレーションを表示します。

clear ip verify statistics

ユニキャスト RPF 統計情報をクリアするには、特権 EXEC モードで **clear ip verify statistics** コマンドを使用します。ユニキャスト RPF をイネーブルにする方法については、**ip verify reverse-path** コマンドを参照してください。

clear ip verify statistics [**interface** *interface_name*]

構文の説明

interface *interface_name*	ユニキャスト RPF 統計情報をクリアするインターフェイスを設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、ユニキャスト RPF 統計情報をクリアする例を示します。

```
hostname# clear ip verify statistics
```

関連コマンド

コマンド	説明
clear configure ip verify reverse-path	**ip verify reverse-path** コンフィギュレーションをクリアします。
ip verify reverse-path	IP スプーフィングを防ぐユニキャスト リバース パス転送機能をイネーブルにします。
show ip verify statistics	ユニキャスト RPF 統計情報を表示します。
show running-config ip verify reverse-path	**ip verify reverse-path** コンフィギュレーションを表示します。

clear ipsec sa

IPSec SA を完全にクリアするには、または指定したパラメータに基づいてクリアするには、特権 EXEC モードで **clear ipsec sa** コマンドを使用します。代替の形式である **clear crypto ipsec sa** も使用できます。

clear ipsec sa [**counters** | **entry** *peer-addr protocol spi* | **peer** *peer-addr* | **map** *map-name*]

構文の説明

counters	（任意）すべてのカウンタをクリアします。
entry	（任意）指定した IPSec ピア、プロトコル、および SPI の IPSec SA をクリアします。
map *map-name*	（任意）指定したクリプト マップの IPSec SA をクリアします。
peer	（任意）指定したピアの IPSec SA をクリアします。
peer-addr	IPSec ピアの IP アドレスを指定します。
protocol	IPSec プロトコル **esp** または **ah** を指定します。
spi	IPSec SPI を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、グローバル コンフィギュレーション モードで、すべての IPSec SA カウンタをクリアする例を示します。

```
hostname# clear ipsec sa counters
hostname#
```

関連コマンド

コマンド	説明
show ipsec sa	指定されたパラメータに基づいて IPSec SA を表示します。
show ipsec stats	IPSec フロー MIB のグローバル IPSec 統計情報を表示します。

clear ipv6 access-list counters

IPv6 アクセス リスト統計情報カウンタをクリアするには、特権 EXEC モードで **clear ipv6 access-list counters** コマンドを使用します。

clear ipv6 access-list *id* **counters**

構文の説明

id	IPv6 アクセス リストの識別子。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、IPv6 アクセス リスト 2 の統計情報データをクリアする例を示します。

```
hostname# clear ipv6 access-list 2 counters
hostname#
```

関連コマンド

コマンド	説明
clear configure ipv6	現在のコンフィギュレーションから **ipv6 access-list** コマンドをクリアします。
ipv6 access-list	IPv6 アクセス リストを設定します。
show ipv6 access-list	現在のコンフィギュレーション内の **ipv6 access-list** コマンドを表示します。

clear ipv6 mld traffic

IPv6 Multicast Listener Discovery（MLD; マルチキャスト リスナー検出）トラフィック カウンタをクリアするには、特権 EXEC モードで **clear ipv6 mld traffic** コマンドを使用します。

clear ipv6 mld traffic

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(4)	このコマンドが導入されました。

使用上のガイドライン

clear ipv6 mld traffic コマンドを使用すると、すべてのマルチキャスト リスナー検出トラフィック カウンタをリセットできます。

例

次に、IPv6 マルチキャスト リスナー検出のトラフィック カウンタをクリアする例を示します。

```
hostname# clear ipv6 mld traffic
hostname#
```

関連コマンド

コマンド	説明
debug ipv6 mld	マルチキャスト リスナー検出のすべてのデバッグ メッセージを表示します。
show debug ipv6 mld	現在のコンフィギュレーション内の **ipv6** マルチキャスト リスナー検出コマンドを表示します。

clear ipv6 neighbors

IPv6 ネイバー探索キャッシュをクリアするには、特権 EXEC モードで **clear ipv6 neighbors** コマンドを使用します。

clear ipv6 neighbors

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、検出されたすべての IPv6 ネイバーをキャッシュから削除します。スタティック エントリは削除しません。

例

次に、IPv6 ネイバー探索キャッシュのすべてのエントリ（スタティック エントリは除く）を削除する例を示します。

```
hostname# clear ipv6 neighbors
hostname#
```

関連コマンド

コマンド	説明
ipv6 neighbor	IPv6 探索キャッシュ内のスタティック エントリを設定します。
show ipv6 neighbor	IPv6 ネイバー キャッシュ情報を表示します。

clear ipv6 traffic

IPv6 トラフィック カウンタをリセットするには、特権 EXEC モードで **clear ipv6 traffic** コマンドを使用します。

clear ipv6 traffic

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、**show ipv6 traffic** コマンドの出力内のカウンタがリセットされます。

例

次に、IPv6 トラフィック カウンタをリセットする例を示します。**ipv6 traffic** コマンドの出力には、カウンタがリセットされたことが示されています。

```
hostname# clear ipv6 traffic
hostname# show ipv6 traffic
IPv6 statistics:
  Rcvd:  1 total, 1 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  1 generated, 0 forwarded
         0 fragmented into 0 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
  Mcast: 0 received, 0 sent

ICMP statistics:
  Rcvd: 1 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
```

```
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 1 neighbor advert
  Sent: 1 output
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 1 neighbor advert

UDP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 0 output

TCP statistics:
  Rcvd: 0 input, 0 checksum errors
  Sent: 0 output, 0 retransmitted
```

関連コマンド

コマンド	説明
show ipv6 traffic	IPv6 トラフィックの統計情報を表示します。

clear isakmp sa

すべての IKE ランタイム SA データベースを削除するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **clear isakmp sa** コマンドを使用します。

clear isakmp sa

構文の説明

このコマンドにはキーワードまたは引数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	**clear isakmp sa** コマンドが、**clear crypto isakmp sa** に変更されました。

例

次に、コンフィギュレーションから IKE ランタイム SA データベースを削除する例を示します。

```
hostname# clear isakmp sa
hostname#
```

関連コマンド

コマンド	説明
clear isakmp	IKE ランタイム SA データベースをクリアします。
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show isakmp stats	実行時統計情報を表示します。
show isakmp sa	追加情報を含め、IKE ランタイム SA データベースを表示します。
show running-config isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

clear local-host

show local-host コマンドを入力することによって表示されるローカル ホストからネットワーク接続を解放するには、特権 EXEC モードで **clear local-host** コマンドを使用します。

clear local-host [*ip_address*] [**all**]

構文の説明

all	（任意）セキュリティ アプライアンスへの接続およびセキュリティ アプライアンスからの接続を含むローカル ホスト状態のホストが作成した接続を消去することを指定します。
ip_address	（任意）ローカル ホストの IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

clear local-host コマンドは、消去されたホストをライセンス制限から除外します。ライセンス制限にカウントされているホストの数は、**show local-host** コマンドを入力して表示できます。

注意　ローカル ホストのネットワーク状態を消去すると、ローカル ホストに関連するネットワーク接続と xlate がすべて停止します。

例

次の例では、**clear local-host** コマンドでローカル ホストに関する情報を消去する方法を示します。

```
hostname# clear local-host 10.1.1.15
```

情報がクリアされると、ホストが接続を再確立するまで、何も表示されません。

関連コマンド

コマンド	説明
show local-host	ローカル ホストのネットワーク状態を表示します。

clear logging asdm

ASDM ロギング バッファをクリアするには、特権 EXEC モードで **clear logging asdm** コマンドを使用します。

clear logging asdm

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**clear pdm logging** コマンドから **clear asdm log** コマンドに変更されました。

使用上のガイドライン

ASDM システム ログ メッセージは、セキュリティ アプライアンスのシステム ログ メッセージとは別のバッファに格納されます。ASDM ロギング バッファをクリアすると、ASDM システム ログ メッセージだけがクリアされます。セキュリティ アプライアンスのシステム ログ メッセージはクリアされません。ASDM システム ログ メッセージを表示するには、**show asdm log** コマンドを使用します。

例

次に、ASDM ロギング バッファをクリアする例を示します。

```
hostname(config)# clear logging asdm
hostname(config)#
```

関連コマンド

コマンド	説明
show asdm log_sessions	ASDM ロギング バッファの内容を表示します。

clear logging queue

ログ関連のキューをクリアするには、特権 EXEC モードで **clear logging queue** コマンドを使用します。

clear logging queue [bufferwrap]

構文の説明

bufferwrap	FTP およびフラッシュ ログ バッファをクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(5)	このコマンドが導入されました。

例

次に、FTP およびフラッシュ ログ バッファをクリアする例を示します。

```
hostname# clear logging queue bufferwrap
```

関連コマンド

コマンド	説明
logging buffered	ロギング バッファを設定します。
show logging	ロギング情報を表示します。

clear mac-address-table

ダイナミック MAC アドレス テーブル エントリをクリアするには、特権 EXEC モードで **clear mac-address-table** コマンドを使用します。

clear mac-address-table [*interface_name*]

構文の説明

interface_name	（任意）選択したインターフェイスの MAC アドレス テーブル エントリをクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、ダイナミック MAC アドレス テーブルのエントリをクリアする例を示します。

```
hostname# clear mac-address-table
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
firewall transparent	ファイアウォール モードをトランスペアレントに設定します。
mac-address-table aging-time	ダイナミック MAC アドレス エントリのタイムアウトを設定します。
mac-learn	MAC アドレス ラーニングをディセーブルにします。
show mac-address-table	MAC アドレス テーブルのエントリを表示します。

clear memory delayed-free-poisoner

delayed free-memory poisoner ツールのキューと統計情報をクリアするには、特権 EXEC モードで **clear memory delayed-free-poisoner** コマンドを使用します。

clear memory delayed-free-poisoner

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear memory delayed-free-poisoner コマンドは、delayed free-memory poisoner ツールのキューで保持されているすべてのメモリを検証なしでシステムに戻し、関連する統計情報カウンタをクリアします。

例

次に、delayed free-memory poisoner ツールのキューと統計情報をクリアする例を示します。

```
hostname# clear memory delayed-free-poisoner
```

関連コマンド

コマンド	説明
memory delayed-free-poisoner enable	delayed free-memory poisoner ツールをイネーブルにします。
memory delayed-free-poisoner validate	delayed free-memory poisoner ツールのキューを検証します。
show memory delayed-free-poisoner	delayed free-memory poisoner ツールのキューの使用状況に関する要約を表示します。

clear memory profile

メモリ プロファイリング機能によって保持されるメモリ バッファをクリアするには、特権 EXEC モードで **clear memory profile** コマンドを使用します。

clear memory profile [peak]

構文の説明

peak	（任意）ピーク メモリ バッファの内容をクリアします。

デフォルト

デフォルトでは、現在「使用されている」プロファイル バッファをクリアします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear memory profile コマンドは、プロファイリング機能によって保持されているメモリ バッファを解放します。したがって、プロファイリングは、クリアされる前に停止している必要があります。

例

次に、プロファイリング機能によって保持されているメモリ バッファをクリアする例を示します。

```
hostname# clear memory profile
```

関連コマンド

コマンド	説明
memory profile enable	メモリ使用状況（メモリ プロファイリング）のモニタリングをイネーブルにします。
memory profile text	プロファイルするメモリのテキスト範囲を設定します。
show memory profile	セキュリティ アプライアンスのメモリ使用状況（プロファイリング）に関する情報を表示します。

clear mfib counters

MFIB ルータ パケット カウンタをクリアするには、特権 EXEC モードで **clear mfib counters** コマンドを使用します。

clear mfib counters [*group* [*source*]]

構文の説明

group	（任意）マルチキャスト グループの IP アドレスです。
source	（任意）マルチキャスト ルート送信元の IP アドレスです。これは、4 分割ドット付き 10 進表記のユニキャスト IP アドレスです。

デフォルト

このコマンドを引数なしで使用した場合、すべてのルートのルート カウンタがクリアされます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、すべての MFIB ルータ パケット カウンタをクリアする例を示します。

```
hostname# clear mfib counters
```

関連コマンド

コマンド	説明
show mfib count	MFIB ルートおよびパケット カウント データを表示します。

clear module recover

hw-module module recover コマンドで設定された AIP SSM のリカバリ ネットワーク設定をクリアするには、特権 EXEC モードで **clear module recover** コマンドを使用します。

clear module 1 recover

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。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、AIP SSM のリカバリ設定をクリアする例を示します。

```
hostname# clear module 1 recover
```

関連コマンド

コマンド	説明
hw-module module recover	TFTP サーバからリカバリ イメージをロードすることにより、AIP SSM を回復します。
hw-module module reset	SSM 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	AIP SSM 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、SSM ソフトウェアをシャットダウンします。
show module	SSM 情報を表示します。

clear nac-policy

NAC ポリシーの使用状況の統計情報をリセットするには、グローバル コンフィギュレーション モードで **clear nac-policy** コマンドを使用します。

clear nac-policy [*nac-policy-name*]

構文の説明

nac-policy-name	（任意）使用状況の統計情報をリセットする NAC ポリシーの名前。

デフォルト

名前を指定しない場合、CLI は、すべての NAC ポリシーに関する使用状況の統計情報をリセットします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

例

次のコマンドでは、framework1 という名前の NAC ポリシーの使用状況の統計情報をリセットしています。

```
hostname(config)# clear nac-policy framework1
```

次のコマンドでは、NAC ポリシーの使用状況の統計情報をすべてリセットしています。

```
hostname(config)# clear nac-policy
```

関連コマンド

コマンド	説明
show nac-policy	セキュリティ アプライアンスでの NAC ポリシー使用状況の統計情報を表示します。
show vpn-session_summary.db	IPSec セッション、WebVPN セッション、および NAC セッションの数を表示します。
show vpn-session.db	NAC の結果を含む、VPN セッションの情報を表示します。

clear nat counters

NAT ポリシー カウンタをクリアするには、グローバル コンフィギュレーション モードで **clear nat counters** コマンドを使用します。

clear nat counters [*src_if* [*src_ip* [*src_mask*]] [*dst_ifc* [*dst_ip* [*dst_mask*]]]]

構文の説明

dst_ifc	（任意）フィルタリングする宛先インターフェイスを指定します。
dst_ip	（任意）フィルタリングする宛先 IP アドレスを指定します。
dst_mask	（任意）宛先 IP アドレスのマスクを指定します。
src_ifc	（任意）フィルタリングする送信元インターフェイスを指定します。
src_ip	（任意）フィルタリングする送信元 IP アドレスを指定します。
src_mask	（任意）送信元 IP アドレスのマスクを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0 (4)	このコマンドが導入されました。

例

次に、NAT ポリシー カウンタをクリアする例を示します。

```
hostname(config)# clear nat counters
```

関連コマンド

コマンド	説明
nat	別のインターフェイス上にあるマップ済みアドレスに変換する、インターフェイス上のアドレスを識別します。
nat-control	NAT コンフィギュレーション要件をイネーブルまたはディセーブルにします。
show nat counters	プロトコル スタック カウンタを表示します。

clear ospf

OSPF プロセス情報をクリアするには、特権 EXEC モードで **clear ospf** コマンドを使用します。

clear ospf [*pid*] {**process** | **counters** [**neighbor** [*neighbor-intf*] [*neighbr-id*]]}

構文の説明

counters	OSPF カウンタをクリアします。
neighbor	OSPF ネイバー カウンタをクリアします。
neighbor-intf	（任意）OSPF インターフェイス ルータ指定をクリアします。
neighbr-id	（任意）OSPF 隣接ルータ ID をクリアします。
pid	（任意）OSPF ルーティング プロセスの内部使用の ID パラメータ。有効な値は、1 ～ 65535 です。
process	OSPF ルーティング プロセスをクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

このコマンドは、コンフィギュレーションのいずれの部分も削除しません。コンフィギュレーションから特定のコマンドをクリアするには、このコンフィギュレーション コマンドの **no** 形式を使用します。または、コンフィギュレーションからすべてのグローバル OSPF コマンドを削除するには、**clear configure router ospf** コマンドを使用します。

（注）　**clear configure router ospf** コマンドは、インターフェイス コンフィギュレーション モードで入力された OSPF コマンドをクリアしません。

例

次に、OSPF プロセス カウンタをクリアする例を示します。

```
hostname# clear ospf process
```

関連コマンド

コマンド	説明
clear configure router	実行コンフィギュレーションからすべてのグローバル ルータ コマンドをクリアします。

clear pc

PC に保持されている接続情報、xlate 情報、またはローカル ホスト情報をクリアするには、特権 EXEC モードで **clear pc** コマンドを使用します。

clear pc

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、PC 情報をクリアする例を示します。

```
hostname# clear pc
```

関連コマンド

コマンド	説明
clear pclu	PC 論理更新統計情報をクリアします。

clear pclu

PC 論理更新統計情報をクリアするには、特権 EXEC モードで **clear pclu** コマンドを使用します。

clear pclu

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、PC 情報をクリアする例を示します。

```
hostname# clear pclu
```

関連コマンド

コマンド	説明
clear pc	PC に保持されている接続情報、xlate 情報、またはローカル ホスト情報をクリアします。

clear pim counters

PIM トラフィック カウンタをクリアするには、特権 EXEC モードで **clear pim counters** コマンドを使用します。

clear pim counters

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、トラフィック カウンタだけをクリアします。PIM トポロジ テーブルをクリアするには、**clear pim topology** コマンドを使用します。

例

次に、PIM トラフィック カウンタをクリアする例を示します。

```
hostname# clear pim counters
```

関連コマンド

コマンド	説明
clear pim reset	リセット時の MRIB 同期を必須にします。
clear pim topology	PIM トポロジ テーブルをクリアします。
show pim traffic	PIM トラフィック カウンタを表示します。

clear pim reset

リセットによって MRIB 同期を強制するには、特権 EXEC モードで **clear pim reset** コマンドを使用します。

clear pim reset

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

トポロジ テーブルのすべての情報がクリアされ、MRIB 接続がリセットされます。このコマンドは、PIM トポロジ テーブルと MRIB データベース間の状態を同期するために使用できます。

例

次に、トポロジ テーブルをクリアし、MRIB 接続をリセットする例を示します。

```
hostname# clear pim reset
```

関連コマンド

コマンド	説明
clear pim counters	PIM カウンタおよび統計情報をクリアします。
clear pim topology	PIM トポロジ テーブルをクリアします。
clear pim counters	PIM トラフィック カウンタをクリアします。

clear pim topology

PIM トポロジ テーブルをクリアするには、特権 EXEC モードで **clear pim topology** コマンドを使用します。

clear pim topology [*group*]

構文の説明

group	（任意）トポロジ テーブルから削除するマルチキャスト グループのアドレスまたは名前を指定します。

デフォルト

オプションの *group* 引数を指定しない場合、トポロジ テーブルからすべてのエントリがクリアされます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、PIM トポロジ テーブルから既存の PIM ルートをクリアします。IGMP ローカル メンバーシップなど、MRIB テーブルから取得した情報は保持されます。マルチキャスト グループを指定した場合は、それらのグループ エントリだけがクリアされます。

例

次に、PIM トポロジ テーブルをクリアする例を示します。

```
hostname# clear pim topology
```

関連コマンド

コマンド	説明
clear pim counters	PIM カウンタおよび統計情報をクリアします。
clear pim reset	リセット時の MRIB 同期を必須にします。
clear pim counters	PIM トラフィック カウンタをクリアします。

clear priority-queue statistics

任意のインターフェイスまたは設定されたすべてのインターフェイスのプライオリティ キュー統計情報カウンタをクリアするには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **clear priority-queue statistics** コマンドを使用します。

clear priority-queue statistics [*interface-name*]

構文の説明

interface-name	（任意）ベストエフォート キューおよび低遅延キューの詳細を表示するインターフェイスの名前を指定します。

デフォルト

インターフェイス名を省略した場合、このコマンドは設定されたすべてのインターフェイスのプライオリティ キュー統計情報をクリアします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、特権 EXEC モードで **clear priority-queue statistics** コマンドを使用して、「test」という名前のインターフェイスのプライオリティ キュー統計情報を削除する例を示します。

```
hostname# clear priority-queue statistics test
hostname#
```

関連コマンド

コマンド	説明
clear configure priority queue	指定されたインターフェイスからプライオリティ キュー コンフィギュレーションを削除します。
priority-queue	インターフェイスにプライオリティ キューイングを設定します。
show priority-queue statistics	指定したインターフェイスまたはすべてのインターフェイスのプライオリティ キュー統計情報を表示します。
show running-config priority-queue	指定したインターフェイスの現在のプライオリティ キュー コンフィギュレーションを表示します。

clear resource usage

リソース使用状況の統計情報をクリアするには、特権 EXEC モードで **clear resource usage** コマンドを使用します。

clear resource usage [**context** *context_name* | **all** | **summary** | **system**] [**resource** {[**rate**] *resource_name* | **all**}]

構文の説明

context *context_name*	（マルチ モードのみ）統計情報をクリアするコンテキスト名を指定します。すべてのコンテキストを対象にする場合は、**all**（デフォルト）を指定します。
resource [**rate**] *resource_name*	特定のリソースの使用状況をクリアします。すべてのリソースを対象にするには、**all**（デフォルト）を指定します。リソース使用状況のレートをクリアする場合は、**rate** を指定します。比率で測定されるリソースには、**conns**、**inspects**、および **syslogs** があります。これらのリソース タイプを指定する場合は、**rate** キーワードを指定する必要があります。conns リソースは、同時接続としても測定されます。1 秒あたりの接続を表示するには、**rate** キーワードのみを使用します。 リソースには、次のタイプがあります。 • **asdm**：ASDM 管理セッション。 • **conns**：1 つのホストと複数のその他のホスト間の接続を含む 2 つのホスト間の TCP または UDP 接続。 • **inspects**：アプリケーション インスペクション。 • **hosts**：セキュリティ アプライアンスを通じて接続可能なホスト。 • **mac-addresses**：トランスペアレント ファイアウォール モードで、MAC アドレス テーブルに含められる MAC アドレスの数。 • **ssh**：SSH セッション。 • **syslogs**：システム ログ メッセージ。 • **telnet**：Telnet セッション。 • **xlates**：NAT 変換。
summary	（マルチ モードのみ）結合されたコンテキスト統計情報をクリアします。
system	（マルチ モードのみ）システム全体（グローバル）の使用状況の統計情報をクリアします。

デフォルト

マルチ コンテキスト モードの場合、デフォルトのコンテキストは **all** で、これにより、すべてのコンテキストのリソース使用状況がクリアされます。シングル モードの場合、コンテキスト名は無視され、すべてのリソース統計情報がクリアされます。

デフォルトのリソース名は **all** で、これにより、すべてのリソース タイプがクリアされます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、すべてのコンテキストの、すべてのリソース使用状況の統計情報（システム全体の使用状況の統計情報は除く）をクリアする例を示します。

```
hostname# clear resource usage
```

次に、システム全体の使用状況の統計情報をクリアする例を示します。

```
hostname# clear resource usage system
```

関連コマンド

コマンド	説明
context	セキュリティ コンテキストを追加します。
show resource types	リソース タイプのリストを表示します。
show resource usage	セキュリティ アプライアンスのリソース使用状況を表示します。

clear route

ダイナミックに学習されたルートをコンフィギュレーションから削除するには、特権 EXEC モードで **clear route** コマンドを使用します。

clear route [*interface_name*]

構文の説明

interface_name	（任意）内部または外部のネットワーク インターフェイス名。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、ダイナミックに学習されたルートを削除する例を示します。

```
hostname# clear route
```

関連コマンド

コマンド	説明
route	インターフェイスのスタティック ルートまたはデフォルト ルートを指定します。
show route	ルート情報を表示します。
show running-config route	設定されているルートを表示します。

clear service-policy

イネーブルになっているポリシーの動作データまたは統計情報（存在する場合）をクリアするには、特権 EXEC モードで **clear service-policy** コマンドを使用します。インスペクション エンジンのサービス ポリシーの統計情報をクリアする方法については、**clear service-policy inspect** コマンドを参照してください。

clear service-policy [**global** | **interface** *intf*]

構文の説明

global	（任意）グローバル サービス ポリシーの統計情報をクリアします。
interface *intf*	（任意）特定のインターフェイスのサービス ポリシーの統計情報をクリアします。

デフォルト

デフォルトでは、このコマンドは、すべてのイネーブルなサービス ポリシーのすべての統計情報をクリアします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**clear service-policy** コマンドの構文例を示します。

```
hostname# clear service-policy outside_security_map interface outside
```

関連コマンド

コマンド	説明
clear service-policy inspect gtp	GTP インスペクション エンジンのサービス ポリシーの統計情報をクリアします。
clear service-policy inspect radius-accounting	RADIUS アカウンティング インスペクション エンジンのサービス ポリシーの統計情報をクリアします。
show service-policy	サービス ポリシーを表示します。
show running-config service-policy	実行コンフィギュレーションに設定されているサービス ポリシーを表示します。
clear configure service-policy	サービス ポリシーのコンフィギュレーションをクリアします。
service-policy	サービス ポリシーを設定します。

clear service-policy inspect gtp

グローバル GTP 統計情報をクリアするには、特権 EXEC モードで **clear service-policy inspect gtp** コマンドを使用します。

clear service-policy inspect gtp {**pdp-context** [**all** | **apn** *ap_name* | **imsi** *IMSI_value* | **ms-addr** *IP_address* | **tid** *tunnel_ID* | **version** *version_num*] | **requests** | **statistics** [**gsn** *IP_address*] }

構文の説明

all	すべての GTP PDP コンテキストをクリアします。
apn	（任意）指定した APN に基づいて PDP コンテキストをクリアします。
ap_name	特定のアクセス ポイント名を指定します。
gsn	（任意）GPRS 無線データ ネットワークと他のネットワーク間のインターフェイスである GPRS サポート ノードを指定します。
gtp	（任意）GTP のサービス ポリシーをクリアします。
imsi	（任意）指定した IMSI に基づいて PDP コンテキストをクリアします。
IMSI_value	特定の IMSI を識別する 16 進数値。
interface	（任意）特定のインターフェイスを指定します。
int	情報をクリアするインターフェイスを指定します。
IP_address	統計情報をクリアする IP アドレス。
ms-addr	（任意）指定した MS アドレスに基づいて PDP コンテキストをクリアします。
pdp-context	（任意）パケット データ プロトコル コンテキストを指定します。
requests	（任意）GTP 要求をクリアします。
statistics	（任意）**inspect gtp** コマンドの GTP 統計情報をクリアします。
tid	（任意）指定した TID に基づいて PDP コンテキストをクリアします。
tunnel_ID	特定のトンネルを識別する 16 進数値。
version	（任意）GTP バージョンに基づいて PDP コンテキストをクリアします。
version_num	PDP コンテキストのバージョンを指定します。有効な範囲は 0 ～ 255 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

パケット データ プロトコル コンテキストは、IMSI と NSAPI の組み合わせであるトンネル ID によって識別されます。GTP トンネルは、異なる GSN ノードの 2 つの関連する PDP コンテキストによって定義され、トンネル ID によって識別されます。GTP トンネルは、外部パケット データ ネットワークと Mobile Station（MS; モバイル ステーション）ユーザとの間でパケットを転送する場合に必要です。

例

次に、GTP 統計情報をクリアする例を示します。

```
hostname# clear service-policy inspect gtp statistics
```

関連コマンド

コマンド	説明
debug gtp	GTP インスペクションの詳細情報を表示します。
gtp-map	GTP マップを定義し、GTP 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。
inspect gtp	アプリケーション インスペクションで使用する GTP マップを適用します。
show service-policy inspect gtp	GTP コンフィギュレーションを表示します。
show running-config gtp-map	設定 GTP マップを表示します。

clear service-policy inspect radius-accounting

RADIUS アカウンティング ユーザをクリアするには、特権 EXEC モードで **clear service-policy inspect radius-accounting** コマンドを使用します。

clear service-policy inspect radius-accounting users {**all** | *ip_address* | *policy_map*}

構文の説明

all	すべてのユーザをクリアします。
ip_address	この IP アドレスのユーザをクリアします。
policy_map	このポリシー マップに関連付けられているユーザをクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、すべての RADIUS ユーザをクリアする例を示します。

```
hostname# clear service-policy inspect radius-accounting users all
```

clear shun

現在イネーブルであるすべての shun をディセーブルにして、shun 統計情報をクリアするには、特権 EXEC モードで **clear shun** コマンドを使用します。

clear shun [*statistics*]

構文の説明

statistics	（任意）インターフェイス カウンタだけをクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、現在イネーブルになっているすべての shun をディセーブルにして、shun 統計情報をクリアする例を示します。

```
hostname(config)# clear shun
```

関連コマンド

コマンド	説明
shun	新規接続を抑制し、既存のすべての接続からのパケットを不許可にすることにより、攻撃元ホストへのダイナミック応答をイネーブルにします。
show shun	回避についての情報を表示します。

clear startup-config errors

メモリからコンフィギュレーション エラー メッセージをクリアするには、特権 EXEC モードで **clear startup-config errors** コマンドを使用します。

clear startup-config errors

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスがスタートアップ コンフィギュレーションをロードしたときに生成されたコンフィギュレーション エラーを表示するには、**show startup-config errors** コマンドを使用します。

例

次に、メモリからすべてのコンフィギュレーション エラーをクリアする例を示します。

```
hostname# clear startup-config errors
```

関連コマンド

コマンド	説明
show startup-config errors	セキュリティ アプライアンスがスタートアップ コンフィギュレーションをロードしたときに生成されたコンフィギュレーション エラーを表示します。

clear sunrpc-server active

Sun RPC アプリケーション インスペクションによって開けられたピンホールをクリアするには、特権 EXEC モードで **clear sunrpc-server active** コマンドを使用します。

clear sunrpc-server active

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

Sun RPC アプリケーション インスペクションによって開けられた、NFS や NIS などのサービス トラフィックがセキュリティ アプライアンスを通過できるようにするピンホールをクリアするには、**clear sunrpc-server active** コマンドを使用します。

例

次に、SunRPC サービス テーブルをクリアする例を示します。

```
hostname# clear sunrpc-server
```

関連コマンド

コマンド	説明
clear configure sunrpc-server	セキュリティ アプライアンスからの Sun リモート プロセッサ コール サービスをクリアします。
inspect sunrpc	Sun RPC アプリケーション インスペクションをイネーブルまたはディセーブルにし、使用されるポートを設定します。
show running-config sunrpc-server	SunRPC サービス コンフィギュレーションに関する情報を表示します。
show sunrpc-server active	アクティブな Sun RPC サービスに関する情報を表示します。

clear threat-detection rate

threat-detection basic-threat コマンドを使用して基本的な脅威の検出をイネーブルにした場合は、特権 EXEC モードで **clear threat detection rate** コマンドを使用して統計情報をクリアできます。

clear threat-detection rate

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

例

次に、レート統計情報をクリアする例を示します。

```
hostname# clear threat-detection rate
```

関連コマンド

コマンド	説明
show running-config all threat-detection	脅威検出コンフィギュレーションを表示します。個別にレート設定をしていない場合はデフォルトのレート設定も表示されます。
show threat-detection rate	基本脅威検出の統計情報を表示します。
threat-detection basic-threat	基本脅威検出をイネーブルにします。
threat-detection rate	イベント タイプごとの脅威検出レート制限を設定します。
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。

clear threat-detection scanning-threat

threat-detection scanning-threat コマンドでスキャンによる脅威の検出をイネーブルにしている場合は、特権 EXEC モードで **clear threat-detection scanning-threat** コマンドを使用して、攻撃者および攻撃対象をクリアします。

clear threat-detection scanning-threat [attacker [*ip_address* [*mask*]] | **target** [*ip_address* [*mask*]]

構文の説明

ip_address	（任意）特定の IP アドレスをクリアします。
mask	（任意）サブネット マスクを設定します。
attacker	（任意）攻撃者だけをクリアします。
target	（任意）攻撃対象だけをクリアします。

デフォルト

IP アドレスを指定しなかった場合は、すべてのホストが解放されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(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

現在の攻撃者および攻撃対象を表示するには、**show threat-detection scanning-threat** コマンドを使用します。

例

次に、**show threat-detection scanning-threat** コマンドで攻撃対象と攻撃者を表示し、次にすべての攻撃対象をクリアする例を示します。

```
hostname# show threat-detection scanning-threat
Latest Target Host & Subnet List:
    192.168.1.0
    192.168.1.249
   Latest Attacker Host & Subnet List:
    192.168.10.234
    192.168.10.0
    192.168.10.2
    192.168.10.3
    192.168.10.4
    192.168.10.5
    192.168.10.6
    192.168.10.7
    192.168.10.8
```

```
    192.168.10.9
hostname# clear threat-detection scanning-threat target
```

関連コマンド

コマンド	説明
show threat-detection shun	現在回避されているホストを表示します。
show threat-detection statistics host	ホストの統計情報を表示します。
show threat-detection statistics protocol	プロトコルの統計情報を表示します。
show threat-detection statistics top	上位 10 位までの統計情報を表示します。
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。

clear threat-detection shun

threat-detection scanning-threat コマンドでスキャンによる脅威の検出をイネーブルにし、ホストへの攻撃を自動的に回避している場合は、特権 EXEC モードで **clear threat-detection shun** コマンドを使用して、現在回避されているホストを解放します。

clear threat-detection shun [*ip_address* [*mask*]]

構文の説明

ip_address	（任意）特定の IP アドレスの回避を解除します。
mask	（任意）回避されているホストの IP アドレスのサブネット マスクを設定します。

デフォルト

IP アドレスを指定しなかった場合は、すべてのホストが解放されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(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

現在回避されているホストを表示するには、**show threat-detection shun** コマンドを使用します。

例

次に、**show threat-detection shun** コマンドで現在回避されているホストを表示し、ホスト 10.1.1.6 を回避状態から解放する例を示します。

```
hostname# show threat-detection shun
Shunned Host List:
10.1.1.6
198.1.6.7
hostname# clear threat-detection shun 10.1.1.6 255.255.255.255
```

関連コマンド

コマンド	説明
show threat-detection shun	現在回避されているホストを表示します。
show threat-detection statistics host	ホストの統計情報を表示します。
show threat-detection statistics protocol	プロトコルの統計情報を表示します。
show threat-detection statistics top	上位 10 位までの統計情報を表示します。
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。

clear threat-detection statistics

threat-detection statistics tcp-intercept コマンドで TCP 代行受信の統計情報をイネーブルにしている場合は、特権 EXEC モードで **clear threat-detection scanning-threat** コマンドを使用してこの統計情報をクリアします。

clear threat-detection statistics [tcp-intercept]

構文の説明

tcp-intercept	（任意）TCP 代行受信の統計情報をクリアします。これはデフォルトです。

デフォルト

TCP 代行受信の統計情報をクリアします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが導入されました。

使用上のガイドライン

TCP 代行受信の統計情報を表示するには、**show threat-detection statistics top** コマンドを入力します。

例

次に、**show threat-detection statistics top tcp-intercept** コマンドで TCP 代行受信の統計情報を表示し、次にすべての統計情報をクリアする例を示します。

```
hostname# show threat-detection statistics top tcp-intercept

Top 10 Protected Servers under Attack (sorted by average rate)
Monitoring Window Size: 30 mins    Sampling Interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
------------------------------------------------------------------------------
1    192.168.1.2:5000 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2    192.168.1.3:5000 inside 10 10 6080 10.0.0.200 (0 secs ago)
3    192.168.1.4:5000 inside 2 6 560 10.0.0.200 (59 secs ago)
4    192.168.1.5:5000 inside 1 5 560 10.0.0.200 (59 secs ago)
5    192.168.1.6:5000 inside 1 4 560 10.0.0.200 (59 secs ago)
6    192.168.1.7:5000 inside 0 3 560 10.0.0.200 (59 secs ago)
7    192.168.1.8:5000 inside 0 2 560 10.0.0.200 (59 secs ago)
8    192.168.1.9:5000 inside 0 1 560 10.0.0.200 (59 secs ago)
9    192.168.1.10:5000 inside 0 0 550 10.0.0.200 (2 mins ago)
10   192.168.1.11:5000 inside 0 0 550 10.0.0.200 (5 mins ago)
```

```
hostname# clear threat-detection statistics
```

関連コマンド

コマンド	説明
show threat-detection statistics top	上位 10 位までの統計情報を表示します。
threat-detection statistics	脅威の検出の統計情報をイネーブルにします。

clear traffic

送信アクティビティおよび受信アクティビティのカウンタをリセットするには、特権 EXEC モードで **clear traffic** コマンドを使用します。

clear traffic

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

clear traffic コマンドは、**show traffic** コマンドで表示される送信アクティビティと受信アクティビティのカウンタをリセットします。これらのカウンタは、最後に clear traffic コマンドが入力されてから、またはセキュリティ アプライアンスがオンラインになってからの、各インターフェイスを通過したパケット数およびバイト数を示します。また、秒数は、セキュリティ アプライアンスが最後にリブートされてからオンラインである継続時間を示します。

例

次に、**clear traffic** コマンドの例を示します。

```
hostname# clear traffic
```

関連コマンド

コマンド	説明
show traffic	送信アクティビティおよび受信アクティビティのカウンタを表示します。

clear uauth

1 人のユーザまたはすべてのユーザのキャッシュされた認証および認可情報をすべて削除するには、特権 EXEC モードで **clear uauth** コマンドを使用します。

clear uauth [*username*]

構文の説明

username	（任意）削除するユーザ認証情報をユーザ名で指定します。

デフォルト

ユーザ名を省略すると、すべてのユーザの認証および認可情報が削除されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

clear uauth コマンドは、1 人のユーザまたはすべてのユーザの AAA 認可および認証のキャッシュを削除します。これにより、これらのユーザは、次回接続を作成するときに、再認証を強制されるようになります。

このコマンドは、**timeout** コマンドとともに使用します。

各ユーザ ホストの IP アドレスには、認可キャッシュが付加されます。正しいホストからキャッシュされているサービスにユーザがアクセスしようとした場合、セキュリティ アプライアンスではそのアクセスが事前に許可されていると見なし、その接続を即座に代理します。ある Web サイトへのアクセスを一度認可されると、たとえば、イメージを読み込むときに、イメージごとに認可サーバと通信しません（イメージが同じ IP アドレスからであると想定されます）。この処理により、パフォーマンスが大幅に向上され、認可サーバの負荷が削減されます。

このキャッシュでは、ユーザ ホストごとに 16 個までのアドレスとサービスのペアが許可されます。

（注） Xauth をイネーブルにすると、クライアントに割り当てられている IP アドレスのエントリが uauth テーブル（**show uauth** コマンドで表示できます）に追加されます。ただし、ネットワーク拡張モードで Easy VPN Remote 機能とともに Xauth を使用すると、ネットワーク間に IPSec トンネルが作成されるため、ファイアウォールの向こう側にいるユーザを 1 つの IP アドレスに関連付けることができません。したがって、Xauth の完了時に uauth エントリが作成されません。AAA 認可またはアカウンティング サービスが必要となる場合は、AAA 認証プロキシをイネーブルにして、ファイアウォールの向こう側にいるユーザを認証します。AAA 認証プロキシの詳細については、AAA コマンドを参照してください。

ユーザの接続がアイドルになった後にキャッシュを保持する期間を指定するには、**timeout uauth** コマンドを使用します。すべてのユーザのすべての認可キャッシュを削除するには、**clear uauth** コマンドを使用します。次回接続を作成するときには再認証される必要が生じます。

例

次に、ユーザが再認証されるようにする例を示します。

```
hostname(config)# clear uauth user
```

関連コマンド

コマンド	説明
aaa authentication	**aaa-server** コマンドで指定されたサーバ上の LOCAL、TACACS+、または RADIUS のユーザ認証をイネーブル化、ディセーブル化、または表示します。
aaa authorization	**aaa-server** コマンドで指定されたサーバ上の TACACS+ または RADIUS のユーザ認可をイネーブル化、ディセーブル化、または表示します。
show uauth	現在のユーザ認証および認可情報を表示します。
timeout	アイドル時間の最大継続期間を設定します。

clear url-block block statistics

ブロック バッファ使用状況カウンタをクリアするには、特権 EXEC モードで **clear url-block block statistics** コマンドを使用します。

clear url-block block statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

clear url-block block statistics コマンドは、ブロック バッファ使用状況カウンタ（`Current number of packets held (global)` カウンタは除く）をクリアします。

例

次に、URL ブロック統計情報をクリアし、クリア後のカウンタのステータスを表示する例を示します。

```
hostname# clear url-block block statistics
hostname# show url-block block statistics

URL Pending Packet Buffer Stats with max block  0
--------------------------------------------------------
Cumulative number of packets held: | 0
Maximum number of packets held (per URL): | 0
Current number of packets held (global): | 38
Packets dropped due to
| exceeding url-block buffer limit: | 0
| HTTP server retransmission: | 0
Number of packets released back to client: | 0
```

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 サーバに送ります。

show url-block	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-block	Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバ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 サーバまたは Websense サーバを指定します。

clear url-cache statistics

コンフィギュレーションから **url-cache** コマンド ステートメントを削除するには、特権 EXEC モードで **clear url-cache** コマンドを使用します。

clear url-cache statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

clear url-cache コマンドは、コンフィギュレーションから **url-cache** 統計情報を削除します。

URL キャッシュを使用しても、Websense プロトコル バージョン 1 の Websense アカウンティング ログはアップデートされません。Websense プロトコル バージョン 1 を使用している場合は、Websense を実行してログを記録し、Websense アカウンティング情報を表示できるようにします。セキュリティ ニーズを満たす使用状況プロファイルを取得した後に、| **url-cache** コマンドを入力してスループットを向上させます。Websense プロトコル バージョン 4 および N2H2 URL フィルタリングでは、**url-cache** コマンドの使用時にアカウンティング ログが更新されます。

例

次に、URL キャッシュ統計情報をクリアする例を示します。

```
hostname# clear url-cache statistics
```

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 サーバに送ります。
show url-cache statistics	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間、Web サーバの応答に使用される URL バッファを管理します。

url-cache	N2H2 サーバまたは Websense サーバ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 サーバまたは Websense サーバを指定します。

clear url-server

URL フィルタリング サーバの統計情報をクリアするには、特権 EXEC モードで **clear url-server** コマンドを使用します。

clear url-server statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

clear url-server コマンドは、コンフィギュレーションから URL フィルタリング サーバの統計情報を削除します。

例

次に、URL サーバの統計情報をクリアする例を示します。

```
hostname# clear url-server statistics
```

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 サーバに送ります。
show url-server	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間、Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバ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 サーバまたは Websense サーバを指定します。

clear wccp

WCCP 情報をリセットするには、特権 EXEC モードで **clear wccp** コマンドを使用します。

clear wccp [**web-cache** | *service_number*]

構文の説明

web-cache	Web キャッシュ サービスを指定します。
service-number	ダイナミック サービス ID。このサービスの定義は、キャッシュによって示されます。ダイナミック サービス番号は 0 ～ 254 で、255 個まで使用できます。**web-cache** キーワードで指定される Web キャッシュ サービスを含めると、許可される最大数は 256 個です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、Web キャッシュ サービスの WCCP 情報をリセットする例を示します。

```
hostname# clear wccp web-cache
```

関連コマンド

コマンド	説明
show wccp	WCCP コンフィギュレーションを表示します。
wccp redirect	WCCP リダイレクションのサポートをイネーブルにします。

clear webvpn sso-server statistics

webvpn Single Sign-On（SSO; シングル サインオン）サーバの統計情報をリセットするには、特権 EXEC モードで **clear webvpn sso-server statistics** コマンドを使用します。

clear webvpn sso-server statistics *servername*

構文の説明

servername	無効にする SSO サーバの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
8.0(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

「保留要求」の統計情報はリセットされません。

例

次に、特権 EXEC モードで、クリプト アクセラレータの統計情報を表示する例を示します。

```
hostname # clear webvpn sso-server statistics
hostname #
```

関連コマンド

コマンド	説明
clear crypto accelerator statistics	暗号アクセラレータ MIB にあるグローバルおよびアクセラレータ固有の統計情報をクリアします。
clear crypto protocol statistics	暗号アクセラレータ MIB にあるプロトコル固有の統計情報をクリアします。
show crypto accelerator statistics	暗号アクセラレータ MIB にあるグローバルおよびアクセラレータ固有の統計情報を表示します。
show crypto protocol statistics	暗号アクセラレータ MIB からプロトコル固有の統計情報を表示します。

clear xlate

現在の変換情報および接続情報を消去するには、特権 EXEC モードで **clear xlate** コマンドを使用します。

clear xlate [**global** *ip1*[**-***ip2*] [**netmask** *mask*]] [**local** *ip1*[**-***ip2*] [**netmask** *mask*]]
[**gport** *port1*[**-***port2*]] [**lport** *port1*[**-***port2*]] [**interface** *if_name*] [**state** *state*]

構文の説明

global *ip1*[**-***ip2*]	（任意）グローバル IP アドレスまたはアドレスの範囲を指定して、アクティブな変換をクリアします。
gport *port1*[**-***port2*]	（任意）グローバル ポートまたはポートの範囲を指定して、アクティブな変換をクリアします。
interface *if_name*	（任意）アクティブな変換をインターフェイス別に表示します。
local *ip1*[**-***ip2*]	（任意）ローカル IP アドレスまたはアドレスの範囲を指定して、アクティブな変換をクリアします。
lport *port1*[**-***port2*]	（任意）ローカル ポートまたはポートの範囲を指定して、アクティブな変換をクリアします。
netmask *mask*	（任意）グローバル IP アドレスまたはローカル IP アドレスを限定するネットワーク マスクを指定します。
state *state*	（任意）状態を指定して、アクティブな変換をクリアします。次の 1 つ以上の状態を入力できます。 • **static**：スタティック変換を指定します。 • **portmap**：PAT グローバル変換を指定します。 • **norandomseq**：**norondomseq** 設定での **nat** または**スタティック**変換を指定します。 • **identity**：**nat 0** 識別アドレス変換を指定します。 複数の状態を指定する場合は、状態をスペースで区切ってください。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

clear xlate コマンドは、変換スロットの内容をクリアします（「xlate」は変換スロットを意味します）。変換スロットは、キーの変更が行われた後でも存続できます。コンフィギュレーション内で **aaa-server**、**access-list**、**alias**、**global**、**nat**、**route**、または **static** コマンドを追加、変更、または削除した後には、必ず **clear xlate** コマンドを使用します。

xlate は、NAT または PAT セッションについて記述します。これらのセッションは、**detail** オプションを指定した **show xlate** コマンドで表示できます。xlate には、スタティックとダイナミックという 2 つのタイプがあります。

スタティック xlate は、**static** コマンドを使用して作成される永続的な xlate です。**clear xlate** コマンドは、スタティック エントリ内のホストをクリアしません。スタティック xlate は、コンフィギュレーションから **static** コマンドを削除することによってのみ削除できます。**clear xlate** コマンドは、スタティック変換ルールを削除しません。コンフィギュレーションから static コマンドを削除しても、スタティック ルールを使用する既存の接続はトラフィックを引き続き転送できます。これらの接続を無効にするには、**clear local-host** コマンドを使用します。

ダイナミック xlate は、**nat** コマンドまたは **global** コマンドを介したトラフィック処理で必要に応じて作成される xlate です。**clear xlate** コマンドを実行すると、ダイナミック xlate および関連付けられた接続が削除されます。また、**clear local-host** コマンドを使用して、xlate および関連付けられた接続を消去することもできます。コンフィギュレーションから **nat** コマンドまたは **global** コマンドを削除した場合、ダイナミック xlate および関連する接続がアクティブのまま残る場合があります。これらの接続を削除するには、**clear xlate** コマンドまたは **clear local-host** コマンドを使用します。

例

次に、現在の変換および接続スロット情報をクリアする例を示します。

```
hostname# clear xlate global
```

関連コマンド

コマンド	説明
clear local-host	ローカル ホストのネットワーク情報をクリアします。
clear uauth	キャッシュされたユーザ認証および認可情報をクリアします。
show conn	すべてのアクティブ接続を表示します。
show local-host	ローカル ホスト ネットワーク情報を表示します。
show xlate	現在の変換情報を表示します。