clear f - clear z

clear facility-alarm output

ISA 3000 で出力リレーの電源を切って、LED のアラーム状態をクリアするには、**clear facility-alarm output** コマンドを使用します。

clear facility-alarm output

コマンド履歴

リリース	変更内容
6.3	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、出力リレーの電源を切り、出力 LED のアラーム状態をクリアします。これにより、外部アラームがオフになります。ただし、このコマンドを実行しても、外部アラームをトリガーしたアラーム条件は修正されません。問題を解決する必要があります。現在のアラーム条件を確認するには、**show facility-alarm status** コマンドを使用します。

例

次に、出力リレーの電源を切り、出力 LED のアラーム状態をクリアする例を示します。

```
> clear facility-alarm output
```

関連コマンド

Command	説明
show alarm settings	すべてのグローバル アラーム設定を表示します。
show environment alarm-contact	入力アラーム コンタクトのステータスを表示します。
show facility-alarm	トリガーされたアラームのステータス情報を表示します。

clear failover statistics

高可用性統計情報カウンタをクリアするには、**clear failover statistics** コマンドを使用します。

clear failover statistics

コマンド履歴

リリース	変更内容
6.1	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、**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。

例

次に、高可用性統計情報カウンタをクリアする例を示します。

```
> clear failover statistics
```

関連コマンド

Command	説明
show failover	高可用性構成および動作統計に関する情報を表示します。

clear flow-export counters

NetFlow 統計情報とエラーデータのランタイムカウンタを 0 にリセットするには、**clear flow-export counters** コマンドを使用します。

clear flow-export counters

コマンド履歴

リリース	変更内容
6.3	このコマンドが導入されました。

例

次に、NetFlow のランタイム カウンタをリセットする例を示します。

```
> clear flow-export counters
```

関連コマンド

Command	説明
show flow-export counters	NetFlow のすべてのランタイム カウンタを表示します。

clear flow-offload

オフロードされたフローのカウンタと統計情報をクリアするには、**clear flow-offload** コマンドを使用します。

このコマンドは Firepower 4100/9300 シャーシ の 脅威に対する防御で使用できます。

clear flow-offload statistics

構文の説明

statistics	すべてのオフロードされたフローの統計情報をゼロにリセットします。

コマンド履歴

リリース	変更内容
6.3	このコマンドが導入されました。

例

次に、すべてのフローカウンタをクリアする例を示します。

```
> clear flow-offload statistics
```

関連コマンド

コマンド	説明
show flow-offload	ダイナミック フロー オフロード カウンタ、統計情報、および情報を表示します。
configure flow-offload	ダイナミック フロー オフロードを有効または無効にします。

clear flow-offload-ipsec

IPsec フローオフロードに関する情報をクリアするには、**clear flow-offload-ipsec** コマンドを使用します。

clear flow-offload-ipsec statistics

構文の説明

statistics	IPsec フローオフロード関連の統計をクリアします。

コマンド履歴

リリース	変更内容
7.2	このコマンドが導入されました。

例

次に、すべての IPsec フローオフロード統計をクリアする例を示します。

```
> clear flow-offload-ipsec statistics
```

関連コマンド

Command	説明
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。

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するには、**clear fragment** コマンドを入力します。

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

構文の説明

queue	IP フラグメント再構築キューをクリアします。
statistics *interface_name*	IP フラグメント再構築統計情報をクリアします。必要に応じて、そのインターフェイスの統計情報のみをクリアするインターフェイス名を指定できます。指定しない場合、すべてのインターフェイスの統計情報がクリアされます。

コマンド履歴

リリース	変更内容
6.1	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、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。

例

次に、IP フラグメント再構成モジュールの運用データをクリアする例を示します。

```
> clear fragment queue
```

関連コマンド

Command	説明
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

ガベージコレクション（GC）プロセスの統計情報を表示するには、**clear gc** コマンドを使用します。

clear gc

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、GC プロセスの統計情報を削除する例を示します。

```
> clear gc
```

関連コマンド

Command	説明
show gc	GC のプロセスの統計情報を表示します。

clear igmp

すべてのIGMPカウンタ、グループキャッシュ、およびトラフィックをクリアするには、**clear igmp** コマンドを使用します。

clear igmp {**counters** [*if_name*] | **group** [**interface** *name*] | **traffic**}

構文の説明

counters [*if_name*]	IGMP統計カウンタをクリアします。必要に応じて、インターフェイス名を指定して、該当インターフェイスのカウンタだけをクリアできます。
group [**interface** *name*]	IGMPグループキャッシュエントリを削除します。必要に応じて、インターフェイス名を指定して、該当インターフェイスにのみ関連付けられているグループを削除できます。 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。
traffic	トラフィックカウンタをクリアします。

コマンド履歴

リリース	変更内容
6.1	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。

```
> clear igmp counters
```

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。

```
> clear igmp group
```

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。

```
> clear igmp traffic
```

関連コマンド

Command	説明
show igmp	IGMP 情報を表示します。

clear ikev1

IPsec IKEv2 SA または統計情報を削除するには、**clear ikev1** コマンドを使用します。

clear ikev1 {**sa** [*ip_address*] | **stats**}

構文の説明

sa *ip_address*	SA をクリアします。すべての IKEv1 SA をクリアするには、IP アドレスを指定せずにこのオプションを使用します。それ以外の場合は、クリアする SA の IPv4 アドレスまたは IPv6 アドレスを指定します。
stats	IKEv1 統計情報をクリアします。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、脅威に対する防御 デバイスからすべての IPsec IKEv1 の統計を削除する例を示します。

```
> clear ikev1 stats
>
```

次に、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。

```
> clear ikev1 sa 10.86.1.1
>
```

関連コマンド

Command	説明
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 ikev2

IPsec IKEv2 SA または統計情報を削除するには、**clear ikev2** コマンドを使用します。

clear ikev2 {**sa** [*ip_address*] | **stats**}

構文の説明

sa *ip_address*	SA をクリアします。すべての IKEv2 SA をクリアするには、IP アドレスを指定せずにこのオプションを使用します。それ以外の場合は、クリアする SA の IPv4 アドレスまたは IPv6 アドレスを指定します。
stats	IKEv2 統計情報をクリアします。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、脅威に対する防御 デバイスからすべての IPsec IKEv2 の統計を削除する例を示します。

```
> clear ikev2 stats
>
```

次に、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。

```
> clear ikev2 sa 10.86.1.1
>
```

関連コマンド

Command	説明
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 interface

IP インターフェイスの統計情報を消去するには、**clear interface** コマンドを使用します。

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

構文の説明

interface_name	（任意）インターフェイス名を指定します。
physical_interface	（任意）**gigabit**ethernet0/1 などのインターフェイス ID を指定します。
サブインターフェイス	（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。

コマンド 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。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

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。

```
> clear interface
```

関連コマンド

Command	説明
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

特定のレガシー機能の統計情報をクリアするには、**clear ip** コマンドを使用します。

clear ip ｛**audit count** ［**global**］ | **verify statistics**｝［**interface** *interface_name*］

構文の説明

audit count［**global**］	監査ポリシーのシグニチャ一致カウントをクリアします。**interface** キーワードを指定しない場合、すべての署名のカウントがグローバルにクリアされます。必要に応じて、このことを明示的に指定する **global** キーワードを含めることができます（global と interface の両方は指定できません）。
interface *interface_name*	（任意）指定されたインターフェイスの統計情報のみクリアします。
verify statistics	ユニキャスト リバース パス フォワーディング（RPF）でドロップされたパケットの数をクリアします。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

通常、これらの機能は有効になっていないため、クリアする統計情報はありません。

例

次に、すべてのインターフェイスの IP 監査数をクリアする例を示します。

```
> clear ip audit count
```

関連コマンド

Command	説明
show ip audit count	ユニキャスト RPF 統計情報を表示します。
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 audit name	**ip audit name** コマンドの設定を表示します。**name** に加えて、**interface** と **signature** の設定を確認できます。
show running-config ip verify reverse-path	**ip verify reverse-path** の設定を表示します。

clear 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、**clear ipsec sa** コマンドを使用します。

clear ipsec sa ［**counters** | **entry** *ip_address* {**esp** | **ah**} *spi* | **inactive** | **map** *map_name* | **peer** *ip_address*］

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 *ip_address*	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。
inactive	すべての非アクティブな IPsec SA をクリアします。
map *map_name*	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。
peer *ip_address*	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。受信 SPI である必要があります。このコマンドは、送信 SPI ではサポートされていません。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

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。

例

次に、グローバル コンフィギュレーション モードで、脅威に対する防御 からすべての IPsec SA を削除する例を示します。

```
> clear ipsec sa
>
```

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。

```
> clear ipsec sa peer 10.86.1.1
```

関連コマンド

Command	説明
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 ipv6 dhcp

DHCPv6 の統計情報をクリアするには、**clear ipv6 dhcp** コマンドを使用します。

clear ipv6 dhcp {**client** [**pd**] | **interface** *interface_name* | **server**} **statistics**

構文の説明

client [**pd**]	DHCPv6 クライアントの統計情報をクリアします。プレフィックス委任クライアントの統計情報をクリアするには、**pd** キーワードを追加します。
interface *interface_name*	指定したインターフェイスの DHCPv6 統計情報をクリアします。
server	DHCPv6 サーバーの統計情報をクリアします。

コマンド履歴

リリース	変更内容
6.2.1	このコマンドが導入されました。

例

次に、DHCPv6 クライアントの統計情報をクリアする例を示します。

```
> clear ipv6 dhcp client statistics
```

関連コマンド

Command	説明
show ipv6 dhcp	DHCPv6 の統計情報を表示します。

clear ipv6 dhcprelay

IPv6 DHCP リレー バインディング エントリおよび統計情報をクリアするには、**clear ipv6 dhcprelay** コマンドを使用します。

clear ipv6 dhcprelay {**binding** [*ip_address*] | **statistics**}

構文の説明

binding	IPv6 DHCP リレー バインディング エントリをクリアします。
ip_address	（オプション）DHCP リレー バインディングの IPv6 アドレスを指定します。IP アドレスを指定した場合、その IP アドレスに関連付けられたリレー バインディング エントリだけがクリアされます。
statistics	IPv6 DHCP リレー エージェントの統計情報をクリアします。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、IPv6 DHCP リレー バインディングの統計情報データをクリアする例を示します。

```
> clear ipv6 dhcprelay binding
>
```

次に、IPv6 DHCP リレー エージェントの統計情報データをクリアする例を示します。

```
> clear ipv6 dhcprelay statistics
```

関連コマンド

Command	説明
show ipv6 dhcprelay binding	リレー エージェントによって作成されたリレー バインディング エントリを表示します。
show ipv6 dhcprelay statistics	IPv6 DHCP リレー エージェントの情報を表示します。

clear ipv6 mld traffic

IPv6 マルチキャストリスナー検出（MLD）トラフィックカウンタをクリアして、リセットするには、**clear ipv6 mld traffic** コマンドを使用します。

clear ipv6 mld traffic

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、IPv6 MLD のトラフィック カウンタをクリアする例を示します。

```
> clear ipv6 mld traffic
>
```

関連コマンド

Command	説明
show ipv6 mld traffic	IPv6 MLD トラフィックカウンタを表示します。

clear ipv6 neighbors

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

clear ipv6 neighbors

コマンド履歴

リリース	変更内容
6.1	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。

```
> clear ipv6 neighbors
>
```

関連コマンド

Command	説明
show ipv6 neighbor	IPv6 ネイバー キャッシュ情報を表示します。

clear ipv6 ospf

OSPFv3 ルーティングパラメータをクリアするには、**clear ipv6 ospf** コマンドを使用します。

clear ipv6 ［*process_id*］［**counters**］［**events**］［**force-spf**］［**process**］［**redistribution**］［**traffic**］

構文の説明

counters	OSPF プロセス カウンタをリセットします。
events	OSPF イベント ログをクリアします。
force-ospf	OSPF プロセスの SPF をクリアします。
process	OSPFv3 プロセスをリセットします。
process_id	プロセス ID の番号をクリアします。有効値の範囲は 1 ～ 65535 です。
redistribution	OSPFv3 ルート再配布をクリアします。
traffic	トラフィック関連の統計情報をクリアします。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、すべての OSPFv3 ルート再配布をクリアする例を示します。

```
> clear ipv6 ospf redistribution
>
```

関連コマンド

Command	説明
show running-config ipv6 router	OSPFv3 プロセスの実行コンフィギュレーションを表示します。

clear ipv6 prefix-list

ルーティング IPv6 プレフィックスリストをクリアするには、**clear ipv6 prefix-list** コマンドを使用します。

clear ipv6 prefix-list ［*name*］

構文の説明

name	名前付き IPv6 プレフィックスリストをクリアします。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、list1 IPv6 プレフィックス リストをクリアする例を示します。

```
> clear ipv6 prefix-list list1
>
```

関連コマンド

Command	説明
show running-config ipv6 prefix-list	IPv6 プレフィックス リストの実行コンフィギュレーションを表示します。

clear ipv6 route

IPv6 ルーティング テーブルからルートを削除するには、clear ipv6 route コマンドを使用します。

clear ipv6 route ［**management-only**］｛**all** ｜ *ipv6-prefix/prefix-length*｝

構文の説明

management-only	IPv6 管理ルーティング テーブルのみをクリアします。
ipv6-prefix/prefix-length	IPv6 プレフィックス用のルーテッドをクリアします。
all	すべての IPv6 ルートをクリアします。

コマンド履歴

リリース	変更内容
6.1	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 ipv6 route コマンドは、IPv6 固有である点を除いて、**clear ip route** コマンドに似ています。

宛先ごとの最大伝送ユニット（MTU）キャッシュもクリアされます。

例

次に、2001:0DB8::/35 用の IPv6 ルートを削除する例を示します。

```
> clear ipv6 route 2001:0DB8::/35
```

関連コマンド

Command	説明
show ipv6 route	IPv6 ルートを表示します。

clear ipv6 traffic

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

clear ipv6 traffic

コマンド履歴

リリース	変更内容
6.1	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をリセットします。

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。

```
> clear ipv6 traffic
>
```

関連コマンド

Command	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

ISAKMP SA または統計情報をクリアするには、**clear isakmp** コマンドを使用します。

clear isakmp ［**sa** | **stats**］

構文の説明

sa	（任意）IKEv1 SA および IKEv2 SA をクリアします。
stats	（任意）IKEv1 および IKEv2 統計情報をクリアします。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

すべての ISAKMP 運用データをクリアするには、このコマンドを引数なしで使用します。

例

次に、すべての ISAKMP SA を削除する例を示します。

```
> clear isakmp sa
>
```

関連コマンド

Command	説明
show isakmp	ISAKMP 運用データ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 isis

IS-IS データ構造をクリアするには、**clear isis** コマンドを使用します。

clear isis {***** | **lspfull** | **rib redistribution** [**level-1** | **level-2**] [*network_prefix*] [*network_mask*]}

構文の説明

*****	すべての IS-IS データ構造をクリアします。
level-1	（任意）再配布キャッシュから、レベル 1 IS-IS 再配布プレフィックスをクリアします。
level-2	（任意）再配布キャッシュから、レベル 2 IS-IS 再配布プレフィックスをクリアします。
lspfull	IS-IS LSPFULL 状態をクリアします。
network_mask	（任意）RIB からクリアするネットワーク プレフィックスのネットワーク マスクのネットワーク ID を A.B.C.D 形式で表したもの。プレフィックスに対するネットワーク マスクを指定しなかった場合、ネットワーク マスクには、プレフィックスのメジャー ネットが使用されます。
network_prefix	（任意）再配布ルーティング情報ベース（RIB）からクリアするネットワーク プレフィックスのネットワーク ID を A.B.C.D 形式で表したもの。プレフィックスに対するネットワーク マスクを指定しなかった場合、ネットワーク マスクには、プレフィックスのメジャー ネットが使用されます。
rib redistribution	IS-IS 再配布キャッシュ内のプレフィックスをクリアします。

コマンド履歴

リリース	変更内容
6.3	このコマンドが導入されました。

使用上のガイドライン

再配布されたルートが多すぎて、リンクステート PDU（LSP）がいっぱいになってしまった場合は、問題の解決後、**clear isis lspfull** コマンドを使用して、この状態をクリアします。

clear isis rib コマンドは、Cisco Technical Assistance Center の担当者がソフトウェアエラーの後で実行を依頼したときに、トラブルシューティングのためにだけ使用することをお勧めします。

例

次に、LSPFULL 状態をクリアする例を示します。

```
> clear isis lspfull
```

次に、IP ローカル再配布キャッシュからネットワーク プレフィックス 10.1.0.0 をクリアする例を示します。

```
> clear isis rib redistribution 10.1.0.0 255.255.0.0
```

関連コマンド

Command	説明
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。

clear kernel cgroup-controller

カーネルの cgroup コントローラの統計情報をクリアするには、**clear kernel cgroup-controller** コマンドを使用します。

clear kernel cgroup-controller ［**cpu** | **memory**］

構文の説明

cpu	（任意）cpu/cpuacct コントローラの統計情報をクリアします。
memory	（任意）メモリコントローラの統計情報をクリアします。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、cgroup コントローラの統計情報をクリアする例を示します。

```
> clear kernel cgroup-controller
```

関連コマンド

Command	説明
show kernel cgroup-controller	cgroup コントローラの統計情報を表示します。

clear lacp

EtherChannel LACP ポートチャネルの統計情報をクリアするには、**clear lacp** コマンドを使用します。

clear lacp ［*channel_group_number*］

構文の説明

channel_group_number	（オプション）1 ー 48 の番号ごとに、チャネルグループ情報をクリアします。

コマンド デフォルト

チャネル番号を指定しないと、すべてのポートチャネルの統計情報がクリアされます。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、ポートチャネル統計情報をクリアする例を示します。

```
> clear lacp 12
```

関連コマンド

Command	説明
show lacp	ポート チャネルの情報を表示します。

clear lisp eid

LISP EID テーブルをクリアするには、**clear list eid** コマンドを使用します。

clear lisp eid ［*ip_address* ］

構文の説明

ip_address	指定した IP アドレスを EID テーブルから削除します。

コマンド履歴

リリース	変更内容
6.2	このコマンドが導入されました。

使用上のガイドライン

デバイスは、EID とサイト ID を関連付ける EID テーブルを保持します。**clear lisp eid** コマンドは、テーブルの EID エントリをクリアします。

関連コマンド

Command	説明
clear cluster info flow-mobility counters	フロー モビリティ カウンタをクリアします。
show cluster info flow-mobility counters	フロー モビリティ カウンタを表示します。
show conn	LISP フロー モビリティの対象となるトラフィックを表示します。
show lisp eid	EID テーブルを表示します。

clear local-host （廃止）

接続制限や初期接続制限など、クライアントごとのランタイム状態を再初期化するには、**clear local-host** コマンドを使用します。

clear local-host ［*hostname* | *ip_address*］［**all**］［**zone**］

構文の説明

all	（任意）to-the-box トラフィックを含む、すべての接続をクリアします。**all** キーワードを指定しない場合は、through-the-box トラフィックだけがクリアされます。
hostname または *ip_address*	（任意）ローカルホスト名か、IPv4 または IPv6 アドレスを指定します。
zone	（任意）トラフィックゾーンのすべての接続をクリアします。

コマンド デフォルト

すべての through-the-box 実行時状態をクリアします。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。
7.0	このコマンドは廃止されました。ローカルアドレスへの接続をクリアするには、**clear conn address** コマンドを使用します。

使用上のガイドライン

コンフィギュレーションに対してセキュリティポリシーの変更を加えた場合は、すべての新しい接続で新しいセキュリティポリシーが使用されます。既存の接続では、その接続が確立された時点で設定されていたポリシーの使用が続行されます。すべての接続で新しいポリシーが確実に使用されるようにするには、**clear local-host** コマンドを使用して、現在の接続を切断し、新しいポリシーを使用して再接続できるようにする必要があります。または、さらにきめ細かく接続をクリアするための **clear conn** コマンドや、ダイナミック NAT を使用する接続用の **clear xlate** コマンドを使用できます。

clear local-host コマンドは、ホストライセンス制限からホストを解放します。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確認できます。

例

次に、10.1.1.15 のホストのランタイム状態および関連する接続をクリアする例を示します。

```
> clear local-host 10.1.1.15
```

関連コマンド

Command	説明
clear conn	あらゆる状態の接続を切断します。
clear xlate	ダイナミック NAT セッションおよび NAT を使用しているすべての接続をクリアします。
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。

clear logging

ロギングバッファをクリアするには、**clear logging** コマンドを使用します。

clear logging {**buffer** | **counter** *option* | **queue bufferwrap** | **unified-client**}

構文の説明

buffer	内部ロギングバッファをクリアします。
counter *[接続先（Destination）]*	指定されたロギングの宛先に対するカウンタと統計情報をクリアします。すべてのロギングの宛先に関する統計情報をクリアするには、**all** を指定します。または、次のいずれかの宛先を指定して、アクションをその 1 つの宛先に制限できます。**buffer**、**console**、**mail**、**monitor**、**trap**。
queue bufferwrap	保存されている FTP およびフラッシュ ロギング バッファ キューをクリアします。
unified-client	統合ロギングクライアント、loggerD からロギング統計情報をクリアします。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。
6.3	**unified-client** キーワードが追加されました。
6.6	**counter** キーワードが追加されました。

例

次の例では、ログ バッファの内容をクリアする方法を示します。

```
> clear logging buffer
```

次に、保存されているログ バッファの内容をクリアする例を示します。

```
> clear logging queue bufferwrap
```

次に、loggerD サービスの統計情報をクリアする例を示します。

```
> clear logging unified-client
```

関連コマンド

Command	説明
logging savelog	任意のフラッシュファイル名を指定します。

Command	説明
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、**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。

コマンド履歴

リリース	変更内容
6.1	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。

```
> clear mac-address-table
```

関連コマンド

Command	説明
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

メモリツールのキューと統計情報をクリアするには、**clear memory** コマンドを使用します。

clear memory {**delayed-free-poisoner** | **profile** [**peak**] | **tracking**}

構文の説明

delayed-free-poisoner	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せずにシステムに戻し、関連する統計情報カウンタをクリアします。この機能を有効にするには、**memory delayed-free-poisoner enable** コマンドを使用します。
profile [**peak**]	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 バッファをクリアします。ピークメモリバッファの内容をクリアするには、任意の **peak** キーワードを含めます。 プロファイルバッファをクリアする前に、メモリプロファイリングを停止するには、**no memory profile enable** コマンドを使用します。
tracking	**memory tracking enable** コマンドによって収集されたメモリトラッキング情報をクリアします。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

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。

```
> clear memory delayed-free-poisoner
```

関連コマンド

Command	説明
memory	さまざまなメモリツールを有効にします。
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。
show memory profile	メモリプロファイリングの結果を表示します。
show memory tracking	メモリトラッキングの結果を表示します。

clear mfib counters

マルチキャスト転送情報ベース（MFIB）ルートパケットカウンタをクリアするには、**clear mfib counters** コマンドを使用します。

clear mfib {**cluster-stats** | **counters** [*source_or_group* [*source*]]}

構文の説明

cluster-stats	MFIB クラスタ同期統計情報をクリアします。
count	MFIB ルートおよびパケットカウントデータをクリアします。**count** 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。
source_or_group [*group*]	（任意）送信元またはグループの IPv4、IPv6、または名前。両方を指定する場合は、最初に送信元を指定します。送信元アドレスはユニキャストアドレスです。

コマンド履歴

リリース	変更内容
6.1	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。

```
> clear mfib counters
```

関連コマンド

Command	説明
show mfib	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 nat counters

NAT ポリシーカウンタをクリアするには、clear nat counters コマンドを使用します。

clear nat counters ［**interface** *name*］［*ip_addr mask* | ｛**object** | **object-group**｝ *name*］［**translated** ［**interface** *name*］［*ip_addr mask* | ｛**object** | **object-group**｝ *name*］］］

構文の説明

interface *name*	（任意）送信元または宛先（変換済み）インターフェイスを指定します。
ip_addr mask	（オプション）IP アドレスおよびサブネット マスクを指定します。
object *name*	（任意）ネットワーク オブジェクトまたはサービス オブジェクトを指定します。
object-group *name*	（任意）ネットワーク オブジェクト グループを指定します。
translated	（オプション）変換されたパラメータを指定します。

コマンド履歴

リリース	変更内容
6.1	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。

```
> clear nat counters
```

関連コマンド

Command	説明
show nat	プロトコル スタック カウンタを表示します。

clear object

ネットワークサービス オブジェクトのヒットカウントをクリアするには、**clear object** コマンドを使用します。

clear object ［ **id** *object_name* | **network-service** ］

構文の説明

id *name*	（オプション）指定したネットワークサービス オブジェクトのカウンタをクリアします。大文字と小文字が区別されます。たとえば、「object-name」は「Object-Name」と一致しません。
network-service	（オプション）すべてのネットワークサービス オブジェクトのカウンタをクリアします。このアクションは、コマンドでパラメータを指定しない場合と同じです。

コマンド デフォルト

パラメータを指定しない場合、すべてのオブジェクトのヒットカウントがクリアされます。

コマンド履歴

リリース	変更内容
7.1	このコマンドが導入されました。

例

次に、すべてのオブジェクトのヒットカウントをクリアする例を示します。

```
> clear object
```

関連コマンド

Command	説明
show object	ネットワークサービス オブジェクトとそのヒットカウントを表示します。

clear object-group

ネットワーク オブジェクト グループまたはネットワークサービスオブジェクト グループにあるオブジェクトのヒットカウントをクリアするには、**show object-group** コマンドを使用します。

clear object-group ［ *object_group_name* ］

構文の説明

object_group_name	カウンタをクリアするオブジェクトグループの名前。名前を指定しない場合、すべてのオブジェクトグループのカウンタがクリアされます。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。
7.1	ネットワークサービス オブジェクトで動作するようにコマンドが拡張されました。

例

次に、「Anet」というオブジェクトグループのヒットカウントをクリアする例を示します。

```
> clear object-group Anet
```

関連コマンド

Command	説明
show object-group	オブジェクトグループの情報を表示します。

clear ospf

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

clear ospf ［**vrf** *name* | **all**］ {**counters** ［**neighbor** *interface*］ | **events** | **force-spf** | **process /noconfirm** | **redistribution** | **traffic**}

構文の説明

counters	OSPF カウンタをクリアします。
neighbor *interface*	（任意）ネイバーの統計情報のみクリアします。
events	OSPF イベント ログをクリアします。
force-spf	増分 SPF 統計情報をクリアします。
process /noconfirm	OSPF ルーティング プロセスを再起動します。
redistribution	OSPF 経路再配布統計情報を消去します。
traffic	OSPF トラフィック関連の統計情報をクリアします。
［**vrf** *name*	**all**］	Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。
6.6	［**vrf** *name*	**all**］ キーワードが追加されました。

使用上のガイドライン

このコマンドは、設定のいずれの部分も削除せず、統計情報のみクリアします。

例

次に、すべての OSPF ネイバーカウンタをクリアする例を示します。

```
> clear ospf counters
```

関連コマンド

Command	説明
show ospf	実行コンフィギュレーションのすべての OSPF 情報を表示します。

clear packet-debugs

デバッグログをデータベースから削除するには、**clear packet-debugs** コマンドを使用します。

clear packet-debugs

コマンド履歴

リリース	変更内容
6.4	このコマンドが導入されました。
6.5	このコマンドは、**clear packet debugs** から **clear packet-debugs** に変更されました。

使用上のガイドライン

データベースからすべてのデバッグログを削除するには、**clear packet-debugs** コマンドを使用します。

例

次に、デバッグログデータベースに保存されているすべてのデバッグログを削除する例を示します。

```
> clear packet-debugs
```

関連コマンド

Command	説明
debug packet-start	データベースへのデバッグログの書き込みを開始します。

clear packet-tracer

永続的なパケットトレーサを削除するには、**clear packet-tracer** コマンドを使用します。

clear packet-tracer

コマンド履歴

リリース	変更内容
6.3	このコマンドが導入されました。

使用上のガイドライン

永続的なパケットトレーサは、**packet-tracer** コマンドで **persist** キーワードを使用して設定します。

例

次に、すべての永続的なパケットトレーサを削除する例を示します。

```
> clear packet-tracer
>
```

関連コマンド

Command	説明
packet-tracer	パケットトレーサを設定します。

clear path-monitoring

インターフェイスのパスモニタリング設定をクリアするには、**clear path-monitoring** コマンドを使用します。

clear path-monitoring ［ **interface** *name* ］

構文の説明

Interface *name*	指定されたインターフェイスで設定されたパスモニタリング設定を削除します。

コマンド履歴

リリース	変更内容
7.2	このコマンドが導入されました。

例

次に、outside1 インターフェイスのパスモニタリング設定をクリアする例を示します。

```
> clear path-montoring outside1
```

関連コマンド

Command	説明
show path-monitoring	パスモニタリングメトリック情報を表示します。

clear pclu

PC の統計情報をクリアするには、**clear pclu** コマンドを使用します。

clear pclu

コマンド履歴

リリース	変更内容
6.1	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。

```
> clear pclu
```

関連コマンド

Command	説明
show pclu	PCLU 情報を表示します。

clear pim

PIM トラフィックのカウンタとマッピングをクリアするには、**clear pim** コマンドを使用します。

clear pim {**counters** | **group-map** [*rp-address*] | **reset** | **topology** [*group*]}

構文の説明

counters	PIM トラフィック カウンタをクリアします。
group-map [*rp-address*]	グループからランデブーポイント（RP）へのマッピングエントリを RPマッピングキャッシュから削除します。必要に応じて、ランデブーポイントの名前を指定して、その RP のエントリのみをクリアすることもできます。次のいずれかの名前を使用できます。 • ドメインネームシステム（DNS）ホストテーブルで定義されている RP の名前。 • RP の IP アドレス。これは、4 分割ドット付き 10 進表記のマルチキャスト IP アドレスです。
reset	リセット時の MRIB 同期を必須にします。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。このオプションを使用して、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こともできます。
topology [*group*]	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。必要に応じて、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できます。次のいずれかの名前を使用できます。 • DNS ホストテーブルで定義されているマルチキャストグループの名前。 • マルチキャストグループの IPv4 または IPV6 アドレス。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

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。

```
> clear pim counters
```

次に、RP アドレス 23.23.23.2 のグループから RP へのマッピングのエントリを削除する例を示します。

```
> show pim group-map

Group Range          Proto Client Groups RP address      Info
224.0.1.39/32*       DM    static 0      0.0.0.0
224.0.1.40/32*       DM    static 0      0.0.0.0
224.0.0.0/24*        L-Localstatic 1      0.0.0.0
232.0.0.0/8*         SSM   config 0      0.0.0.0
224.0.0.0/4*         SM    config 0      9.9.9.9         RPF: ,0.0.0.0
224.0.0.0/4          SM    BSR    0      23.23.23.2      RPF: Gi0/3,23.23.23.2
> clear pim group-map 23.23.23.2
> show pim group-map
Group Range          Proto Client Groups RP address      Info
224.0.1.39/32*       DM    static 0      0.0.0.0
224.0.1.40/32*       DM    static 0      0.0.0.0
224.0.0.0/24*        L-Localstatic 1      0.0.0.0
232.0.0.0/8*         SSM   config 0      0.0.0.0
224.0.0.0/4*         SM    config 0      9.9.9.9         RPF: ,0.0.0.0
224.0.0.0/4          SM    static 0      0.0.0.0         RPF: ,0.0.0.0
```

関連コマンド

Command	説明
show pim	PIM トラフィックの情報を表示します。

clear prefix-list

プレフィックスリストのエントリのヒットカウントをリセットするには、**clear prefix-list** コマンドを使用します。

clear prefix-list ［*prefix_list_name*］

構文の説明

prefix_list_name	（任意）ヒットカウントをクリアするプレフィックスリストの名前。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、first_list という名前のリストからプレフィックスリスト情報をクリアする例を示します。

```
> clear prefix-list first_list
>
```

関連コマンド

Command	説明
show prefix-list	プレフィックス リストまたはプレフィックス リスト エントリに関する情報を表示します。

clear priority-queue statistics

特定のインターフェイス、またはすべての設定済みインターフェイスに関する priority-queue statistics のカウンタをクリアするには、**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）指定されたインターフェイスの priority-queue statistics をクリアします。

コマンド履歴

リリース	変更内容
6.3	このコマンドが導入されました。

例

次に、すべてのインターフェイスの priority-queue statistics をクリアする例を示します。

```
> clear priority-queue statistics
```

関連コマンド

Command	説明
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。

clear process

脅威に対する防御 デバイスで実行されている特定のプロセスの統計をクリアするには、clear process コマンドを使用します。

clear process {**cpu-hog** | **internals**}

構文の説明

cpu-hog	高 CPU 負荷統計情報をクリアします。
internals	プロセス内部統計情報をクリアします。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、高 CPU 負荷統計情報をクリアする例を示します。

```
> clear process cpu-hog
```

関連コマンド

Command	説明
cpu hog granular-detection	リアルタイム高 CPU 負荷検出情報をトリガーします。
show processes	脅威に対する防御 で動作しているプロセスのリストを表示します。

clear resource usage

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

clear resource usage ［**detail** ｜ **resource** ｛［**rate**］ *resource_name* ｜ **all**｝］

構文の説明

detail	すべてのリソース使用状況の詳細をクリアします。
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。rate で測定されるリソースには、**conns**、**inspects**、および **syslogs** があります。これらのリソースの種類を指定する場合は、**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。 • **Conns**：任意の 2 つのホスト間の TCP または UDP 接続（1 つのホストと他の複数ホストとの間の接続を含む）。 • **Hosts**：デバイスを介して接続できるホスト。 • **IPSec**：デバイスを介して接続する IPSec 管理トンネル。 • **Mac-addresses**：MAC アドレステーブルで許可される MAC アドレス数。 • **Routes**：ルーティング テーブル エントリ。 • **SSH**：SSH セッション。 • **Storage**：ストレージサイズ制限（MB 単位）。 • **Telnet**：Telnet セッション。 • **VPN**：VPN リソース。 • **Xlates**：NAT 変換。

コマンド デフォルト

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

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

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。

```
> clear resource usage resource all
```

関連コマンド

Command	説明
show resource types	リソース タイプのリストを表示します。
show resource usage	デバイ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ルーティングテーブルから削除するには、**clear route** コマンドを使用します。

clear route ［ **vrf** *name* | **all** ］ ［ **management-only** ］ ［ **all** | *ip_address* ［ *ip_mask_or_prefix* ］］

構文の説明

all	学習したすべてのルートを削除するように指定します。
ip_address mask_or_prefix	削除するルートの IPv4 または IPv6 宛先アドレスとマスクまたはプレフィックス。ルートを指定しない場合、動的に学習されたすべてのルートが削除されます。
management-only	（オプション）管理ルーティングテーブルをクリアします。宛先アドレスを指定して、特定の管理ルートをクリアできます。
［**vrf** *name*	**all**］	Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。
6.6	［**vrf** *name*	**all**］ キーワードが追加されました。
7.1	バージョン 7.1 以降では、ユニットがハイアベイラビリティ グループまたはクラスタの一部である場合、このコマンドはアクティブユニットまたは制御ユニットにのみ使用できます。HA グループまたはクラスタのすべてのユニットのルートがクリアされます。以前のリリースでは、コマンドを実行したユニットのルートのみがクリアされます。

例

次に、すべての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。

```
> clear route
```

関連コマンド

Command	説明
show route	ルート情報を表示します。

clear rule hits

アクセスコントロールポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報をクリアし、ゼロにリセットするには、**clear rule hits** コマンドを使用します。

clear rule hits ［*id*］

構文の説明

id	（オプション）ルールの ID。この引数を含めると、指定したルールのルールヒット情報のみがクリアされます。 ルール ID を識別するには、**show access-list** コマンドを使用します。

コマンド デフォルト

ルールIDを指定しない場合、すべてのルールのルールヒット情報がクリアされ、ゼロにリセットされます。

（注） このアクションは元に戻せないため、このコマンドの使用には注意が必要です。

コマンド履歴

リリース	変更内容
6.4	このコマンドが導入されました。

使用上のガイドライン

ルールヒット情報は、アクセスコントロールルールとプレフィルタルールのみを対象としています。

例

すべてのルールヒット情報をクリアする例を次に示します。

```
> clear rule hits
```

関連コマンド

Command	説明
show rule hits	アクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報を表示します。
show cluster rule hits	クラスタ内のすべてのノードから、アクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報をクリアし、ゼロにリセットします。
cluster exec show rule hits	クラスタの各ノードから、アクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報を分離形式で表示します。

Command	説明
cluster exec clear rule hits	クラスタ内のすべてのノードから、アクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報をクリアし、ゼロにリセットします。

clear service-policy

有効になっているポリシーの動作データまたは統計情報をクリアするには、**clear service-policy** コマンドを使用します。

clear service-policy ［**global** | **interface** *intf* | **shape** | **user-statistics**］

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。
shape	（任意）シェイプポリシーの統計情報をクリアします。
user-statistics	（オプション）ユーザー統計情報のグローバル カウンタはクリアしますが、ユーザーごとの統計情報はクリアしません。この機能は 脅威に対する防御 ではサポートされていません。

コマンド 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。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

一部のインスペクションエンジンでは、統計情報を選択してクリアできます。**clear service-policy inspect** コマンドを参照してください。

例

次に、外部インターフェイスのサービス ポリシー統計情報をクリアする方法の例を示します。

```
> clear service-policy interface outside
```

関連コマンド

Command	説明
clear service-policy inspect	GTP、M3UA、およびRADIUS検査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 service-policy inspect gtp

GTP インスペクションの統計情報をクリアするには、**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** [**map** *name* | **version** *version_num*] | **statistics** [*IP_address*]}

構文の説明

pdp-context {**all** | **apn** *ap_name* | **imsi** *IMSI_value* | **ms-addr** *IP_address* | **tid** *tunnel_ID* | **version** *version_num*}	パケット データ プロトコル（PDP）またはベアラー コンテキスト情報をクリアします。次のキーワードを使用して、クリアするコンテキストを指定できます。 • **all**：すべてのコンテキストをクリアします。 • **apn** *ap_name*：指定されたアクセスポイント名のコンテキストをクリアします。 • **imsi** *IMSI_value*：指定された IMSI 16 進数のコンテキストをクリアします。 • **ms-addr** *IP_address*：指定されたモバイルサブスクライバ（MS）の IP アドレスのコンテキストをクリアします。 • **tid** *tunnel_ID*：指定された GTP トンネル ID（16 進数）のコンテキストをクリアします。 • **version** *version_num*：指定された GTP バージョン（0 ～ 255）のコンテキストをクリアします。
requests [**map** *name* | **version** *version_num*]	GTP 要求をクリアします。次のパラメータを使用して、クリアする要求を任意で制限できます。 • **map** *name*：指定された GTP インスペクション ポリシー マップに関連付けられている要求をクリアします。 • **version** *version_num*：指定された GTP バージョン（0 ～ 255）の要求をクリアします。
statistics [*IP_address*]	**inspect gtp** コマンドの GTP 統計情報をクリアします。エンドポイントのアドレスを指定すると、特定のエンドポイントの統計情報をクリアできます。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、GTP 統計情報をクリアする例を示します。

```
> clear service-policy inspect gtp statistics
```

関連コマンド

Command	説明
show service-policy inspect gtp	GTP 統計情報を表示します。

clear service-policy inspect m3ua

M3UA インスペクションの統計情報をクリアするには、**clear service-policy inspect m3ua** コマンドを使用します。

clear service-policy inspect m3ua {**drops** | **endpoint** [*ip_address*]}

構文の説明

drops	M3UA ドロップの統計情報をクリアします。
endpoint [*ip_address*]	M3UAエンドポイントの統計情報をクリアします。必要に応じて、エンドポイントの IP アドレスを指定して、そのエンドポイントの統計情報のみをクリアできます。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用して、M3UAインスペクションの統計情報をクリアします。統計情報を表示するには、このコマンドの **show** バージョンを使用します。

例

次に、M3UA エンドポイントの統計情報をクリアする例を示します。

```
> clear service-policy inspect m3ua endpoint
```

関連コマンド

コマンド	説明
show service-policy inspect m3ua	M3UA 統計情報を表示します。

clear service-policy inspect radius-accounting

RADIUS アカウンティングユーザーをクリアするには、**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	すべてのユーザーをクリアします。
ip_address	この IP アドレスのユーザーをクリアします。
policy_map	このポリシーマップに関連付けられているユーザーをクリアします。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、すべての RADIUS アカウンティング ユーザーをクリアする例を示します。

```
> clear service-policy inspect radius-accounting users all
```

clear shun

現在有効になっているすべての shun を無効にして、shun 統計情報をクリアするには、**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。

コマンド履歴

リリース	変更内容
6.1	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。

```
> clear shun
```

関連コマンド

Command	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 snmp-server statistics

SNMP サーバー統計情報（SNMP パケットの入力カウンタと出力カウンタ）をクリアするには、**clear snmp-server statistics** コマンドを使用します。

clear snmp-server statistics

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、SNMP サーバー統計情報をクリアする例を示します。

```
> clear snmp-server statistics
```

関連コマンド

Command	説明
show snmp-server statistics	SNMP サーバー コンフィギュレーション情報を表示します。

clear snort statistics

Snort 統計情報（パケットカウンタ、フローカウンタ、およびイベントカウンタ）をクリアするには、**clear snort statistics** コマンドを使用します。

clear snort statistics

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、Snort 統計情報をクリアする例を示します。

```
> clear snort statistics
```

関連コマンド

Command	説明
show snort statistics	Snort 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。

clear snort tls-offload

SSL ハードウェア アクセラレーション（接続、暗号化、暗号解読）に関連した Snort 統計情報をクリアするには、**clear snort tls-offload** コマンドを使用します。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。このコマンドは、SSL ハードウェア アクセラレーションをサポートする次の管理対象デバイスでのみ使用できます。

- Threat Defense を搭載した Firepower 2100
- を搭載した Firepower 4100/9300 Threat Defense

  Firepower 4100/9300 Threat Defense コンテナインスタンスでの TLS 暗号化アクセラレーションのサポートの詳細については、『*FXOS Configuration Guide*』を参照してください。

仮想アプライアンス上および上記以外のハードウェアでの TLS 暗号化アクセラレーション はサポートされていません。

clear snort tls-offload [proxy | tracker]

構文の説明

proxy	（オプション）プロキシの統計情報のみをクリアします。
tracker	（オプション）トラッカーの統計情報のみをクリアします。

コマンド履歴

リリース	変更内容
6.2.3	このコマンドが導入されました。

次に、プロキシの統計情報をクリアする例を示します。

```
> clear snort tls-offload proxy
```

関連コマンド

Command	説明
show snort tls-offload	すべての Snort プロセスの統計情報を表示します。
debug snort tls-offload	すべての Snort プロセスの全タイプのエラーデバッグメッセージを表示します。

clear ssl

デバッグ目的で SSL 情報をクリアするには、**clear ssl** コマンドを使用します。

clear ssl {**cache** [**all**] | **errors** | **mib** | **objects**}

構文の説明

cache [**all**]	SSL セッション キャッシュ内の期限切れセッションをクリアします。SSL セッションキャッシュ内のすべてのセッションおよび統計情報をクリアするには、任意の **all** キーワードを追加します。
errors	ssl エラーをクリアします。
mib	SSL MIB 統計情報をクリアします。
objects	SSL オブジェクト統計情報をクリアします。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

AnyConnect 機能に影響するため、DTLS キャッシュがクリアされることはありません。

例

次に、SSL キャッシュをクリアし、SSL セッション キャッシュ内のすべてのセッションおよび統計情報をクリアする例を示します。

```
> clear ssl cache
SSL session cache cleared: 2
No SSL VPNLB session cache
No SSLDEV session cache
DLTS caches are not cleared
> clear ssl cache all
Clearing all sessions and statistics
SSL session cache cleared: 5
No SSL VPNLB session cache
No SSLDEV session cache
DLTS caches are not cleared
```

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、**clear sunrpc-server active** コマンドを使用します。

clear sunrpc-server active

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

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 トラフィックがデバイ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。

```
> clear sunrpc-server active
```

関連コマンド

Command	説明
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

脅威検出レート統計情報をゼロにリセットするには、**clear threat-detection rate** コマンドを使用します。

clear threat-detection rate

コマンド履歴

リリース	変更内容
6.3	このコマンドが導入されました。

例

```
> clear threat-detection rate
>
```

関連コマンド

Command	説明
show threat-detection rate	脅威検出レート統計情報を表示します。

clear threat-detection scanning-threat

スキャン脅威検出によって識別された攻撃者およびターゲットに関する情報を削除するには、**clear threat-detection scanning-threat** コマンドを使用します。

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

構文の説明

attacker [*ip_address* [*mask*]]	（オプション）攻撃者のみをクリアします。IPアドレスとオプションのマスクを指定して、単一の攻撃者をクリアできます。
target [*ip_address* [*mask*]]	（オプション）ターゲットのみをクリアします。IP アドレスとオプションのマスクを指定して、1 つのターゲットをクリアできます。

コマンド デフォルト

すべての攻撃者とターゲットがクリアされます。

コマンド履歴

リリース	変更内容
6.3	このコマンドが導入されました。

例

次の例では、現在のスキャンの脅威を表示してからクリアします。

```
> 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
> clear threat-detection scanning-threat
```

関連コマンド

Command	説明
show threat-detection scanning-threat	スキャンする脅威の攻撃者とターゲットを表示します。

clear threat-detection shun

攻撃者を自動的に回避するようにスキャン脅威検出を設定した場合は、**clear threat-detection shun** コマンドを使用して自動回避リストからホストを削除できます。**clear shun** コマンドを使用して、手動で回避されたホストの回避を停止します。

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

構文の説明

ip_address [*mask*]	（任意）特定の IP アドレスの回避を解除します。サブネットマスクはオプションです。

コマンド デフォルト

すべての回避された攻撃者が解放されます。

コマンド履歴

リリース	変更内容
6.3	このコマンドが導入されました。

例

次に、回避リストを表示し、ホスト 10.1.1.6 を解放する例を示します。

```
> show threat-detection shun
Shunned Host List:
10.1.1.6
198.1.6.7
> clear threat-detection shun 10.1.1.6
```

関連コマンド

Command	説明
show threat-detection shun	自動的に回避されたホストを表示します。

clear threat-detection statistics

脅威検出統計情報をゼロにリセットするには、**clear threat-detection statistics** コマンドを使用します。

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。

コマンド履歴

リリース	変更内容
6.3	このコマンドが導入されました。

例

脅威検出統計情報をクリアする例を次に示します。

```
> clear threat-detection statistics
```

関連コマンド

Command	説明
show threat-detection statistics	脅威検出統計情報を表示します。

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、**clear traffic** コマンドを使用します。

clear traffic

コマンド履歴

リリース	変更内容
6.1	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 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、またはデバイスがオンラインになってから、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、デバイ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。

```
> clear traffic
```

関連コマンド

Command	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 vpn-sessiondb statistics

VPN セッションの統計情報をクリアするには、**clear vpn-sessiondb statistics** コマンドを使用します。

clear vpn-sessiondb statistics {**all** | **anyconnect** | **failover** | **global** | **index** *number* | **ipaddress** *IP_address* | **l2l** | **name** *username* | **ospfv3** | **protocol** *protocol* | **ra-ikev1-ipsec** | **ra-ikev2-ipsec** | **tunnel-group** *name* | **vpn-lb** | **webvpn**}

構文の説明

all	すべてのセッションの統計情報をクリアします。
anyconnect	AnyConnect VPN クライアント セッションの統計情報をクリアします。
failover	フェールオーバー IPsec セッションの統計情報をクリアします。
global	グローバル セッション データの統計情報をクリアします。
index *index_number*	インデックス番号を指定して単一のセッションの統計情報をクリアします。**show vpn-sessiondb detail** コマンドの出力には、セッションごとにインデックス番号が表示されます。
ipaddress *IP_address*	指定した IP アドレスのセッションの統計情報をクリアします。
l2l	VPN LAN-to-LAN セッションの統計情報をクリアします。
protocol *protocol*	特定のプロトコルの統計情報をクリアします。プロトコルのリストを表示するには、「?」と入力します。
ra-ikev1-ipsec	IPsec IKEv1 セッションの統計情報をクリアします。
ra-ikev2-ipsec	IPsec IKEv2 セッションの統計情報をクリアします。
tunnel-group *groupname*	指定したトンネル グループ（接続プロファイル）のセッションの統計情報をクリアします。
vpn-lb	VPN ロードバランシング管理セッションの統計情報をクリアします。
webvpn	クライアントレス SSL VPN セッションの統計情報をクリアします。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、すべての VPN セッションの統計情報をクリアする例を示します。

```
> clear vpn-sessiondb statistics all
INFO: Number of sessions cleared : 20
```

関連コマンド

コマンド	説明
show vpn-sessiondb	VPN セッションに関する情報を表示します。

clear wccp

Web Cache Communication Protocol（WCCP）情報をリセットするには、**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 の範囲で指定できます。

コマンド履歴

リリース	変更内容
6.1	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。

```
> clear wccp web-cache
```

関連コマンド

Command	説明
show wccp	WCCP コンフィギュレーションを表示します。

clear webvpn statistics

リモートアクセス VPN の統計情報をクリアするには、**clear webvpn statistics** コマンドを使用します。

clear webvpn statistics

コマンド履歴

リリース	変更内容
6.2.1	このコマンドが導入されました。

例

次に、リモートアクセス VPN の統計情報をクリアする例を示します。

```
> clear webvpn statistics
```

関連コマンド

コマンド	説明
show webvpn	リモートアクセス VPN に関する情報を表示します。

clear xlate

現在のダイナミック NAT 変換および接続情報をクリアするには、**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*］［**type** *type*］

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または IPv6 プレフィックスを指定します。
type *type*	（任意）タイプを指定して、アクティブな変換をクリアします。次のタイプのいずれかを入力できます。 • **dynamic**：ダイナミ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。 • **static**：スタティック変換を指定します。 • **twice-nat**：手動 NAT 変換を指定します。

コマンド履歴

リリース	変更内容
6.1	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 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。NAT ルールを追加、変更、または削除した後は、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、**show xlate detail** 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、スタティック NAT ルールを使用して作成される永続的な xlate です。**clear xlate** コマンドでは、スタティックエントリは消去されません。スタティック xlate は、スタティック NAT ルールを設定から削除することによってのみ削除できます。設定からスタティックルールを削除しても、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。これらの接続を非アクティブにするには、**clear local-host** コマンドか **clear conn** コマンドを使用します。

ダイナミック xlate は、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 および関連した接続が削除されます。**clear local-host** または **clear conn** コマンドを使用して、xlate および関連した接続を消去することもできます。設定から NAT ルールを削除した場合、ダイナミック xlate および関連した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。

```
> clear xlate global
```

関連コマンド

Command	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。
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。

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。