



# clear configuration session through clear isis コマンド

## clear configuration session

コンフィギュレーションセッションを削除するには、グローバル コンフィギュレーション モードで **clear configuration session** コマンドを使用します。

**clear configuration session** [*session\_name*]

### 構文の説明

*session\_name* 既存のコンフィギュレーションセッションの名前。現在のセッションのリストを表示するには、**show configuration session** コマンドを使用します。このパラメータを省略した場合は、既存のすべてのセッションが削除されます。

### 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。

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

### コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

### 使用上のガイドライン

このコマンドは、ACL やその他のオブジェクトを編集するために隔離されたセッションを作成する、**configure session** コマンドとともに使用します。作成したセッションが必要でなくなり、かつそのセッションで定義した変更をコミットしない場合は、このコマンドを使用してセッションおよび含まれている変更を削除します。

セッションは削除しないで、セッションで加えた変更をクリアするのみの場合は、このコマンドではなく **clear session** コマンドを使用します。

### 例

次に、old-session という名前のセッションを削除する例を示します。

```
ciscoasa(config)# clear configuration session old-session
```

### 関連コマンド

コマンド	説明
<b>clear session</b>	コンフィギュレーションセッションの内容をクリアするか、そのアクセス フラグをリセットします。
<b>configure session</b>	セッションを作成するか、開きます。
<b>show configuration session</b>	現在の各セッションで行われた変更を表示します。

# clear configure

実行コンフィギュレーションをクリアするには、グローバル コンフィギュレーション モードで **clear configure** コマンドを使用します。

```
clear configure {primary | secondary | all | command}
```

## 構文の説明

<b>all</b>	実行コンフィギュレーション全体をクリアします。
<i>command</i>	指定したコマンドのコンフィギュレーションをクリアします。使用可能なコマンドについては、 <b>clear configure ?</b> コマンドを使用して CLI ヘルプを確認してください。
<b>primary</b>	フェールオーバー ペアの場合に、プライマリ ユニットのコンフィギュレーションをクリアします。
<b>secondary</b>	フェールオーバー ペアの場合に、セカンダリ ユニットのコンフィギュレーションをクリアします。

## 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。

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

## コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

## 使用上のガイドラ イン

このコマンドをセキュリティ コンテキストで入力すると、コンテキスト コンフィギュレーションだけがクリアされます。このコマンドをシステム実行スペースで入力すると、システム実行コンフィギュレーションと、すべてのコンテキスト実行コンフィギュレーションがクリアされます。システム コンフィギュレーション内のすべてのコンテキスト エントリがクリアされるため (**context** コマンドを参照)、コンテキストは実行されなくなり、コンテキスト実行スペースに移動できなくなります。

コンフィギュレーションをクリアする前に、(スタートアップ コンフィギュレーションの場所を指定する) **boot config** コマンドへのすべての変更をスタートアップ コンフィギュレーションに必ず保存してください。スタートアップ コンフィギュレーションの場所を実行コンフィギュレーション内だけで変更した場合、再起動時にコンフィギュレーションはデフォルトの場所からロードされます。



(注)

---

**clear configure all** コマンドを入力した場合、パスワードの暗号化で 사용되는マスター パスフレーズは削除されません。マスター パスフレーズの詳細については、**config key password-encryption** コマンドを参照してください。

---

---

**例**

次に、実行コンフィギュレーション全体をクリアする例を示します。

```
ciscoasa(config)# clear configure all
```

次に、AAA コンフィギュレーションをクリアする例を示します。

```
ciscoasa(config)# clear configure aaa
```

---

**関連コマンド**

コマンド	説明
<b>show running-config</b>	実行コンフィギュレーションを表示します。

---

# 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。

```
clear conn [all] [protocol {tcp | udp | sctp}] [address src_ip[-src_ip] [netmask mask]]
[port src_port[-src_port]] [address dest_ip[-dest_ip] [netmask mask]]
[port dest_port[-dest_port] [user [domain_nickname\]user_name | user-group
[domain_nickname\]user_group_name] | zone [zone_name]] [data-rate]
```

## 構文の説明

<b>address</b>	(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。
<b>all</b>	(任意) to-the-box 接続を含む、すべての接続をクリアします。 <b>all</b> キーワードを指定しない場合は、through-the-box 接続だけがクリアされます。
<i>dest_ip</i>	(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、IP アドレスをダッシュ (-) で区切ります。次に例を示します。 10.1.1.1-10.1.1.5
<i>dest_port</i>	(任意) 宛先ポート番号を指定します。範囲を指定するには、ポート番号をダッシュ (-) で区切ります。次に例を示します。 1000-2000
<b>netmask mask</b>	(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。
<b>port</b>	(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。
<b>protocol {tcp   udp   sctp}</b>	(任意) 指定されたプロトコルを持つ接続をクリアします。
<i>src_ip</i>	(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、IP アドレスをダッシュ (-) で区切ります。次に例を示します。 10.1.1.1-10.1.1.5
<i>src_port</i>	(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、ポート番号をダッシュ (-) で区切ります。次に例を示します。 1000-2000
<b>user</b> [ <i>domain_nickname</i> \] <i>use</i> <i>r_name</i>	(オプション) 指定したユーザに所属する接続をクリアします。 <i>domain_nickname</i> 引数を含めない場合、ASA はデフォルト ドメイン内のユーザの接続をクリアします。
<b>user-group</b> [ <i>domain_nickname</i> \] <i>us</i> <i>er_group_name</i>	(オプション) 指定したユーザ グループに所属する接続をクリアします。 <i>domain_nickname</i> 引数を含めない場合、ASA はデフォルト ドメイン内のユーザ グループの接続をクリアします。
<b>zone</b> [ <i>zone_name</i> ]	トラフィック ゾーンに所属する接続をクリアします。
<b>data-rate</b>	(任意) 保存されている現在の最大データレートをクリアします。

**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。

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

#### コマンド履歴

リリース	変更内容
7.0(8)/7.2(4)/8.0(4)	このコマンドが追加されました。
8.4(2)	アイデンティティファイアウォールをサポートするための <b>user</b> および <b>user-group</b> キーワードが追加されました。
9.3(2)	<b>zone</b> キーワードが追加されました。
9.5(2)	<b>protocol sctp</b> キーワードが追加されました。
9.14(1)	<b>data-rate keyword</b> 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 IPv4 および IPv6 のアドレスをサポートします。

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 conn** 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、ホスト単位で接続をクリアするための **clear local-host** コマンドを使用したり、ダイナミック NAT を使用する接続用の **clear xlate** コマンドを使用したりできます。

ASA が、セカンダリ接続を許可するためのピンホールを作成している場合には、これが **show conn** コマンドの出力に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、10.10.10.108:4168 と 10.0.8.112:22 の間の管理接続をクリアする例を示します。

```
ciscoasa# 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
```

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

次の例では、拡張メモリに保存されている接続の最大データレートをクリアする方法について示します。

```
ciscoasa# clear conn data-rate
Released conn extension memory for 10 connection(s)
```

## 関連コマンド

コマンド	説明
<b>clear local-host</b>	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。
<b>clear xlate</b>	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。
<b>show conn</b>	接続情報を表示します。
<b>show local-host</b>	ローカル ホストのネットワーク状態を表示します。
<b>show xlate</b>	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。

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

### コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

### 例

次に、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。

```
ciscoasa# clear console-output
```

### 関連コマンド

コマンド	説明
<b>console timeout</b>	ASA 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。
<b>show console-output</b>	キャプチャされているコンソール出力を表示します。
<b>show running-config console timeout</b>	ASA 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 coredump

コアダンプ ログをクリアするには、グローバル コンフィギュレーション モードで **clear coredump** コマンドを使用します。

## clear coredump

### 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

デフォルトでは、コアダンプはイネーブルではありません。

### コマンドモード

次の表に、コマンドを入力できるモードを示します。

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



(注)

4100/9300 プラットフォームで動作している ASA の場合は、ブートストラップ CLI モードを使用してコアダンプを処理します。

### コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

### 使用上のガイドライン

このコマンドは、コアダンプ ファイル システムの内容およびコアダンプ ログを削除します。コアダンプ ファイル システムは、元の状態のままです。現在のコアダンプ コンフィギュレーションは変更されないままです。

### 例

次に、コアダンプ ファイル システムの内容およびコアダンプ ログを削除する例を示します。

```
ciscoasa(config)# clear coredump
Proceed with removing the contents of the coredump filesystem on 'disk0:' [confirm]
```

## 関連コマンド

コマンド	説明
<b>coredump enable</b>	コアダンプ機能をイネーブルにします。
<b>clear configure coredump</b>	コアダンプ ファイル システムとコアダンプ ファイル システムの内容をシステムから削除します。
<b>show coredump filesystem</b>	コアダンプ ファイル システム上のファイルを表示します。
<b>show coredump log</b>	コアダンプ ログを表示します。

# 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

<b>all</b>	(任意)すべてのフィルタ詳細をクリアします。
<b>context context-name</b>	(任意) コンテキスト名を指定します。
<b>counter_name</b>	(任意) 名前 でカウンタを指定します。どのカウンタが使用可能かを 確認するには、 <b>show counters protocol</b> コマンドを使用します。
<b>detail</b>	(任意) カウンタの詳細情報をクリアします。
<b>protocol protocol_name</b>	(任意) 指定したプロトコルのカウンタをクリアします。
<b>summary</b>	(任意) カウンタの要約をクリアします。
<b>threshold n</b>	(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。
<b>top n</b>	(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** コマンドがデフォルトです。

## 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。

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

## コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

## 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。

```
ciscoasa(config)# clear counters
```

## 関連コマンド

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

# clear cpu profile

CPU プロファイリングの統計情報をクリアするには、特権 EXEC モードで **clear cpu profile** コマンドを使用します。

## clear cpu profile

### 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。

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

### コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

### 例

次に、クラッシュ ファイルを削除する例を示します。

```
ciscoasa# clear cpu profile
```

### 関連コマンド

<b>show cpu</b>	CPU に関する情報を表示します。
<b>show cpu profile</b>	CPU プロファイリング データを表示します。

# clear crashinfo

フラッシュメモリに保存されたすべてのクラッシュ情報ファイルを削除するには、特権 EXEC モードで **clear crashinfo** コマンドを使用します。

**clear crashinfo [module {0|1}]**

構文の説明	<b>module {0 1}</b>	(任意)スロット 0 または 1 のモジュールのクラッシュ ファイルをクリアします。
-------	---------------------	--

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。

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

コマンド履歴	リリース	変更内容
	7.0(1)	このコマンドが追加されました。
	9.7(1)	フラッシュメモリに書き込まれたすべてのクラッシュ情報ファイルを削除するように出力が更新されました。

例 次に、クラッシュ ファイルを削除する例を示します。

```
ciscoasa# clear crashinfo
```

関連コマンド	説明
<b>crashinfo force</b>	ASA を強制的にクラッシュさせます。
<b>crashinfo save disable</b>	クラッシュ情報のフラッシュメモリへの書き込みをディセーブルにします。
<b>crashinfo test</b>	ASA 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。
<b>show crashinfo</b>	フラッシュメモリに格納されている最新のクラッシュ情報ファイルの内容を表示します。
<b>show crashinfo files</b>	最後の 5 つのクラッシュ情報ファイルを日付とタイムスタンプに基づいて表示します。

# 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

次の表は、このコマンドを入力できるモードを示しています。

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

### コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

### 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。

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

### 関連コマンド

コマンド	説明
<b>clear crypto protocol statistics</b>	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。
<b>show crypto accelerator statistics</b>	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。
<b>show crypto protocol statistics</b>	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たすべての CRL キャッシュをクリアするか、trustpool に関連付けられたすべての CRL をキャッシュからクリアするか、またはすべての CRL のキャッシュをクリアするには、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** [**trustpool** | **trustpoint** *trust\_point\_name*]

## 構文の説明

<b>trustpoint</b> <i>trust_point_name</i>	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。 <i>trust_point_name</i> を指定せず <b>trustpoint</b> キーワードを指定した場合、コマンドは失敗します。
<b>trustpool</b>	trustpool 内の証明書に関連付けられた CRL にのみアクションが適用されることを示します。

## デフォルト

デフォルトの動作や値はありません。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

## 例

次に、特権 EXEC コンフィギュレーション モードで、ASA からすべての trustpool CRL を削除する例、trustpoint123 に関連付けられた CLR を削除する例、およびすべての CRL を削除する例を個別に示します。

```
ciscoasa# clear crypto ca crl trustpool
ciscoasa# clear crypto ca crl trustpoint trustpoint123
ciscoasa# clear crypto ca crl
```

## 関連コマンド

コマンド	説明
<b>crypto ca crl request</b>	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。
<b>show crypto ca crl</b>	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 ca trustpool

trustpool からすべての証明書を削除するには、特権 EXEC モードで **clear crypto ca trustpool** コマンドを使用します。

## clear crypto ca trustpool [noconfirm]

### 構文の説明

**noconfirm** (任意)ユーザ確認プロンプトを抑制し、コマンドが要求どおりに処理されます。

### 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。

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

### コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

### 使用上のガイドライン

ユーザは、このアクションを実行する前に確認を求められます。

### 例

次に、すべての証明書をクリアする例を示します。

```
ciscoasa# clear crypto ca trustpool
You are about to clear the trusted certificate pool. Do you want to continue? (y/n) y
ciscoasa#
```

### 関連コマンド

コマンド	説明
<b>crypto ca trustpool export</b>	PKI trustpool を構成する証明書をエクスポートします。
<b>crypto ca trustpool import</b>	PKI trustpool を構成する証明書をインポートします。
<b>crypto ca trustpool remove</b>	指定された 1 つの証明書を trustpool から削除します。

# clear crypto ikev1

IPsec IKEv1 の SA または統計情報を削除するには、特権 EXEC モードで **clear crypto ikev1** コマンドを使用します。すべての IKEv1 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 ikev1 {sa ip_address | stats}
```

## 構文の説明

<b>sa ip_address</b>	SA をクリアします。
<b>stats</b>	IKEv1 統計情報をクリアします。

## 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。

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

## コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

## 使用上のガイドライン

すべての IPsec IKEv1 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、ASA からすべての IPsec IKEv1 統計情報を削除する例を示します。

```
ciscoasa# clear crypto ikev1 stats
ciscoasa#
```

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。

```
ciscoasa# clear crypto ikev1 sa peer 10.86.1.1
ciscoasa#
```

## 関連コマンド

コマンド	説明
<b>clear configure crypto map</b>	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。
<b>clear configure isakmp</b>	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。
<b>show ipsec sa</b>	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。
<b>show running-config crypto</b>	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 ikev2

IPsec IKEv2 の SA または統計情報を削除するには、特権 EXEC モードで **clear crypto ikev2** コマンドを使用します。すべての IKEv2 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 ikev2 {sa ip_address | stats}
```

## 構文の説明

<b>sa ip_address</b>	SA をクリアします。
<b>stats</b>	IKEv2 統計情報をクリアします。

## 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。

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

## コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

## 使用上のガイドライン

すべての IPsec IKEv2 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、ASA からすべての IPsec IKEv2 統計情報を削除する例を示します。

```
ciscoasa# clear crypto ikev2 stats
ciscoasa#
```

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。

```
ciscoasa# clear crypto ikev2 sa peer 10.86.1.1
ciscoasa#
```

## 関連コマンド

コマンド	説明
<b>clear configure crypto map</b>	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。
<b>clear configure isakmp</b>	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。
<b>show ipsec sa</b>	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。
<b>show running-config crypto</b>	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 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 ip\_address {esp | ah} spi** | **map map name** | **peer ip\_address**]

## 構文の説明

<b>ah</b>	認証ヘッダー。
<b>counters</b>	各 SA 統計情報のすべての IPsec をクリアします。
<b>entry ip_address</b>	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。
<b>esp</b>	暗号化セキュリティ プロトコル。
<b>map map name</b>	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。
<b>peer ip_address</b>	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。
<b>spi</b>	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。

## デフォルト

デフォルトの動作や値はありません。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

## 使用上のガイドライン

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、ASA からすべての IPsec SA を削除する例を示します。

```
ciscoasa# clear crypto ipsec sa
ciscoasa#
```

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。

```
ciscoasa# clear crypto ipsec peer 10.86.1.1
ciscoasa#
```

## 関連コマンド

コマンド	説明
<b>clear configure crypto map</b>	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。
<b>clear configure isakmp</b>	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。
<b>show ipsec sa</b>	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。
<b>show running-config crypto</b>	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 isakmp

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

**clear crypto isakmp [sa | stats]**

## 構文の説明

<b>sa</b>	IKEv1 および IKEv2 SA をクリアします。
<b>stats</b>	IKEv1 および IKEv2 統計情報をクリアします。

## 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。

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

## コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

## 使用上のガイドライン

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。

```
ciscoasa# clear crypto isakmp sa
ciscoasa#
```

## 関連コマンド

コマンド	説明
<b>clear configure crypto map</b>	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。
<b>clear configure isakmp</b>	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。

コマンド	説明
<b>show isakmp</b>	ISAKMP 運用データに関する情報を表示します。
<b>show running-config crypto</b>	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

<i>protocol</i>	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。 <ul style="list-style-type: none"> <li>• <b>all</b>: 現在サポートされているすべてのプロトコル。</li> <li>• <b>ikev1</b>: インターネット キー エクスチェンジ (IKE) バージョン 1</li> <li>• <b>ikev2</b>: インターネット キー エクスチェンジ (IKE) バージョン 2</li> <li>• <b>ipsec-client</b>: IP Security (IPsec) フェーズ 2 プロトコル</li> <li>• <b>other</b>: 新規プロトコル用に予約済み。</li> <li>• <b>srtsp</b>: RTP (SRTP) プロトコル</li> <li>• <b>ssh</b>: セキュア シェル (SSH) プロトコル</li> <li>• <b>ssl-client</b>: セキュア ソケット レイヤ (SSL) プロトコル</li> </ul>
-----------------	--

### デフォルト

デフォルトの動作や値はありません。

### コマンドモード

次の表は、このコマンドを入力できるモードを示しています。

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

### コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.4(1)	<b>ikev1</b> および <b>ikev2</b> キーワードが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

### 例

次に、すべての暗号化アクセラレータ統計情報をクリアする例を示します。

```
ciscoasa# clear crypto protocol statistics all
ciscoasa#
```

## 関連コマンド

コマンド	説明
<b>clear crypto accelerator statistics</b>	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。
<b>show crypto accelerator statistics</b>	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。
<b>show crypto protocol statistics</b>	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 crypto ssl

SSL 情報をクリアするには、特権 EXEC モードで **clear crypto ssl** コマンドを使用します。

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

## 構文の説明

<b>cache</b>	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。
<b>all</b>	(任意)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します。
<b>errors</b>	SSL エラーをクリアします。
<b>mib</b>	SSL MIB 統計情報をクリアします。
<b>objects</b>	SSL オブジェクト統計情報をクリアします。

## 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

次の表は、このコマンドを入力できるモードを示しています。

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

## コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

## 例

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

```
ciscoasa# clear crypto ssl cache all
ciscoasa#
```

## 関連コマンド

コマンド	説明
<b>show crypto ssl</b>	SSL 情報を表示します。

## clear cts

Cisco TrustSec と統合したときに ASA によって使用されたデー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 cts** コマンドを使用します。

**clear cts {environment-data | pac} [noconfirm]**

### 構文の説明

<b>noconfirm</b>	確認を求めずにデータをクリアします。
<b>environment-data</b>	Cisco ISE からダウンロードされたすべての CTS 環境データをクリアします。
<b>pac</b>	NVRAM に保存されている CTS PAC 情報をクリアします。

### 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。

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

### コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

### 使用上のガイドライン

環境データをクリアすると、次の環境データの更新を手動でトリガーできます。また、リフレッシュ タイマーが期限切れになると、システムによってデータが更新されます。環境データをクリアしても、Cisco TrustSec PAC はシステムから削除されませんが、トラフィック ポリシーに影響を与えません。

保存された PAC をクリアする前に、システムでは、PAC を使用しないと、Cisco TrustSec 環境データをダウンロードできないことを理解してください。ただし、システムにすでに存在する環境データが引き続き使用されます。**clear cts pac** コマンドを実行すると、システムが環境データのアップデートを取得できなくなります。

クラスターでは、このコマンドはマスター ユニットのみで使用できます。アクティブ/スタンバイ ハイ アベイラビリティ (フェールオーバー) では、このコマンドはアクティブ ユニットのみで使用できます。

## 例

次に、システムから CTS データをクリアする例を示します。

```
ciscoasa# clear cts pac
```

```
Are you sure you want to delete the cts PAC? (y/n) y
```

```
ciscoasa# clear cts environment-data
```

```
Are you sure you want to delete the cts environment data? (y/n) y
```

## 関連コマンド

コマンド	説明
<b>clear configure cts</b>	ASA と Cisco TrustSec を統合するためのコンフィギュレーションをクリアします。
<b>cts sxp enable</b>	ASA で SXP プロトコルをイネーブルにします。
<b>show cts</b>	Cisco TrustSec (CTS) 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 dhcpd** コマンドを使用します。

```
clear dhcpd {binding [all | ip_address] | statistics}
```

## 構文の説明

<b>all</b>	(任意)すべての dhcpd バインディングをクリアします。
<b>binding</b>	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。
<b>ip_address</b>	(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。
<b>statistics</b>	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。

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

## コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

## 使用上のガイドライン

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。

```
ciscoasa# clear dhcpd statistics
```

## 関連コマンド

コマンド	説明
<b>clear configure dhcpd</b>	すべての DHCP サーバ設定を削除します。
<b>show dhcpd</b>	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。

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

### コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

### 使用上のガイドライン

**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。

```
ciscoasa# clear dhcprelay statistics
ciscoasa#
```

### 関連コマンド

コマンド	説明
<b>clear configure dhcprelay</b>	DHCP リレー エージェントの設定をすべて削除します。
<b>debug dhcprelay</b>	DHCP リレー エージェントのデバッグ情報を表示します。
<b>show dhcprelay statistics</b>	DHCP リレー エージェントの統計情報を表示します。
<b>show running-config dhcprelay</b>	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

指定された完全修飾ドメイン名 (FQDN) ホストに関連付けられたすべての IP アドレスをクリアするには、特権 EXEC モードで **clear dns** コマンドを使用します。

```
clear dns [host fqdn_name]
```

## 構文の説明

<i>fqdn_name</i>	(オプション) 選択されたホストの完全修飾ドメイン名を指定します。
<b>host</b>	(オプション) 指定したホストの 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。

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

## コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

## 例

次に、指定した FQDN ホストに関連付けられた IP アドレスをクリアする例を示します。

```
ciscoasa# clear dns 10.1.1.2 www.example.com
```



(注)

**dns expire-entry** キーワードの設定は、このコマンドでは無視されます。新しい DNS クエリーは、アクティブ化された各 FQDN ホストに送信されます。

## 関連コマンド

コマンド	説明
<b>dns domain-lookup</b>	ASA 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。
<b>dns name-server</b>	DNS サーバアドレスを設定します。
<b>dns retries</b>	ASA 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。
<b>dns timeout</b>	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。
<b>show dns-hosts</b>	DNS キャッシュを表示します。

# 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。

## 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。

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

### コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

### 使用上のガイドライン

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。

### 例

次に、DNS キャッシュをクリアする例を示します。

```
ciscoasa# clear dns-hosts cache
```

### 関連コマンド

コマンド	説明
<b>dns domain-lookup</b>	ASA 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。
<b>dns name-server</b>	DNS サーバアドレスを設定します。
<b>dns retries</b>	ASA 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。
<b>dns timeout</b>	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。
<b>show dns-hosts</b>	DNS キャッシュを表示します。

## clear dynamic-filter dns-snoop

ボットネットトラフィックフィルタのDNSスヌーピングデータをクリアするには、特権 EXEC モードで **clear dynamic-filter dns-snoop** コマンドを使用します。

### clear dynamic-filter dns-snoop

#### 構文の説明

このコマンドには引数またはキーワードはありません。

#### コマンドデフォルト

デフォルトの動作や値はありません。

#### コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

#### コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

#### 例

次に、ボットネットトラフィックフィルタのDNSスヌーピングデータをすべてクリアする例を示します。

```
ciscoasa# clear dynamic-filter dns-snoop
```

#### 関連コマンド

コマンド	説明
<b>address</b>	IP アドレスをブラックリストまたはホワイトリストに追加します。
<b>clear configure dynamic-filter</b>	実行ボットネットトラフィックフィルタ コンフィギュレーションをクリアします。
<b>clear dynamic-filter reports</b>	ボットネットトラフィックフィルタのレポートデータをクリアします。
<b>clear dynamic-filter statistics</b>	ボットネットトラフィックフィルタの統計情報をクリアします。

コマンド	説明
<b>dns domain-lookup</b>	サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにします。
<b>dns server-group</b>	ASA の DNS サーバを指定します。
<b>dynamic-filter ambiguous-is-black</b>	グレイリストに登録されているトラフィックをブラックリストに登録されているトラフィックと同様のアクションで処理します。
<b>dynamic-filter blacklist</b>	ボットネット トラフィック フィルタのブラックリストを編集します。
<b>dynamic-filter database fetch</b>	ボットネット トラフィック フィルタのダイナミック データベースを手動で取得します。
<b>dynamic-filter database find</b>	ドメイン名または IP アドレスをダイナミック データベースから検索します。
<b>dynamic-filter database purge</b>	ボットネット トラフィック フィルタのダイナミック データベースを手動で削除します。
<b>dynamic-filter drop blacklist</b>	ブラックリストに登録されているトラフィックを自動でドロップします。
<b>dynamic-filter enable</b>	アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネット トラフィック フィルタをイネーブルにします。
<b>dynamic-filter updater-client enable</b>	ダイナミック データベースのダウンロードをイネーブルにします。
<b>dynamic-filter use-database</b>	ダイナミック データベースの使用をイネーブルにします。
<b>dynamic-filter whitelist</b>	ボットネット トラフィック フィルタのホワイトリストを編集します。
<b>inspect dns dynamic-filter-snoop</b>	DNS インспекションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。
<b>name</b>	ブラックリストまたはホワイトリストに名前を追加します。
<b>show asp table dynamic-filter</b>	高速セキュリティ パスにインストールされているボットネット トラフィック フィルタ ルールを表示します。
<b>show dynamic-filter data</b>	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプル エントリなど、ダイナミック データベースに関する情報を表示します。
<b>show dynamic-filter dns-snoop</b>	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。 <b>detail</b> キーワードを指定した場合は、実際の IP アドレスおよび名前を表示します。
<b>show dynamic-filter reports</b>	上位 10 個のボットネット サイト、ポート、および感染したホストに関するレポートを生成します。
<b>show dynamic-filter statistics</b>	ボットネット トラフィック フィルタでモニタされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。

コマンド	説明
<b>show dynamic-filter updater-client</b>	サーバの IP アドレス、ASA が次にサーバに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデート サーバに関する情報を表示します。
<b>show running-config dynamic-filter</b>	ボットネット トラフィック フィルタの実行コンフィギュレーションを表示します。

# clear dynamic-filter reports

ボットネットトラフィックフィルタのレポートデータをクリアするには、特権 EXEC モードで **clear dynamic-filter reports** コマンドを使用します。

```
clear dynamic-filter reports {top [malware-sites | malware-ports | infected-hosts] |
infected-hosts}
```

## 構文の説明

<b>malware-ports</b>	(任意) 上位 10 のマルウェア ポートのレポートデータをクリアします。
<b>malware-sites</b>	(任意) 上位 10 のマルウェア サイトのレポートデータをクリアします。
<b>infected-hosts (top)</b>	(任意) 上位 10 の感染したホストのレポートデータをクリアします。
<b>top</b>	上位 10 のマルウェア サイト、ポート、および感染したホストのレポートデータをクリアします。
<b>infected-hosts</b>	感染したホストのレポートデータをクリアします。

## コマンドデフォルト

デフォルトの動作や値はありません。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。
8.2(2)	<b>botnet-sites</b> キーワードおよび <b>botnet-ports</b> キーワードは <b>malware-sites</b> および <b>malware-ports</b> に変更されました。 <b>top</b> キーワードが、上位 10 のレポートのクリアを、感染したホストに関する新しいレポートのクリアと区別するために追加されました。 <b>infected-hosts</b> キーワードが追加されました ( <b>top</b> なし)。

## 例

次に、すべてのボットネットトラフィックフィルタの上位 10 のレポートデータをクリアする例を示します。

```
ciscoasa# clear dynamic-filter reports top
```

次に、上位 10 のマルウェア サイトのレポートデータだけをクリアする例を示します。

```
ciscoasa# clear dynamic-filter reports top malware-sites
```

次に、感染したホストのすべてのレポートデータをクリアする例を示します。

```
ciscoasa# clear dynamic-filter reports infected-hosts
```

## 関連コマンド

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

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

## clear dynamic-filter statistics

ボットネットトラフィックフィルタの統計情報をクリアするには、特権 EXEC モードで **clear dynamic-filter statistics** コマンドを使用します。

**clear dynamic-filter statistics [interface name]**

### 構文の説明

**interface name** (任意) 特定のインターフェイスの統計情報をクリアします。

### コマンドデフォルト

デフォルトの動作や値はありません。

### コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

### コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

### 例

次に、ボットネットトラフィックフィルタの DNS 統計情報をすべてクリアする例を示します。

```
ciscoasa# clear dynamic-filter statistics
```

### 関連コマンド

コマンド	説明
<b>dynamic-filter ambiguous-is-black</b>	グレイリストに登録されているトラフィックをブラックリストに登録されているトラフィックと同様のアクションで処理します。
<b>dynamic-filter drop blacklist</b>	ブラックリストに登録されているトラフィックを自動でドロップします。
<b>address</b>	IP アドレスをブラックリストまたはホワイトリストに追加します。
<b>clear configure dynamic-filter</b>	実行ボットネットトラフィックフィルタコンフィギュレーションをクリアします。
<b>clear dynamic-filter dns-snoop</b>	ボットネットトラフィックフィルタの DNS スヌーピングデータをクリアします。

コマンド	説明
<b>clear dynamic-filter reports</b>	ボットネットトラフィックフィルタのレポートデータをクリアします。
<b>dns domain-lookup</b>	サポートされているコマンドに対してネームルックアップを実行するために、ASAがDNSサーバにDNS要求を送信できるようにします。
<b>dns server-group</b>	ASAのDNSサーバを指定します。
<b>dynamic-filter blacklist</b>	ボットネットトラフィックフィルタのブラックリストを編集します。
<b>dynamic-filter database fetch</b>	ボットネットトラフィックフィルタのダイナミックデータベースを手動で取得します。
<b>dynamic-filter database find</b>	ドメイン名またはIPアドレスをダイナミックデータベースから検索します。
<b>dynamic-filter database purge</b>	ボットネットトラフィックフィルタのダイナミックデータベースを手動で削除します。
<b>dynamic-filter enable</b>	アクセスリストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネットトラフィックフィルタをイネーブルにします。
<b>dynamic-filter updater-client enable</b>	ダイナミックデータベースのダウンロードをイネーブルにします。
<b>dynamic-filter use-database</b>	ダイナミックデータベースの使用をイネーブルにします。
<b>dynamic-filter whitelist</b>	ボットネットトラフィックフィルタのホワイトリストを編集します。
<b>inspect dns dynamic-filter-snoop</b>	DNSインスペクションとボットネットトラフィックフィルタスヌーピングをイネーブルにします。
<b>name</b>	ブラックリストまたはホワイトリストに名前を追加します。
<b>show asp table dynamic-filter</b>	高速セキュリティパスにインストールされているボットネットトラフィックフィルタルールを表示します。
<b>show dynamic-filter data</b>	ダイナミックデータベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10個のサンプルエントリなど、ダイナミックデータベースに関する情報を表示します。
<b>show dynamic-filter dns-snoop</b>	ボットネットトラフィックフィルタのDNSスヌーピングの概要を表示します。 <b>detail</b> キーワードを指定した場合は、実際のIPアドレスおよび名前を表示します。
<b>show dynamic-filter reports infected-hosts</b>	感染ホストのレポートを生成します。
<b>show dynamic-filter reports top</b>	マルウェアサイト、ポート、および感染ホストの上位10件のレポートを生成します。
<b>show dynamic-filter statistics</b>	ボットネットトラフィックフィルタでモニタされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。
<b>show dynamic-filter updater-client</b>	サーバのIPアドレス、ASAが次にサーバに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデーターサーバに関する情報を表示します。
<b>show running-config dynamic-filter</b>	ボットネットトラフィックフィルタの実行コンフィギュレーションを表示します。

# 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

<i>as-number</i>	(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。ASA 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。

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

### コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードはサポートされます。

### 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。

```
ciscoasa# clear eigrp events
```

### 関連コマンド

コマンド	説明
<b>show eigrp events</b>	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

<i>as-number</i>	(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。ASA 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 (AS) (プロセス ID) を指定する必要はありません。
<i>if-name</i>	(任意) <b>nameif</b> 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。
<i>ip-addr</i>	(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。
<b>soft</b>	ASA 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。

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

## コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

## 使用上のガイドライン

**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。

```
ciscoasa# 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。

```
ciscoasa# clear eigrp neighbors outside
```

## 関連コマンド

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

<i>as-number</i>	(任意)EIGRP プロセスの自律システム番号を指定します。ASA 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(AS) (プロセス ID)を指定する必要はありません。
<i>ip-addr</i>	トポロジ テーブルからクリアする IP アドレス。
<i>mask</i>	(任意) <i>ip-addr</i> 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。

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

## コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

## 使用上のガイドライン

このコマンドは、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。

```
ciscoasa# clear eigrp topology 192.168.1.0 255.255.255.0
```

## 関連コマンド

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

## 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、特権 EXEC モードで **clear facility-alarm output** コマンドを使用します。

### clear facility-alarm 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。

#### コマンドデフォルト

デフォルトの動作や値はありません。

#### コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

#### コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

#### 使用上のガイドライン

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。

```
ciscoasa(config)# clear facility-alarm output
```

#### 関連コマンド

コマンド	説明
<b>alarm contact description</b>	アラーム入力の説明を指定します。
<b>alarm contact severity</b>	アラームの重大度を指定します。
<b>alarm contact trigger</b>	1 つまたはすべてのアラーム入力のトリガーを指定します。

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

# clear 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。

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

### コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

### 使用上のガイドライン

このコマンドは、**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。

```
ciscoasa# clear failover statistics
ciscoasa#
```

### 関連コマンド

コマンド	説明
<b>debug fover</b>	フェールオーバーのデバッグ情報を表示します。
<b>show failover</b>	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 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、特権 EXEC モードで **clear flow-export counters** コマンドを使用します。

## clear flow-export 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。

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

### コマンド履歴

リリース	変更内容
8.1(1)	このコマンドが追加されました。

### 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。

```
ciscoasa# clear flow-export counters
```

### 関連コマンド

コマンド	説明
<b>flow-export destination</b>	NetFlow コレクタの IP アドレスまたはホスト名と、NetFlow コレクタがリスンする UDP ポートを指定します。
<b>flow-export template timeout-rate</b>	テンプレート情報が NetFlow コレクタに送信される間隔を制御します。
<b>logging flow-export-syslogs enable</b>	<b>logging flow-export-syslogs disable</b> コマンドを入力した後に、syslog メッセージをイネーブルにし、さらに NetFlow データに関連付けられた syslog メッセージをイネーブルにします。
<b>show flow-export counters</b>	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統計情報またはオフロードされたフローをクリアするには、特権 EXEC モードで **clear flow-offload** コマンドを使用します。

**clear flow-offload {statistics | flow all}**

## 構文の説明

<b>statistics</b>	オフロードされたフローの統計情報をクリアします。
<b>flow all</b>	オフロードされたフローをクリアします。

## 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。

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

## コマンド履歴

リリース	変更内容
9.5(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 flow-offload statistics** コマンドは、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。

**clear flow-offload flow all** を使用してオフロードされたフローを削除すると、それらのフローの後続パケットは ASA に送信されます。ASA は、フローを再度オフロードします。このため、クリアしたフローの統計情報が不正確になります。このコマンドは、デバッグのためだけに使用します。

## 例

次に、統計情報をクリアする例を示します。

```
ciscoasa# clear flow-offload statistics
```

## 関連コマンド

コマンド	説明
<b>flow-offload</b>	フロー オフロードを有効にします。
<b>set-connection advanced-options flow-offload</b>	オフロードの対象としてトラフィック フローを指定します。
<b>show flow-offload</b>	オフロードするフロー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。

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

## 構文の説明

<i>interface_name</i>	(任意)ASA のインターフェイスを指定します。
<b>queue</b>	IP フラグメント再構築キューをクリアします。
<b>statistics</b>	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\_name* 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。

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

## コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、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、 <b>clear fragment</b> および <b>clear configure fragment</b> という 2 つのコマンドに分けられました。

## 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。

```
ciscoasa# clear fragment queue
```

## 関連コマンド

コマンド	説明
<b>clear configure fragment</b>	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。
<b>fragment</b>	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。
<b>show fragment</b>	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。
<b>show running-config fragment</b>	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(GC)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。

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

#### コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

#### 例

次に、GC プロセスの統計情報を削除する例を示します。

```
ciscoasa# clear gc
```

#### 関連コマンド

コマンド	説明
<b>show gc</b>	GC の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。

## デフォルト

デフォルトの動作や値はありません。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

## 例

次に、IGMP 統計情報カウンタをクリアする例を示します。

```
ciscoasa# clear igmp counters
```

## 関連コマンド

コマンド	説明
<b>clear igmp group</b>	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。
<b>clear igmp traffic</b>	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

<i>group</i>	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。
<i>interface name</i>	<b>namif</b> 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。

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

## コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

## 使用上のガイドライン

グループ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。

```
ciscoasa# clear igmp group
```

## 関連コマンド

コマンド	説明
<b>clear igmp counters</b>	すべての IGMP カウンタをクリアします。
<b>clear igmp traffic</b>	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。

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

### コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

### 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。

```
ciscoasa# clear igmp traffic
```

### 関連コマンド

コマンド	説明
<b>clear igmp group</b>	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。
<b>clear igmp counters</b>	すべての IGMP カウンタをクリアします。

# clear ikev1

IPsec IKEv1 SA または統計情報を削除するには、特権 EXEC モードで **clear ikev1** コマンドを使用します。すべての IKEv1 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 ikev1** {sa ip\_address | stats}

## 構文の説明

<b>sa ip_address</b>	SA をクリアします。
<b>stats</b>	IKEv1 統計情報をクリアします。

## 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。

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

## コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

## 使用上のガイドライン

すべての IPsec IKEv1 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、ASA からすべての IPsec IKEv1 統計情報を削除する例を示します。

```
ciscoasa# clear ikev1 stats
ciscoasa#
```

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。

```
ciscoasa# clear ikev1 sa peer 10.86.1.1
ciscoasa#
```

## 関連コマンド

コマンド	説明
<b>clear configure crypto map</b>	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。
<b>clear configure isakmp</b>	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。
<b>show ipsec sa</b>	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。
<b>show running-config crypto</b>	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、特権 EXEC モードで **clear ikev2** コマンドを使用します。すべての IKEv2 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 ikev2** {sa ip\_address | stats}

## 構文の説明

<b>sa ip_address</b>	SA をクリアします。
<b>stats</b>	IKEv2 統計情報をクリアします。

## 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。

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

## コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

## 使用上のガイドライン

すべての IPsec IKEv2 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、ASA からすべての IPsec IKEv2 統計情報を削除する例を示します。

```
ciscoasa# clear ikev2 stats
ciscoasa#
```

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。

```
ciscoasa# clear ikev2 sa peer 10.86.1.1
ciscoasa#
```

## 関連コマンド

コマンド	説明
<b>clear configure crypto map</b>	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。
<b>clear configure isakmp</b>	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。
<b>show ipsec sa</b>	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。
<b>show running-config crypto</b>	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

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

<i>interface_name</i>	(任意) <b>nameif</b> 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。
<i>mapped_name</i>	(任意) <b>allocate-interface</b> 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。
<i>physical_interface</i>	(任意) <b>gigabitenet0/1</b> 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、 <b>interface</b> コマンドを参照してください。
<i>subinterface</i>	(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。

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

## コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

## 使用上のガイドライン

インターフェイス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、ASA 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、ASA 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。

```
ciscoasa# clear interface
```

## 関連コマンド

コマンド	説明
<b>clear configure interface</b>	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。
<b>interface</b>	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。
<b>show interface</b>	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。
<b>show running-config interface</b>	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ー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

<b>global</b>	(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。
<b>interface</b> <i>interface_name</i>	(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。

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

### コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

### 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。

```
ciscoasa# clear ip audit count
```

### 関連コマンド

コマンド	説明
<b>ip audit interface</b>	監査ポリシーをインターフェイスに割り当てます。
<b>ip audit name</b>	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。
<b>show ip audit count</b>	監査ポリシーのシグニチャー一致の数を表示します。
<b>show running-config ip audit attack</b>	<b>ip audit attack</b> コマンドの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。

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

### 構文の説明

<b>counters</b>	(任意)すべてのカウンタをクリアします。
<b>entry</b>	(オプション)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。
<b>inactive</b>	(オプション)トラフィックを渡すことができない IPsec SA をクリアします。
<b>map map-name</b>	(オプション)指定したクリプトマップの IPsec SA をクリアします。
<b>peer</b>	(オプション)指定したピアの IPsec SA をクリアします。
<b>peer-addr</b>	IPsec ピアの IP アドレスを指定します。
<b>protocol</b>	IPsec プロトコル <b>esp</b> または <b>ah</b> を指定します。
<b>spi</b>	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。

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

### コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

### 使用上のガイドライン

同じ機能を実行するために、このコマンドの別の形式である **clear crypto ipsec sa** を使用できます。

## 例

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

```
ciscoasa# clear ipsec sa counters  
ciscoasa#
```

## 関連コマンド

コマンド	説明
<b>show ipsec sa</b>	指定されたパラメータに基づいて IPsec SA を表示します。
<b>show ipsec stats</b>	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 (廃止)

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。

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

### コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	このコマンドは廃止されました。

### 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。

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

### 関連コマンド

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

# 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、特権 EXEC モードで **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

<b>binding</b>	IPv6 DHCP リレー バインディング エントリをクリアします。
<i>ip_address</i>	(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。
<b>statistics</b>	IPv6 DHCP リレー エージェントの統計情報をクリアします。

## 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		
	ルーテッド	トランスペ アレント	シングル	マルチ コンテキ スト	システム
コマンドモード					
特権 EXEC	• 対応	—	• 対応	• 対応	—

## コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

## 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。

```
ciscoasa# clear ipv6 dhcprelay binding
ciscoasa#
```

## 関連コマンド

コマンド	説明
<b>show ipv6 dhcprelay binding</b>	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。
<b>show ipv6 dhcprelay statistics</b>	IPv6 DHCP リレー エージェントの情報を表示します。

## clear ipv6 dhcp statistics

DHCPv6 クライアントと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、特権 EXEC モードで **clear ipv6 dhcp client statistics** 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

<b>client</b>	DHCPv6 クライアントの統計情報をクリアします。
<b>interface</b> <i>interface_name</i>	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。
<b>pd</b>	プレフィックス委任クライアントの統計情報をクリアします。
<b>server</b>	DHCPv6 サーバの統計情報をクリアします。

### コマンドデフォルト

デフォルトの動作や値はありません。

### コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

### コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

### 使用上のガイドライン

このコマンドは、DHCPv6 クライアントの統計情報をクリアします。

### 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。

```
ciscoasa# clear ipv6 dhcp client statistics
```

次に、DHCPv6 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例を示します。

```
ciscoasa# clear ipv6 dhcp client pd statistics
```

次に、外部インターフェイスで統計情報をクリアする例を示します。

```
ciscoasa# clear ipv6 dhcp interface outside statistics
```

次に、DHCPv6 サーバの統計情報をクリアする例を示します。

```
ciscoasa# clear ipv6 dhcp server statistics
```

関連コマンド

コマンド	説明
<b>clear ipv6 dhcp statistics</b>	DHCPv6 統計情報をクリアします。
<b>domain-name</b>	IR メッセージへの応答で SLAAC クライアントに提供されるドメイン名を設定します。
<b>dns-server</b>	IR メッセージへの応答で SLAAC クライアントに提供される DNS サーバを設定します。
<b>import</b>	ASA がプレフィックス委任クライアントインターフェイスで DHCPv6 サーバから取得した 1 つ以上のパラメータを使用し、その後、IR メッセージへの応答でそれらを SLAAC クライアントに提供します。
<b>ipv6 address</b>	IPv6 を有効にし、インターフェイスに IPv6 アドレスを設定します。
<b>ipv6 address dhcp</b>	インターフェイスの DHCPv6 を使用してアドレスを取得します。
<b>ipv6 dhcp client pd</b>	委任されたプレフィックスを使用して、インターフェイスのアドレスを設定します。
<b>ipv6 dhcp client pd hint</b>	受信を希望する委任されたプレフィックスについて 1 つ以上のヒントを提供します。
<b>ipv6 dhcp pool</b>	DHCPv6 ステートレス サーバを使用して、特定のインターフェイスで SLAAC クライアントに提供する情報を含むプールを作成します。
<b>ipv6 dhcp server network</b>	DHCPv6 ステートレス サーバを有効にします。
<b>network</b>	サーバから受信した委任されたプレフィックスをアドバタイズするように BGP を設定します。
<b>nis address</b>	IR メッセージへの応答で SLAAC クライアントに提供される NIS アドレスを設定します。
<b>nis domain-name</b>	IR メッセージへの応答で SLAAC クライアントに提供される NIS ドメイン名を設定します。
<b>nisp address</b>	IR メッセージへの応答で SLAAC クライアントに提供される NISP アドレスを設定します。
<b>nisp domain-name</b>	IR メッセージへの応答で SLAAC クライアントに提供される NISP ドメイン名を設定します。
<b>show bgp ipv6 unicast</b>	IPv6 BGP ルーティング テーブルのエントリを表示します。
<b>show ipv6 dhcp</b>	DHCPv6 情報を表示します。
<b>show ipv6 general-prefix</b>	DHCPv6 プレフィックス委任クライアントによって獲得されたすべてのプレフィックスと、そのプレフィックスの他のプロセスへの ASA 配布を表示します。
<b>sip address</b>	IR メッセージへの応答で SLAAC クライアントに提供される SIP アドレスを設定します。
<b>sip domain-name</b>	IR メッセージへの応答で SLAAC クライアントに提供される SIP ドメイン名を設定します。
<b>sntp address</b>	IR メッセージへの応答で SLAAC クライアントに提供される SNTP アドレスを設定します。

# 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。

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

### コマンド履歴

リリース	変更内容
7.2(4)	このコマンドが追加されました。

### 使用上のガイドライン

**clear ipv6 mld traffic** コマンドを使用すると、すべての MLD トラフィック カウンタをリセットできます。

### 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。

```
ciscoasa# clear ipv6 mld traffic
ciscoasa#
```

### 関連コマンド

コマンド	説明
<b>debug ipv6 mld</b>	MLD のすべてのデバッグ メッセージを表示します。
<b>show debug ipv6 mld</b>	現在のコンフィギュレーション内の IPv6 に対する MLD 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。

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

### コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

### 使用上のガイドライン

このコマンドは、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。

```
ciscoasa# clear ipv6 neighbors
ciscoasa#
```

### 関連コマンド

コマンド	説明
<b>ipv6 neighbor</b>	IPv6 ネイバー探索キャッシュのスタティック エントリを設定します。
<b>show ipv6 neighbor</b>	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、特権 EXEC モードで **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

<b>counters</b>	OSPF プロセス カウンタをリセットします。
<b>events</b>	OSPF イベント ログをクリアします。
<b>force-ospf</b>	OSPF プロセスの SPF をクリアします。
<b>process</b>	OSPFv3 プロセスをリセットします。
<i>process_id</i>	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。
<b>redistribution</b>	OSPFv3 ルート再配布をクリアします。
<b>traffic</b>	トラフィック関連の統計情報をクリアします。

## 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。

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

## コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

## 使用上のガイドライン

このコマンドは、すべての OSPFv3 ルーティング パラメータを削除します。

## 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。

```
ciscoasa# clear ipv6 ospf redistribution
ciscoasa#
```

## 関連コマンド

コマンド	説明
<b>show running-config ipv6 router</b>	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。
<b>clear configure ipv6 router</b>	OSPFv3 ルーティング プロセスをクリアします。

# clear ipv6 prefix-list

ルーティング プレフィックス リストをクリアするには、特権 EXEC モードで **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* **ipv6 prefix-list** コマンドによって作成された名前付きプレフィックス リストをクリアします。

## 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。

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

## コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

## 使用上のガイドライン

このコマンドは、IPv6 プレフィックス リストを削除します。

## 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。

```
ciscoasa# clear ipv6 prefix-list list1
ciscoasa#
```

## 関連コマンド

コマンド	説明
<b>show running-config ipv6 prefix-list</b>	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。
<b>clear configure ipv6 prefix-list</b>	IPv6 プレフィックス損失コンフィギュレーションをクリアします。

# 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、特権 EXEC モードで **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

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

## 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。

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

## コマンド履歴

リリース	変更内容
9.5(1)	このコマンドが追加されました。

## 使用上のガイドライン

**clear ipv6 route** コマンドは、IPv6 に固有であることを除き、**clear ip route** コマンドと類似しています。

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。

```
ciscoasa# clear ipv6 route 2001:0DB8::/35
```

## 関連コマンド

コマンド	説明
<b>show ipv6 route</b>	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、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。

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

### コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

### 使用上のガイドライン

このコマンドを使用すると、**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。

```
ciscoasa# clear ipv6 traffic
ciscoasa# 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
<b>show ipv6 traffic</b>	IPv6 トラフィックの統計情報を表示します。

# 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。

**clear ip verify statistics** [**interface** *interface\_name*]

## 構文の説明

**interface** 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。  
*interface\_name*

## デフォルト

デフォルトの動作や値はありません。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

## 使用上のガイドライン

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。

## 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。

```
ciscoasa# clear ip verify statistics
```

## 関連コマンド

コマンド	説明
<b>clear configure ip verify reverse-path</b>	<b>ip verify reverse-path</b> コンフィギュレーションをクリアします。
<b>ip verify reverse-path</b>	ユニキャスト RPF 機能をイネーブルにして、IP スプーフィングを防ぎます。
<b>show ip verify statistics</b>	ユニキャスト RPF 統計情報を表示します。
<b>show running-config ip verify reverse-path</b>	<b>ip verify reverse-path</b> コンフィギュレーションを表示します。

# clear isakmp sa

IKEv1 および IKEv2 ランタイム SA データベースをすべて削除するには、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。

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

### コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(1)	<b>clear isakmp sa</b> コマンドが、 <b>clear crypto isakmp sa</b> に変更されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

### 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。

```
ciscoasa# clear isakmp sa
ciscoasa#
```

### 関連コマンド

コマンド	説明
<b>clear isakmp</b>	IKE ランタイム SA データベースをクリアします。
<b>isakmp enable</b>	IPsec ピアが ASA 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。
<b>show isakmp stats</b>	実行時統計情報を表示します。
<b>show isakmp sa</b>	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。
<b>show running-config isakmp</b>	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 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

<b>*</b>	すべての IS-IS データ構造をクリアします。
<b>level-1</b>	(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。
<b>level-2</b>	(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。
<b>lspfull</b>	IS-IS LSPFULL 状態をクリアします。
<i>network_mask</i>	(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。
<i>network_prefix</i>	(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。
<b>rib redistribution</b>	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。

## デフォルト

デフォルトの動作や値はありません。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

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。

```
ciscoasa# 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。

```
ciscoasa# clear isis rib redistribution 10.1.0.0 255.255.0.0
```

関連コマンド

コマンド	説明
<b>advertise passive-only</b>	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
<b>area-password</b>	IS-IS エリア認証パスワードを設定します。
<b>authentication key</b>	IS-IS の認証をグローバルで有効にします。
<b>authentication mode</b>	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
<b>authentication send-only</b>	グローバルな IS-IS インスタンスでは、送信される (受信ではなく) IS-IS パケットでのみ認証が実行されるように設定します。
<b>default-information originate</b>	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
<b>distance</b>	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
<b>domain-password</b>	IS-IS ドメイン認証パスワードを設定します。
<b>fast-flood</b>	IS-IS LSP がフルになるように設定します。
<b>hello padding</b>	IS-IS hello をフル MTU サイズに設定します。
<b>hostname dynamic</b>	IS-IS ダイナミック ホスト名機能を有効にします。
<b>ignore-lsp-errors</b>	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
<b>isis adjacency-filter</b>	IS-IS 隣接関係の確立をフィルタ処理します。
<b>isis advertise-prefix</b>	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
<b>isis authentication key</b>	インターフェイスに対する認証を有効にします。
<b>isis authentication mode</b>	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
<b>isis authentication send-only</b>	送信される (受信ではなく) IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
<b>isis circuit-type</b>	IS-IS で使用される隣接関係のタイプを設定します。
<b>isis csnp-interval</b>	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
<b>isis hello-interval</b>	IS-IS が連続して hello パケットを送信する時間の長さを指定します。

コマンド	説明
<b>isis hello-multiplier</b>	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
<b>isis hello padding</b>	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
<b>isis lsp-interval</b>	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
<b>isis metric</b>	IS-IS メトリックの値を設定します。
<b>isis password</b>	インターフェイスの認証パスワードを設定します。
<b>isis priority</b>	インターフェイスでの指定された ASA のプライオリティを設定します。
<b>isis protocol shutdown</b>	インターフェイスごとに IS-IS プロトコルを無効にします。
<b>isis retransmit-interval</b>	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
<b>isis retransmit-throttle-interval</b>	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
<b>isis tag</b>	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
<b>is-type</b>	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
<b>log-adjacency-changes</b>	NLSP IS-IS 隣接関係がステートを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
<b>lsp-full suppress</b>	PDU がフルになったときに、抑制されるルートを設定します。
<b>lsp-gen-interval</b>	LSP 生成の IS-IS スロットリングをカスタマイズします。
<b>lsp-refresh-interval</b>	LSP の更新間隔を設定します。
<b>max-area-addresses</b>	IS-IS エリアの追加の手动アドレスを設定します。
<b>max-lsp-lifetime</b>	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
<b>maximum-paths</b>	IS-IS のマルチパス ロード シェアリングを設定します。
<b>metric</b>	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
<b>metric-style</b>	新規スタイル、長さ、および値オブジェクト (TLV) を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
<b>net</b>	ルーティング プロセスの NET を指定します。
<b>passive-interface</b>	パッシブ インターフェイスを設定します。
<b>prc-interval</b>	PRC の IS-IS スロットリングをカスタマイズします。
<b>protocol shutdown</b>	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
<b>redistribute isis</b>	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
<b>route priority high</b>	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
<b>router isis</b>	IS-IS ルーティングをイネーブルにします。
<b>set-attached-bit</b>	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。

コマンド	説明
<b>set-overload-bit</b>	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
<b>show clns</b>	CLNS 固有の情報を表示します。
<b>show isis</b>	IS-IS の情報を表示します。
<b>show route isis</b>	IS-IS ルートを表示します。
<b>spf-interval</b>	SPF 計算の IS-IS スロットリングをカスタマイズします。
<b>summary-address</b>	IS-IS の集約アドレスを作成します。

