CHAPTER 6

clear configuration session コマンド ～ clear isis rib distribution 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。

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

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
clear session	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。
configure session	セッションを作成するか、開きます。
show configuration session	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

all	実行コンフィギュレーション全体をクリアします。
command	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、**clear configure ?** コマンドを使用して CLI ヘルプを確認してください。
primary	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。
secondary	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。

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

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使用されるマスター 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
show running-config	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*]]

構文の説明

address	（任意）指定された送信元または宛先の IP アドレスとの接続をクリアします。
all	（任意）to-the-box 接続を含む、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 接続だけがクリアされます。
dest_ip	（任意）宛先 IP アドレス（IPv4 または IPv6）を指定します。範囲を指定するには、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`
dest_port	（任意）宛先ポート番号を指定します。範囲を指定するには、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`
netmask *mask*	（任意）指定された IP アドレスで使用するサブネット マスクを指定します。
port	（任意）指定された送信元または宛先のポートとの接続をクリアします。
protocol {tcp | udp | sctp}	（任意）指定されたプロトコルを持つ接続をクリアします。
src_ip	（任意）送信元 IP アドレス（IPv4 または IPv6）を指定します。範囲を指定するには、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`
src_port	（任意）送信元ポートの番号を指定します。範囲を指定するには、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`
user [*domain_nickname*****]*user_name*	（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。*domain_nickname* 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。
user-group [*domain_nickname*****]*user_group_name*	（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。*domain_nickname* 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。
zone [*zone_name*]	トラフィック ゾーンに所属する接続をクリアします。

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	• Yes	• Yes	• Yes	• Yes	—

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 **user** および **user-group** キーワードが追加されました。
9.3(2)	**zone** キーワードが追加されました。
9.5(2)	**protocol sctp** 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
```

関連コマンドS

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

clear console-output

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

clear console-output

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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
console timeout	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。
show console-output	キャプチャされているコンソール出力を表示します。
show running-config console timeout	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。

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

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
coredump enable	コアダンプ機能をイネーブルにします。
clear configure coredump	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。
show coredump filesystem	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。
show coredump log	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

all	（任意）すべてのフィルタ詳細をクリアします。
context *context-name*	（任意）コンテキスト名を指定します。
counter_name	（任意）名前でカウンタを指定します。どのカウンタが使用可能かを確認するには、**show counters protocol** コマンドを使用します。
detail	（任意）カウンタの詳細情報をクリアします。
protocol *protocol_name*	（任意）指定したプロトコルのカウンタをクリアします。
summary	（任意）カウンタの要約をクリアします。
threshold *n*	（任意）指定されたしきい値以上になっているカウンタをクリアします。指定できる範囲は 1 ～ 4294967295 です。
top *n*	（任意）指定されたしきい値以上になっているカウンタをクリアします。指定できる範囲は 1 ～ 4294967295 です。

デフォルト

clear counters summary detail 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。

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

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
show counters	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。

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

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

show cpu	CPU に関する情報を表示します。
show cpu profile	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

module {**0** | **1**}	（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。

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

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

crashinfo force	ASAを強制的にクラッシュさせます。
crashinfo save disable	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。
crashinfo test	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。
show crashinfo	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。
show crashinfo files	日付とタイムスタンプに基づいて、最新の 5 つのクラッシュ情報ファイルを表示します。

clear crypto accelerator statistics

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

clear crypto accelerator statistics

構文の説明

このコマンドには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。

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

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

clear crypto ca crls

指定したトラストポイントに関連付けられたすべての 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

trustpoint *trust_point_name*	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。*trust_point_name* を指定せず trustpoint キーワードを指定した場合、コマンドは失敗します。
trustpool	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。

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

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
crypto ca crl request	トラストポイントの CRL コンフィギュレーションに基づいて CRL をダウンロードします。
show crypto ca crl	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。

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

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
crypto ca trustpool export	PKI trustpool を構成する証明書をエクスポートします。
crypto ca trustpool import	PKI trustpool を構成する証明書をインポートします。
crypto ca trustpool remove	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

sa *ip_address*	SA をクリアします。
stats	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。

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

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

clear crypto 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

sa *ip_address*	SA をクリアします。
stats	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。

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

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

clear crypto 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

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。
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。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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

clear crypto 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

sa	IKEv1 および IKEv2 SA をクリアします。
stats	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。

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

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
clear configure crypto map	すべてまたは指定されたクリプト マップをコンフィギュレーションからクリアします。
clear configure isakmp	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
show 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 crypto protocol statistics

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

clear crypto protocol statistics *protocol*

構文の説明

protocol	統計情報をクリアするプロトコルの名前を指定します。プロトコルの選択肢は次のとおりです。 • **all**：現在サポートされているすべてのプロトコル。 • **ikev1**：インターネット キー エクスチェンジ（IKE）バージョン 1 • **ikev2**：インターネット キー エクスチェンジ（IKE）バージョン 2 • **ipsec-client**：IP Security（IPsec）フェーズ 2 プロトコル • **other**：新規プロトコル用に予約済み。 • **srtp**：RTP（SRTP）プロトコル • **ssh**：セキュア シェル（SSH）プロトコル • **ssl-client**：セキュア ソケット レイヤ（SSL）プロトコル

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

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)	**ikev1** および **ikev2** 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
clear crypto accelerator statistics	暗号アクセラレータ MIB にあるグローバルおよびアクセラレータ固有の統計情報をクリアします。
show crypto accelerator statistics	暗号アクセラレータ MIB からグローバルおよびアクセラレータ固有の統計情報を表示します。
show crypto protocol statistics	クリプト アクセラレータ MIB のプロトコル固有の統計情報を表示します。

clear 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

cache	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。
all	(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。
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。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

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
show crypto ssl	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**}

構文の説明

environment-data	すべての CTS 環境データをクリアします。
pac	保存された CTS PAC をクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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

clear cts コマンドに **environment-data** キーワードを使用すると、Cisco ISE からダウンロードされた Cisco TrustSec 環境データがクリアされます。次回の環境データの更新を手動でトリガーできます。または、リフレッシュ タイマーが期限切れになると、ASAによってデータが更新されます。**clear cts environment-data** を実行しても、Cisco TrustSec PAC はASA から削除されません。**clear cts nvironment-data** コマンドの実行はトラフィック ポリシーに影響するため、アクションの確認が求められます。

clear cts コマンドに **pac** キーワードを使用すると、ASA 上の NVRAM に保存された PAC 情報がクリアされます。PAC がない場合、ASAは Cisco TrustSec 環境データをダウンロードできません。ただし、ASA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、ASA が環境データのアップデートを取得できなくなるため、アクションを確認するように求められます。

制約事項

- HA: このコマンドは、HA 設定のスタンバイ デバイスではサポートされません。スタンバイ デバイスで **clear cts** [**environment-data** | **pac**] を実行すると、次のエラー メッセージが表示されます。

  This command is only permitted on the primary device.

- クラスタリング: このコマンドは、マスター デバイスでのみサポートされます。スレーブ デバイスで **clear cts** [**environment-data | pac**] を実行すると、次のエラー メッセージが表示されます。

  This command is only permitted on the master device.

例

次に、ASAと Cisco TrustSec との統合で使用されたデータを ASA から削除する例を示します。

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

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

関連コマンド

コマンド	説明
clear configure all	ASA上の実行コンフィギュレーション全体をクリアします。
clear configure cts	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。
cts sxp enable	ASAで SXP プロトコルをイネーブルにします。

clear dhcpd

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

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

構文の説明

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

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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

clear dhcprelay statistics

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

clear dhcprelay statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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

clear dns

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

fqdn_name	（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。
host	（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。

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

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
dns domain-lookup	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。
dns name-server	DNS サーバ アドレスを設定します。
dns retries	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。
dns timeout	次の DNS サーバを試行するまでに待機する時間を指定します。
show dns-hosts	DNS キャッシュを表示します。

clear 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。

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

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
dns domain-lookup	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。
dns name-server	DNS サーバ アドレスを設定します。
dns retries	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。
dns timeout	次の DNS サーバを試行するまでに待機する時間を指定します。
show dns-hosts	DNS キャッシュを表示します。

clear 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。

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

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
address	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。
clear configure dynamic-filter	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。
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します。
dns domain-lookup	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。
dns server-group	ASAの DNS サーバを指定します。

コマンド	説明
dynamic-filter ambiguous-is-black	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。
dynamic-filter blacklist	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。
dynamic-filter database fetch	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。
dynamic-filter database find	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。
dynamic-filter database purge	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。
dynamic-filter drop blacklist	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。
dynamic-filter enable	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。
dynamic-filter updater-client enable	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。
dynamic-filter use-database	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。
dynamic-filter whitelist	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。
inspect dns dynamic-filter-snoop	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。
name	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。
show asp table dynamic-filter	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。
show dynamic-filter data	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。
show dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。**detail** 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。
show dynamic-filter reports	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。
show dynamic-filter statistics	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。
show dynamic-filter updater-client	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。
show running-config dynamic-filter	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

malware-ports	（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。
malware-sites	（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。
infected-hosts (**top**)	（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。
top	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。
infected-hosts	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。

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

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)	**botnet-sites** キーワードおよび **botnet-ports** キーワードは **malware-sites** および **malware-ports** に変更されました。**top** 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。**infected-hosts** キーワードが追加されました（**top** 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
address	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。
clear configure dynamic-filter	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。
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します。
dns domain-lookup	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。
dns server-group	ASAの DNS サーバを指定します。
dynamic-filter ambiguous-is-black	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。
dynamic-filter blacklist	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。
dynamic-filter database fetch	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。
dynamic-filter database find	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。
dynamic-filter database purge	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。
dynamic-filter drop blacklist	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。
dynamic-filter enable	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。
dynamic-filter updater-client enable	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。
dynamic-filter use-database	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。
dynamic-filter whitelist	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。
inspect dns dynamic-filter-snoop	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。
name	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。
show asp table dynamic-filter	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。
show dynamic-filter data	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。
show dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。**detail** 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。

コマンド	説明
show dynamic-filter reports infected-hosts	感染ホストのレポートを生成します。
show dynamic-filter reports top	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。
show dynamic-filter statistics	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。
show dynamic-filter updater-client	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。
show running-config dynamic-filter	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。

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

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
dynamic-filter ambiguous-is-black	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。
dynamic-filter drop blacklist	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。
address	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。
clear configure dynamic-filter	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。
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 データをクリアします。

コマンド	説明
dns domain-lookup	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。
dns server-group	ASAの DNS サーバを指定します。
dynamic-filter blacklist	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。
dynamic-filter database fetch	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。
dynamic-filter database find	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。
dynamic-filter database purge	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。
dynamic-filter enable	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。
dynamic-filter updater-client enable	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。
dynamic-filter use-database	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。
dynamic-filter whitelist	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。
inspect dns dynamic-filter-snoop	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。
name	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。
show asp table dynamic-filter	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。
show dynamic-filter data	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。
show dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。**detail** 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。
show dynamic-filter reports infected-hosts	感染ホストのレポートを生成します。
show dynamic-filter reports top	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。
show dynamic-filter statistics	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。
show dynamic-filter updater-client	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。
show running-config dynamic-filter	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

as-number	(任意)イベント ログをクリアする EIGRP プロセスの自律システム番号を指定します。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。

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

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
show eigrp events	EIGRP イベント ログを表示します。

clear eigrp neighbors

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

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

構文の説明

as-number	（任意）ネイバー エントリを削除する EIGRP プロセスの自律システム番号を指定します。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。
if-name	（任意）**nameif** コマンドで指定されたインターフェイスの名前。インターフェイス名を指定すると、このインターフェイスを介して学習されたすべてのネイバー テーブル エントリが削除されます。
ip-addr	（任意）ネイバー テーブルから削除するネイバーの IP アドレス。
soft	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。

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

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

clear eigrp topology

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

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

構文の説明

as-number	（任意）EIGRP プロセスの自律システム番号を指定します。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。
ip-addr	トポロジ テーブルからクリアする IP アドレス。
mask	（任意）*ip-addr* 引数に適用するネットワーク マスク。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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
show eigrp topology	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。

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

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、LED のアラーム状態をクリアします。ただし、実際のアラーム条件は引き続き有効で、**show facility-alarm status** コマンドで確認できます。

例

次に、出力リレーの電源を切り、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
alarm contact description	アラーム入力の説明を指定します。
alarm contact severity	アラームの重大度を指定します。
alarm contact trigger	1 つまたはすべてのアラーム入力にトリガーを指定します。
alarm facility input-alarm	アラーム入力のロギングと通知のオプションを指定します。
alarm facility power-supply rps	電源アラームを設定します。

コマンド	説明
alarm facility temperature	温度アラームを設定します。
alarm facility temperature（上限および下限しきい値）	下限または上限の温度しきい値を設定します。
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	すべての外部アラーム設定を表示します。
show facility-alarm relay	アクティブ状態のリレーを表示します。
show facility-alarm status	すべてのトリガーされたアラーム、または指定された重大度に基づく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。

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

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

clear flow-export counters

NetFlow データに関連付けられているランタイム 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。

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

コマンド履歴

リリース	変更内容
8.1(1)	このコマンドが追加されました。

使用上のガイドライン

ランタイム カウンタには、統計データおよびエラー データが含まれます。

例

次に、NetFlow データに関連付けられているランタイム 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
flow-export destination	NetFlow コレクタの IP アドレスまたはホスト名と、NetFlow コレクタがリッスンする UDP ポートを指定します。
flow-export template timeout-rate	テンプレート情報が NetFlow コレクタに送信される間隔を制御します。
logging flow-export-syslogs enable	**logging flow-export-syslogs disable** コマンドを入力した後に、syslog メッセージをイネーブルにし、さらに NetFlow データに関連付けられた syslog メッセージをイネーブルにします。
show flow-export counters	NetFlow の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

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

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

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
flow-offload	フロー オフロードを有効にします。
set-connection advanced-options flow-offload	トラフィック フローをオフロード対象として特定します。
show flow-offload	オフロードするフローに関する情報を表示します。

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

interface_name	（任意）ASAのインターフェイスを指定します。
queue	IP フラグメント再構築キューをクリアします。
statistics	IP フラグメント再構築統計情報をクリアします。

デフォルト

interface_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。

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

コマンド履歴

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

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
clear configure fragment	IP フラグメント再構成コンフィギュレーションをクリアし、デフォルトにリセットします。
fragment	パケット フラグメンテーションを詳細に管理できるようにし、NFS との互換性を高めます。
show fragment	IP フラグメント再構成モジュールの動作データを表示します。
show running-config fragment	IP フラグメント再構成コンフィギュレーションを表示します。

clear gc

ガーベッジ コレクション(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。

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

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
show gc	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。

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

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

clear igmp group

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

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

構文の説明

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

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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

clear igmp traffic

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

clear igmp traffic

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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

clear 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

sa *ip_address*	SA をクリアします。
stats	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。

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

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
clear configure crypto map	すべてまたは指定されたクリプト マップをコンフィギュレーションからクリアします。
clear configure isakmp	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。

コマンド	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、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

sa *ip_address*	SA をクリアします。
stats	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。

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

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

clear interface

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

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

構文の説明

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

デフォルト

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

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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
clear configure interface	インターフェイス コンフィギュレーションをクリアします。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。
show running-config interface	インターフェイスの設定を表示します。

clear ip audit count

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

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

構文の説明

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

デフォルト

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

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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

clear 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

counters	(任意)すべてのカウンタをクリアします。
entry	(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。
inactive	(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。
map *map-name*	(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。
peer	(オプション)指定したピアの IPsec SA をクリアします。
peer-addr	IPsec ピアの IP アドレスを指定します。
protocol	IPsec プロトコル **esp** または **ah** を指定します。
spi	IPsec SPI を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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

clear ipv6 access-list counters（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。

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

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

clear ipv6 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

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。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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
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 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

client	DHCPv6 クライアントの統計情報をクリアします。
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。
pd	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。
server	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。

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

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
clear ipv6 dhcp statistics	DHCPv6 統計情報をクリアします。
domain-name	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。
dns-server	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。
import	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。
ipv6 address	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。
ipv6 address dhcp	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。
ipv6 dhcp client pd	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。
ipv6 dhcp client pd hint	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。
ipv6 dhcp pool	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。
ipv6 dhcp server	DHCPv6 ステートレス サーバを有効にします。
network	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。
nis address	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。
nis domain-name	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。
nisp address	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。
nisp domain-name	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。
show bgp ipv6 unicast	IPv6 BGP ルーティング テーブルのエントリを表示します。
show ipv6 dhcp	DHCPv6 情報を表示します。
show ipv6 general-prefix	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。
sip address	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。
sip domain-name	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。
sntp address	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。

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

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
debug ipv6 mld	MLD のすべてのデバッグ メッセージを表示します。
show debug ipv6 mld	現在のコンフィギュレーション内の IPv6 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。

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

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
ipv6 neighbor	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。
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、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

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。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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
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 configure ipv6 router	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。

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

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
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 configure ipv6 prefix-list	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

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 モード

次の表に、コマンドを入力できるモードを示します。

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

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
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、特権 EXEC モードで **clear ipv6 traffic** コマンドを使用します。

clear ipv6 traffic

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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
show ipv6 traffic	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 *interface_name*	ユニキャスト RPF 統計情報をクリアするインターフェイスを設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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
clear configure ip verify reverse-path	**ip verify reverse-path** コンフィギュレーションをクリアします。
ip verify reverse-path	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。
show ip verify statistics	ユニキャスト RPF 統計情報を表示します。
show running-config ip verify reverse-path	**ip verify reverse-path** コンフィギュレーションを表示します。

clear 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。

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

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)	**clear isakmp sa** コマンドが、**clear crypto isakmp sa** 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
clear isakmp	IKE ランタイム SA データベースをクリアします。
isakmp enable	IPsec ピアが 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。
show isakmp stats	実行時統計情報を表示します。
show isakmp sa	追加情報を含め、IKE ランタイム SA データベースを表示します。
show running-config isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

clear 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。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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

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

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