clear a – clear k

clear aaa kerberos

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

clear aaa kerberos { **tickets** [**username** *user*] | **keytab** }

構文の説明

keytab	Kerberos キータブファイルをクリアします。
tickets [**username** *user*]	Kerberosチケット情報をクリアします。チケットをクリアするユーザーを指定するusernameキーワードを含めない限り、すべてのチケットがクリアされます。

コマンド デフォルト

デフォルト設定はありません。

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。
9.8(4)	**keytab** キーワードが追加されました。

例

次に、すべての Kerberos チケットをクリアする例を示します。

```
ciscoasa# clear aaa kerberos tickets

Proceed with deleting kerberos tickets? [confirm] y
```

次に、Kerberos キータブファイルを表示した後にクリアする例を示します。

```
ciscoasa# show aaa kerberos keytab

Principal:   host/asa2@BXB-WIN2016.EXAMPLE.COM
Key version: 10
Key type:    arcfour (23)
ciscoasa# clear aaa kerberos keytab
```

```
ciscoasa# show aaa kerberos keytab

No keys found
ciscoasa#
```

関連コマンド

コマンド	説明
show aaa kerberos	システム上のキャッシュされたすべてのKerberosチケット、またはキータブファイルを表示します。

clear aaa local user

ユーザーをロック解除したり、ユーザーの失敗した認証試行回数をゼロにリセットしたりするには、特権 EXEC モードで **clear aaa local user** コマンドを使用します。

clear aaa local user { **fail-attempts** | **lockout** } { **username** *name* | **all** }

構文の説明

all	ロックアウトされたすべてのユーザーをロック解除するか、すべてのユーザーについて、失敗試行カウンタを 0 にリセットします。
failed-attempts	指定したユーザーまたはすべてのユーザーについて、失敗試行カウンタを 0 にリセットします。
lockout	現在ロックアウトされているユーザーをロック解除し、ユーザーの失敗試行カウンタを 0 にリセットします。このオプションは、ロックアウトされていないユーザーには影響を与えません。 管理者をデバイスからロックアウトすることはできません。
username *name*	ロック解除するか、失敗試行カウンタを 0 にリセットする特定のユーザー名を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、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

ユーザーが認証試行を何回か失敗した後に、ユーザー認証を失敗にするには、このコマンドを使用します。

設定された認証試行の失敗数に達すると、ユーザーは、システムからロックアウトされ、システム管理者がこのユーザー名のロックを解除するか、またはシステムをリブートするまで、正常にログインできません。ユーザーが正常に認証されるか、またはシステムをリブートする

と、失敗試行数が 0 にリセットされ、ロックアウト ステータスが No にリセットされます。また、コンフィギュレーションが変更されると、システムがカウンタを 0 にリセットします。

ユーザー名のロックまたはアンロックにより、システム ログ メッセージが生成されます。特権レベル 15 のシステム管理者は、ロック アウトされません。

例

次に、ユーザー名 anyuser の失敗試行カウンタを 0 にリセットする例を示します。

```
ciscoasa# clear aaa local user fail-attempts
            username anyuser
ciscoasa#
```

次に、すべてのユーザーの失敗試行カウンタを 0 にリセットする例を示します。

```
ciscoasa# clear aaa local user fail-attempts
            all
ciscoasa#
```

次に、ユーザー名 anyuser のロックアウト状態をクリアし、失敗試行カウンタを 0 にリセットする例を示します。

```
ciscoasa# clear aaa local user lockout username anyuser
ciscoasa#
```

関連コマンド

コマンド	説明
aaa local authentication attempts max-fail	許可される失敗ユーザー認証試行の回数制限を設定します。
show aaa local user	試行失敗カウンタおよびロックアウト ステータスを持つユーザー名のリストを表示します。

clear aaa sdi node-secret

RSA SecurID サーバーのノードシークレットファイルを削除するには、特権 EXEC モードで **clear aaa sdi node-secret** コマンドを使用します。

clear aaa sdi node-secret *rsa_server_address*

構文の説明

rsa_server_address	ノードシークレットファイルを削除する RSA SecurID/Authentication Manager サーバーの IP アドレスまたは完全修飾ホスト名。

コマンド デフォルト

デフォルト設定はありません。

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
9.15(1)	このコマンドが追加されました。

例

次に、ノードシークレットファイルのリストを表示し、その 1 つを削除する例を示します。必要に応じて、aaa sdi import-node-secret コマンドを使用して、サーバーの新しいノードシークレットファイルをインポートしてください。

```
ciscoasa# show aaa sdi node-secrets

Last update                  SecurID server
---------------------        --------------------
15:16:13 Jun 24 2020         rsaam.example.com
15:20:07 Jun 24 2020         10.11.12.13
ciscoasa# clear aaa sdi node-secret rsaam.example.com
```

関連コマンド

コマンド	説明
aaa sdi import-node-secret	RSA SecurID Authentication Manager ノードシークレットファイルをインポートします。
show aaa sdi node-secrets	すべての SecurID ノードシークレットファイルを表示します。

clear aaa-server statistics

AAA サーバーの統計情報をリセットするには、特権 EXEC モードで **clear aaa-server statistics** コマンドを使用します。

clear aaa-server statistics [**LOCAL** | *groupname* [**host** *hostname*] | **protocol** *protocol*]

構文の説明

groupname	（任意）グループ内のサーバーの統計情報をクリアします。
host *hostname*	（任意）グループ内の特定のサーバーの統計情報をクリアします。
LOCAL	（任意）LOCAL ユーザー データベースの統計情報をクリアします。
protocol *protocol*	（任意）指定するプロトコルのサーバーの統計情報をクリアします。 • **kerberos** • **ldap** • **nt** • **radius** • **sdi** • **tacacs+**

コマンド デフォルト

すべてのグループのすべての AAA サーバーの統計情報を削除します。

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(1)	CLI ガイドラインに沿うように、このコマンドが変更されました。プロトコルの値において、以前の **nt-domain** から **nt** に、以前の **rsa-ace** から **sdi** に置き換えられました。

例

次に、グループ内の特定のサーバーの AAA 統計情報をリセットする例を示します。

```
ciscoasa
(config)#

clear aaa-server statistics svrgrp1 host 1.2.3.4
```

次に、サーバー グループ全体の AAA 統計情報をリセットする例を示します。

```
ciscoasa
(config)#

clear aaa-server statistics svrgrp1
```

次に、すべてのサーバー グループの AAA 統計情報をリセットする例を示します。

```
ciscoasa
(config)#
clear aaa-server statistics
```

次に、特定のプロトコル（この場合は TACACS+）の AAA 統計情報をリセットする例を示します。

```
ciscoasa
(config)#
clear aaa-server statistics protocol tacacs+
```

関連コマンド

コマンド	説明
aaa-server protocol	AAA サーバー接続データのグループ化の指定および管理を行います。
clear configure aaa-server	デフォルト以外のすべての AAA サーバー グループを削除するか、または指定したグループをクリアします。
show aaa-server	AAA サーバーの統計情報を表示します。
show running-config aaa-server	現在の AAA サーバー コンフィギュレーションの値を表示します。

clear access-list

アクセスリスト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 access-list** コマンドを使用します。

clear access-list *ID* **counters**

構文の説明

counters	アクセス リストのカウンタをクリアします。
id	アクセス リストの名前または番号。

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	• 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 access-list コマンドを入力する際には、カウンタをクリアするアクセスリストの *id* を指定する必要があります。

例

次に、特定のアクセス リスト カウンタをクリアする例を示します。

```
ciscoasa# clear access-list inbound counters
```

関連コマンド

コマンド	説明
access-list extended	アクセス リストをコンフィギュレーションに追加し、ファイアウォールを通過する IP トラフィック用のポリシーを設定します。

コマンド	説明
access-list standard	OSPF ルートの宛先 IP アドレスを識別するアクセス リストを追加します。このアクセス リストは、OSPF 再配布のルート マップで使用できます。
clear configure access-list	実行コンフィギュレーションからアクセス リストをクリアします。
show access-list	アクセス リスト エントリを番号で表示します。
show running-config access-list	適応型セキュリティ アプライアンスで実行中のアクセス リスト コンフィギュレーションを表示します。

clear arp

ダイナミック ARP エントリまたは ARP 統計情報をクリアするには、特権 EXEC モードで **clear arp** コマンドを使用します。

clear arp [**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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、すべての ARP 統計情報をクリアする例を示します。

```
ciscoasa# clear arp statistics
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
arp-inspection	トランスペアレント ファイアウォール モードで、ARP パケットを調査し、ARP スプーフィングを防止します。
show arp statistics	ARP 統計情報を表示します。
show running-config arp	ARP タイムアウトの現在のコンフィギュレーションを表示します。

clear asp

高速セキュリティパス（ASP）の統計情報をクリアするには、 **clear asp** コマンドを使用します。

clear asp { **cluster counter** | **drop** [**flow** | **frame**] | **event dp-cp** | **queue-exhaustion** [**snapshot** *number*] | **load-balance history** | **overhead** | **table** [**arp** | **classify** | **filter** [**access-list** *acl_name*]] }

構文の説明

access-list *acl_name*	（任意）指定したアクセス リストのヒット カウンタだけをクリアします。
arp	（任意）ASP ARP テーブルのみでヒット カウンタをクリアします。
classify	（任意）ASP 分類テーブルのみでヒット カウンタをクリアします。
cluster counter	クラスタ カウンタをクリアします。
event	データ パスからコントロール プレーンへのイベントの統計情報をクリアします。
filter	（任意）ASP フィルタ テーブルのみでヒット カウンタをクリアします。
flow	（任意）ドロップされたフロー統計情報をクリアします。
frame	（任意）ドロップされたフレーム/パケット統計情報をクリアします。
load-balance history	パケット単位の ASP ロード バランシングの履歴をクリアし、自動切り替えが発生した回数をリセットします。
overhead	すべての ASP マルチプロセッサ オーバーヘッドの統計情報をクリアします。
queue-exhaustion	データ パス インスペクションの Snort キュー スナップショットをクリアします。
snapshot *number*	（任意）スナップショット ID 別にキューの枯渇をクリアします。
table	ASP ARP テーブルおよび ASP 分類テーブルのヒット カウンタをクリアします。

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。

リリース	変更内容
7.2(4)	**table**キーワードが追加されました。
8.2(2)	**filter** キーワードが追加されました。
9.3(1)	**load-balance history** キーワードが追加されました。

例

次に、すべての ASP テーブルの統計情報をクリアする例を示します。

```
ciscoasa# clear asp table
Warning: hits counters in asp arp and classify tables are cleared, which might impact
the hits statistic of other modules and output of other "show" commands! ciscoasa#clear
 asp table arp
Warning: hits counters in asp arp table are cleared, which might impact the hits statistic
 of other modules and output of other "show" commands! ciscoasa#clear asp table classify

Warning: hits counters in classify tables are cleared, which might impact the hits
statistic of other modules and output of other "show" commands! ciscoasa(config)# clear
 asp table
Warning: hits counters in asp tables are cleared, which might impact the hits statistics
 of other modules and output of other "show" commands! ciscoasa# sh asp table arp
Context: single_vf, Interface: inside 10.1.1.11 Active 00e0.8146.5212 hits 0
Context: single_vf, Interface: identity :: Active 0000.0000.0000 hits 0 0.0.0.0 Active
0000.0000.0000 hits 0
```

関連コマンド

コマンド	説明
asp load-balance per-packet	ロード バランシング動作を変更します。
show asp load-balance	ロード バランサのキュー サイズのヒストグラムを表示します。
show asp load-balance per-packet	現在のステータス、最高水準点と最低水準点、およびグローバルなしきい値を表示します。
show asp load-balance per-packet history	現在のステータス、最高水準点と最低水準点、グローバルなしきい値、最後のリセット以降のパケットごとの ASP ロードバランシングのオンとオフの切り替え回数、タイムスタンプ付きのパケットごとの ASP ロードバランシングの履歴、およびオンとオフを切り替えた理由を表示します。
show asp	ASP 統計情報を表示します。

clear bfd counters

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

clear bfd counters [**ld** *local_discr* | *interface_name* | **ipv4** *ip-address* | **ipv6** *ipv6-address*]

構文の説明

ld *local_discr*	（任意）指定したローカル識別子の BFD カウンタをクリアします（1 - 4294967295）。
interface_name	（任意）指定したインターフェイスの BFD カウンタをクリアします。
ipv4 *ip_address*	（任意）指定したネイバー IP アドレスの BFD カウンタをクリアします。
ipv6 *ip_address*	（任意）指定したネイバー IPv6 アドレスの BFD カウンタをクリアします。

コマンド デフォルト

このコマンドは、すべての BFD カウンタをクリアします。

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	—

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。

例

次に、すべての BFD カウンタをクリアする例を示します。

```
ciscoasa# clear bfd counters
```

関連コマンド

コマンド	説明
authentication	シングルホップ セッションとマルチホップ セッションの BFD テンプレートに認証を設定します。
bfd echo	インターフェイスで BFD エコー モードを有効にします。

コマンド	説明
bfd interval	インターフェイスにベースライン BFD パラメータを設定します。
bfd map	アドレスとマルチホップ テンプレートを関連付ける BFD マップを設定します。
bfd slow-timers	BFD スロー タイマー値を設定します。
bfd template	シングルホップ BFD テンプレートをインターフェイスにバインドします。
bfd-template single-hop | multi-hop	BFDテンプレートを設定し、BFDコンフィギュレーション モードを開始します。
echo	BFD シングルホップ テンプレートにエコーを設定します。
neighbor	BGP が登録され、BFD から転送パス検出失敗メッセージを受信できるように、BGP の BFD サポートを設定します。
show bfd drops	BFD でドロップされたパケットの数を表示します。
show bfd map	設定済みの BFD マップを表示します。
show bfd neighbors	既存の BFD 隣接関係の詳細なリストを表示します。
show bfd summary	BFD のサマリー情報を表示します。

clear bgp

ハードまたはソフト再構成を使用してボーダー ゲートウェイ プロトコル（BGP）接続をリセットするには、特権 EXEC モードで **clear bgp** コマンドを使用します。

clear bgp { [***** | **external**] [**ipv4 unicast** [*as_number* | *neighbor_address* | **table-map**] | **ipv6 unicast** [*as_number* | *neighbor_address*]] [**soft**] [**in** | **out**] | *as_number* [**soft**] [**in** | **out**] | *neighbor_address* [**soft**] [**in** | **out**] | **table-map** }

構文の説明

*。	現在のすべての BGP セッションをリセットすることを指定します。
as_number	（任意）すべての BGP ピア セッションがリセットされる自律システムの番号。
external	外部のすべての BGP セッションをリセットすることを指定します。
in	（オプション）インバウンド再構成を開始します。**in** と **out** のどちらのキーワードも指定しない場合は、インバウンドとアウトバウンドの両方のセッションがリセットされます。
ipv4 unicast	IPv4 アドレス ファミリ セッションのハードまたはソフト再構成を使用して BGP 接続をリセットします。
ipv6 unicast	IPv6 アドレス ファミリ セッションのハードまたはソフト再構成を使用して BGP 接続をリセットします。
neighbor_address	（任意）指定された BGP ネイバーのみをリセットすることを指定します。この引数の値には、IPv4 アドレスまたは IPv6 アドレスを指定できます。
out	（オプション）インバウンド再構成またはアウトバウンド再構成を開始します。**in** と **out** のどちらのキーワードも指定しない場合は、インバウンドとアウトバウンドの両方のセッションがリセットされます。
soft	（任意）低速ピアのステータスを強制的にクリアして、元のアップデート グループに移します。
table-map	BGP ルーティング テーブルの table-map 設定情報をクリアします。このコマンドを使用して、BGP ポリシー アカウンティング機能で設定されたトラフィック インデックス情報をクリアできます。

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
9.2(1)	このコマンドが導入されました。

使用上のガイドライン

clear bgp コマンドを使用して、ハードリセットまたはソフト再構成を開始できます。ハードリセットは、指定されたピアリング セッションを切断して再構築し、BGP ルーティング テーブルを再構築します。ソフト再構成は、保存されたプレフィックス情報を使用し、既存のピアリング セッションを切断せずに BGP ルーティング テーブルの再構成とアクティブ化を行います。ソフト再構成では、保存されているアップデート情報が使用されます。アップデートを保存するために追加のメモリが必要になりますが、ネットワークを中断せずに、新しい BGP ポリシーを適用することができます。ソフト再構成は、インバウンドセッション、またはアウトバウンド セッションに対して設定できます。

マルチコンテキストモードでは、 **clear bgp *** コマンドだけがシステム実行スペースで使用可能です。

例

次の例では、システム実行スペースで **clear bgp** コマンドが指定されたときに、すべてのコンテキストですべてのBGPセッションがリセットされます。このコマンドはすべてのBGPセッションをリセットするため、アクションを確認する警告が表示されます。

```
ciscoasa# clear bgp *
This command will reset BGP in ALL contexts.
Are you sure you want to continue? [no]:
```

次の例では、すべての BGP セッションが、シングル モードまたはマルチ コンテキスト モードのコンテキストでリセットされます。

```
ciscoasa# clear bgp *
```

次の例では、ネイバー 10.100.0.1 とのインバウンド セッションに対してソフト再構成が開始され、アウトバウンド セッションは影響を受けません。

```
ciscoasa# clear bgp 10.100.0.1 soft in
```

次の例では、ルート リフレッシュ機能が BGP ネイバー ルータでイネーブルになっており、ネイバー172.16.10.2 とのインバウンドセッションに対してソフト再構成が開始され、アウトバウンド セッションは影響を受けません。

```
ciscoasa# clear bgp 172.16.10.2 in
```

次の例では、自律システム番号 35700 のすべてのルータとのセッションに対してハード リセットが開始されます。

```
ciscoasa# clear bgp 35700
```

次の例では、すべてのインバウンド eBGP ピアリング セッションに対してソフト再構成が設定されます。

```
ciscoasa# clear bgp external soft in
```

次の例では、すべてのアウトバウンド アドレス ファミリ IPv4 マルチキャスト eBGP ピアリング セッションがクリアされます。

```
ciscoasa# clear bgp external ipv4 multicast out
```

次の例では、自律システム 65400 の IPv4 ユニキャスト アドレス ファミリ セッションで BGP ネイバーのインバウンド セッションに対してソフト再構成が開始され、アウトバウンド セッションは影響を受けません。

```
ciscoasa# clear bgp ipv4 unicast 65400 soft in
```

次の例では、asplain 表記の 4 バイトの自律システム番号 65538 の IPv4 ユニキャスト アドレス ファミリ セッションで BGP ネイバーに対してハード リセットが開始されます。

```
ciscoasa# clear bgp ipv4 unicast 65538
```

次の例では、asdot 表記の 4 バイトの自律システム番号 1.2 の IPv4 ユニキャスト アドレス ファミリ セッションで BGP ネイバーに対してハード リセットが開始されます。

```
ciscoasa# clear bgp ipv4 unicast 1.2
```

次の例は、IPv4 ユニキャスト ピアリング セッションのテーブル マップをクリアします。

```
ciscoasa# clear bgp ipv4 unicast table-map
```

clear blocks

枯渇状態や履歴情報などのパケット バッファ カウンタをリセットするには、特権 EXEC モードで **clear blocks** コマンドを使用します。

clear blocks [**exhaustion** { **history** | **snapshot** } | **export-failed** | **queue** [**history** [**core-local** [*number*]]]]

構文の説明

core-local [*number*]	（任意）すべてのコア、またはコア番号を指定する場合は特定のコアに対し、アプリケーションによってキューに入れられたシステムバッファをクリアします。
exhaustion	（任意）枯渇状態をクリアします。
export-failed	（任意）エクスポート失敗カウンタをクリアします。
history	（任意）履歴をクリアします。
queue	（任意）キューに入れられたブロックをクリアします。
snapshot	（任意）スナップショット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。
9.1(5)	**history** および **snapshot** オプションが追加されました。

使用上のガイドライン

最低水準点カウンタを各プール内で現在使用可能なブロックにリセットします。また、このコマンドは、前回のバッファ割り当ての失敗時に保存された履歴情報をクリアします。

例

次に、ブロックをクリアする例を示します。

```
ciscoasa# clear blocks
```

関連コマンド

コマンド	説明
blocks	ブロック診断に割り当てるメモリを増やします。
show blocks	システム バッファの使用状況を表示します。

clear-button

WebVPN ユーザーが ASA に接続したときに表示される WebVPN ページログインフィールドの [クリア（Clear）] ボタンをカスタマイズするには、カスタマイゼーション コンフィギュレーション モードで **clear-button** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

clear-button { **text** | **style** } *value*
no clear-button [{ **text** | **style** }] *value*

構文の説明

style	スタイルを変更することを指定します。
text	テキストを変更することを指定します。
value	実際に表示するテキストまたは Cascading Style Sheet（CSS）パラメータ（それぞれ許容最大文字数は 256 です）。

コマンド デフォルト

デフォルトのテキストは「Clear」です。

デフォルトのスタイルは、border:1px solid black;background-color:white;font-weight:bold;font-size:80% です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

style オプションは有効なカスケーディング スタイル シート（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web コンソーシアム（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPNページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注） WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次に、[Clear] ボタンのデフォルトの背景色を黒から青に変更する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# clear-button style background-color:blue
```

関連コマンド

コマンド	説明
group-prompt	WebVPN ページの Login フィールドのグループ プロンプトをカスタマイズします。
login-button	WebVPN ページの Login フィールドのログイン ボタンをカスタマイズします。
login-title	WebVPN ページの Login フィールドのタイトルをカスタマイズします。
password-prompt	WebVPN ページの Login フィールドのパスワード プロンプトをカスタマイズします。
username-prompt	WebVPN ページの Login フィールドのユーザー名プロンプトをカスタマイズします。

clear capture

キャプチャバッファをクリアするには、特権 EXEC コンフィギュレーション モードで **clear capture** コマンドを使用します。

clear capture { **/all** | *capture_name* }

構文の説明

/all	すべてのインターフェイス上のパケットをクリアします。
capture_name	パケット キャプチャの名前を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、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	•	•	•	•	•

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

誤ってすべてのパケットキャプチャを破棄することを防止するために、**clear capture** の短縮形（たとえば、 **cl cap** や **clear cap**）は、サポートされていません。

例

次に、キャプチャ バッファ「example」のキャプチャ バッファをクリアする例を示します。

```
ciscoasa
(config)#
clear capture example
```

関連コマンド

コマンド	説明
capture	パケット スニッフィングおよびネットワーク障害の切り分けのためにパケット キャプチャ機能をイネーブルにします。
show capture	オプションが指定されていない場合は、キャプチャ コンフィギュレーションを表示します。

clear clns cache

Connectionless Network Service（CLNS）ルーティング キャッシュをクリアして再初期化するには、clear clns cache EXEC コマンドを使用します。

clear clns 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。

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

EXEC

使用上のガイドライン

ルーティングキャッシュ情報をクリアするには、**clear clns cache** コマンドを使用します。

例

次に、CLNS ルーティング キャッシュをクリアする例を示します。

```
ciscoasa# clear clns cache
```

関連コマンド

コマンド	説明
show clns cache	clns ルーティング キャッシュを表示します。

clear clns is-neighbors

隣接データベースから IS ネイバー情報を削除するには、clear clns is-neighbors EXEC コマンドを使用します。

clear clns is-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。

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

EXEC

使用上のガイドライン

隣接データベースから IS ネイバー情報をクリアするには、**clear clns is-neighbors** コマンドを使用します。

例

次に、CLNS es-neighbor をクリアする例を示します。

```
ciscoasa# clear clns is-neighbors
```

関連コマンド

コマンド	説明
clear clns neighbors	clns ネイバー情報を削除します。
show clns is-neighbors	clns がネイバー情報であることを示します。

clear clns neighbors

隣接データベースから CLNS ネイバー情報を削除するには、clear clns neighbors EXEC コマンドを使用します。

clear clns 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。

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

EXEC

使用上のガイドライン

隣接データベースからネイバー情報をクリアするには、**clear clns neighbors** コマンドを使用します。

例

次に、隣接データベースから CLNS ネイバー情報を削除する例を示します。

```
ciscoasa# clear clns neighbors
```

関連コマンド

コマンド	説明
clear clns is-neighbors	clns is-neighbor 情報を削除します。
show clns neighbors	clns ネイバー情報を表示します。

clear clns route

動的に導出されたすべての CLNS ルーティング情報を削除するには、clear clns route EXEC コマンドを使用します。

clear clns route

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

EXEC

使用上のガイドライン

ルーティング情報をクリアするには、**clear clns is-neighbors** コマンドを使用します。

例

次に、動的に導出されたすべての CLNS ルーティング情報を削除する例を示します。

```
ciscoasa# clear clns route
```

関連コマンド

コマンド	説明
show clns route	clns ルート情報を表示します。

clear cluster info

クラスタ統計情報をクリアするには、特権 EXEC モードで **clear cluster info** コマンドを使用します。

clear cluster info { **flow-mobility counters** | **health details** | **trace** | **transport** }

構文の説明

flow-mobility counters	クラスタ フローモビリティ カウンタをクリアします。
health details	クラスタ ヘルス情報をクリアします。
trace	クラスタ イベント トレース情報をクリアします。
transport	クラスタ転送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	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.5(2)	**flow-mobility counters** キーワードが導入されました。
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

クラスタの統計情報をクリアするには、**show cluster info** コマンドを使用します。

例

次に、クラスタ イベント トレース情報をクリアする例を示します。

```
ciscoasa# clear cluster info trace
```

関連コマンド

コマンド	説明
show cluster info	クラスタ統計情報を表示します。

clear compression

すべての SVC および WebVPN の接続の圧縮統計情報をクリアするには、特権 EXEC モードで **clear compression** コマンドを使用します。

clear compression { **all** | **anyconnect-ssl** | **http-comp** }

構文の説明

all	すべての圧縮統計情報をクリアします。
http-comp	HTTP-COMP 統計情報をクリアします。
anyconnect-ssl	AnyConnect SSL 圧縮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	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。
8.4(1)	SVC は AnyConnect SSL に置き換えられました。
9.5(2)	マルチ コンテキスト モードのサポートが追加されました。
9.0(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、ユーザーの圧縮コンフィギュレーションをクリアする例を示します。

```
hostname# clear configure compression
```

関連コマンド

コマンド	説明
圧縮	すべての SVC 接続および WebVPN 接続の圧縮をイネーブルにします。

コマンド	説明
svc compression	特定のグループまたはユーザーに対して、SVC 接続経由でのデータの圧縮をイネーブルにします。

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。

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
グローバル設定	• 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 およびそのオブジェクトの編集用に独立し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 ヘルプを確認します。
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。

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
グローバル設定	• 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 **conn** コマンドを使用します。

clear conn [**all**] [**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

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）指定したユーザー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ーの接続をクリアします。
user-group [*domain_nickname* \\ ] *user_group_name*	（オプション）指定したユーザー 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ー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。
data-rate	（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に、 **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。
9.14(1)	**data-rate** 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することもできます。

セカンダリ接続を許可するためのピンホールを ASA が作成している場合は、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
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表示するには、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。

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
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。

コマンド 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
グローバル設定	• 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
coredump enable	コアダンプ機能をイネーブルにします。

コマンド	説明
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。

コマンド デフォルト

clear counters summary detail コマンドはデフォルトです。

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
グローバル設定	• 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
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。

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
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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
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	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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

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
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）ユーザー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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
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

ユーザーは、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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(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 ipsec stats

グローバル IPsec 統計情報を削除し、統計情報をリセットするには、特権 EXEC モードで **clear crypto ipsec stats** コマンドを使用します。

clear crypto ipsec stats

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.16(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

すべてのグローバル IPsec 統計情報をクリアするには、このコマンドを引数なしで使用します。

例

次に、ASA の IPsec 統計情報を削除してリセットする例を示します。

```
ciscoasa# clear crypto ipsec stats
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。
show ipsec stats	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、ダイナミックスクリプトマップ、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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(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。

コマンド	説明
show isakmp	ISAKMP 運用データに関する情報を表示します。
show running-config crypto	IPsec、クリプトマップ、ダイナミック クリプトマップ、ISAKMP など、暗号コンフィギュレーション全体を表示します。

clear 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 セキュリティ（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

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

構文の説明

noconfirm	確認を求めずにデータをクリアします。
environment-data	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。
pac	NVRAM に保存されている CTS PAC 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
グローバル設定	• 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、次回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す。

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ります。

クラスタでは、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
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。
show cts	Cisco TrustSec （CTS）情報を表示します。

clear dhcpd

DHCP サーバー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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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表示されます。

すべての DHCP サーバー 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 サーバー設定を削除します。
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

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 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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(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

完全修飾ドメイン名（FQDN）ホストに関連付けられた 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* ｜ **ip-cache** ［ **counters** ］］

構文の説明

host *fqdn_name*	（オプション）アドレスをクリアするホストの完全修飾ドメイン名を指定します。
ip-cache ［**counters**］	ネットワークサービス オブジェクトのドメイン名解決を保持する IP キャッシュをクリアします。削除後は、クライアントの DNS 解決要求が解決およびスヌーピングされてキャッシュが再構築されるまで、ネットワークサービス オブジェクトのドメインは照合されません。 ドメインのヒットカウントのリセットのみを行い、IP キャッシュはそのまま残す場合は、**counters** キーワードを含めます。

コマンド デフォルト

パラメータを指定しない場合、アクセスコントロールルールで使用されるホストのすべての DNS 解決がクリアされます。ネットワークサービス オブジェクトで使用されるドメイン名の場合、カウンタはクリアされますが、IP キャッシュは削除されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
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。
9.17(1)	**ip-cache** キーワードが追加されました。

例

次に、FQDN ネットワークオブジェクトで使用される指定した 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 host www.example.com
```

（注） 解決をクリアする際、**dns expire-entry** キーワードの設定は無視されます。新しい DNS クエリは、FQDN ネットワークオブジェクトでの指定に従って、アクティブ化された各 FQDN ホストに送信されます。

次に、ネットワークサービス オブジェクトで使用されるドメインのヒットカウントをクリアする例を示します。

```
ciscoasa# clear dns ip-cache counters
```

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 サーバー アドレスを設定します。
show dns ip-cache	ネットワークサービス オブジェクトに使用される DNS 解決 IP キャッシュを表示します。
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。

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
グローバル設定	• 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
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 サーバー 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 サーバーのリストを再試行する回数を指定します。
dns timeout	次の DNS サーバー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。

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
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。

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 サーバーに DNS 要求を送信できるようにします。
dns server-group	ASA の DNS サーバーを指定します。
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。

コマンド	説明
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 フィルタでモニターされた接続の数、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	サーバーの IP アドレス、ASA が次にサーバーに接続する日時、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ー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。

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)	**botnet-sites** および **botnet-ports** キーワードが **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** なしで）。

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 サーバーに DNS 要求を送信できるようにします。
dns server-group	ASA の DNS サーバーを指定します。
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。

コマンド	説明
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 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 フィルタでモニターされた接続の数、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	サーバーの IP アドレス、ASA が次にサーバーに接続する日時、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ーに関する情報を表示します。

コマンド	説明
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。

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
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。

コマンド	説明
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。
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 サーバーに DNS 要求を送信できるようにします。
dns server-group	ASA の DNS サーバーを指定します。
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。

コマンド	説明
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 フィルタでモニターされた接続の数、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	サーバーの IP アドレス、ASA が次にサーバーに接続する日時、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ー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 イベントログを表示するには、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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
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。

コマンド 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
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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
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。

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
alarm contact description	アラーム入力の説明を指定します。
alarm contact severity	アラームのシビラティ（重大度）を指定します。

コマンド	説明
alarm contact trigger	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。
alarm facility input-alarm	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。
alarm facility power-supply rps	電源アラームを設定します。
alarm facility temperature	温度アラームを設定します。
alarm facility temperature (high and low thresholds)	温度しきい値の下限または上限を設定します。
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	アクティブ化された状態のリレーを表示します。
show facility-alarm status	トリガーされたすべてのアラームを表示するか、または指定されたシビラティ（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。

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
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 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。

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
8.1(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
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。

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
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。

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

clear flow-offload-ipsec

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

clear flow-offload-ipsec statistics

構文の説明

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

コマンド デフォルト

すべての統計がクリアされます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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
9.18(1)	このコマンドが導入されました。

例

次に、すべての IPsec フローオフロード統計をクリアする例を示します。

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

関連コマンド

コマンド	説明
flow-offload-ipsec	IPsec フローオフロードを設定します。
show flow-offload-ipsec	IPsec フローオフロード統計および情報を表示します。

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。

コマンド 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 データと動作データを分けるために、**clear fragment** および **clear configure fragment** の 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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

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。

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	—	—

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 [グループ | **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。

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	—	—

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。

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	—	—

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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
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。
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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
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* ［ **.** サブインターフェイス ］| *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）インターフェイス ID（**gigabitethernet0/1** など）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。
サブインターフェイス	（任意）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。

コマンド デフォルト

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

コマンド 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
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。

コマンド 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
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。

コマンド	説明
show running-config ip audit attack	**ip audit attack** コマンドの設定を表示します。

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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
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 ipsec stats

IPsec 統計情報をクリアし、統計情報をリセットするには、特権 EXEC モードで **clear ipsec stats** コマンドを使用します。

clear ipsec stats

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
9.16(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

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 stats** 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 統計情報をクリアする例を示します。

```
ciscoasa# clear ipsec stats
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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
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 サーバー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 サーバー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 サーバーを設定します。
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 サーバーから取得した 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 サーバーを使用して、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 サーバーを有効にします。
network	サーバー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。

コマンド	説明
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 マルチキャストリスナー検出（MLD）トラフィックカウンタをクリアするには、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

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(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。
トラフィック	トラフィック関連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	—

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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
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。

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
9.5(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 固有である点を除いて、**clear ip route** コマンドに似ています。

宛先ごとの最大伝送ユニット（MTU）キャッシュもクリアされます。

例

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

```
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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(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をリセットします。

例

次に、IPv6 トラフィック カウンタをリセットする例を示します。**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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(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。

コマンド	説明
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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(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。

コマンド	説明
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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
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。
clear isis	IS-IS データ構造をクリアします。
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。

コマンド	説明
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。
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。

コマンド	説明
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。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。