



# show ddns update interface コマンド ～ show ipv6 traffic コマンド

## show ddns update interface

セキュリティ アプライアンス インターフェイスに指定された DDNS 方式を表示するには、特権 EXEC モードで **show ddns update interface** コマンドを表示します。

```
show ddns update interface [interface-name]
```

### シンタックスの説明

*interface-name* (オプション) ネットワーク インターフェイスの名前。

### デフォルト

*interface-name* 文字列を省略すると、各インターフェイスに指定された DDNS 方式が表示されます。

### 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	透過	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
7.2(1)	このコマンドが導入されました。

### 例

次の例では、内部インターフェイスに指定された DDNS 方式を表示します。

```
hostname# show ddns update interface inside
Dynamic DNS Update on inside:
  Update Method Name      Update Destination
  ddns-2                  not available
hostname#
```

## 関連コマンド

コマンド	説明
<b>ddns</b> (DDNS アップデート方式モード)	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
<b>ddns update</b> (インターフェイス コンフィギュレーション モード)	セキュリティアプライアンス インターフェイスを、DDNS アップデート方式または DDNS アップデート ホスト名に関連付けます。
<b>ddns update method</b> (グローバル コンフィギュレーション モード)	DNS のリソース レコードを動的にアップデートするための方式を作成します。
<b>show ddns update method</b>	設定済みの各 DDNS 方式について、タイプおよび間隔を表示します。DDNS アップデートを実行する DHCP サーバ。
<b>show running-config ddns</b>	実行コンフィギュレーションに含まれている、設定済みのすべての DDNS 方式について、タイプおよび間隔を表示します。

# show ddns update method

実行コンフィギュレーションに含まれている DDNS アップデート方式を表示するには、特権 EXEC モードで **show ddns update method** コマンドを使用します。

```
show ddns update method [method-name]
```

## シンタックスの説明

*method-name* (オプション) 設定されている DDNS アップデート方式の名前です。

## デフォルト

*method-name* 文字列を省略すると、設定されたすべての DDNS アップデート方式が表示されます。

## 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	透過	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
7.2(1)	このコマンドが導入されました。

## 例

次の例では、ddns-2 という名前の DDNS 方式を表示します。

```
hostname(config)# show ddns update method ddns-2

Dynamic DNS Update Method: ddns-2
  IETF standardized Dynamic DNS 'A' and 'PTR' records update
  Maximum update interval: 0 days 0 hours 10 minutes 0 seconds
hostname(config)#
```

## 関連コマンド

コマンド	説明
<b>ddns</b> (DDNS アップデート方式モード)	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
<b>ddns update</b> (インターフェイス コンフィギュレーションモード)	セキュリティ アプライアンス インターフェイスを、ダイナミック DDNS アップデート方式または DDNS アップデート ホスト名に関連付けます。
<b>ddns update method</b> (グローバル コンフィギュレーションモード)	DNS のリソース レコードを動的にアップデートするための方式を作成します。
<b>show ddns update interface</b>	設定済みの各 DDNS 方式に関連付けられているインターフェイスを表示します。
<b>show running-config ddns</b>	実行コンフィギュレーションに含まれている、設定済みのすべての DDNS 方式について、タイプおよび間隔を表示します。

# show debug

現在のデバッグ コンフィギュレーションを表示するには、**show debug** コマンドを使用します。

```
show debug [command [keywords]]
```

## シンタックスの説明

*command* (オプション) 現在のコンフィギュレーションを表示するデバッグ コマンドを指定します。*command* 以降のシンタックスは、各 *command* の関連 **debug** コマンドでサポートされているシンタックスと同じです。たとえば、**show debug aaa** 以降で有効となる *keywords* は、**debug aaa** コマンドで有効となるキーワードと同じです。つまり、**show debug aaa** の場合は **accounting** キーワードをサポートしています。このキーワードを使用すると、AAA デバッグの当該部分のデバッグ コンフィギュレーションを表示することを指定できます。

## デフォルト

このコマンドにデフォルト設定はありません。

## 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	透過	シングル	マルチ コンテキスト
特権 EXEC	•	•	•	•

## コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

## 使用上のガイドライン

有効となる *command* 値は、次のとおりです。*command* 以降で有効となるシンタックスについては、該当する **debug command** のエントリを参照してください。



(注)

それぞれの *command* 値を入力できるかどうかは、該当する **debug** コマンドをサポートしているコマンドモードによって異なります。

- aaa
- appfw
- arp
- asdm
- context
- crypto
- ctique
- ctm
- dhcpc
- dhcpcd

- **dheprelay**
- **disk**
- **dns**
- **email**
- **entity**
- **fixup**
- **fover**
- **fsm**
- **ftp**
- **generic**
- **gtp**
- **h323**
- **http**
- **http-map**
- **icmp**
- **igmp**
- **ils**
- **imagemgr**
- **ipsec-over-tcp**
- **ipv6**
- **iua-proxy**
- **kerberos**
- **ldap**
- **mfib**
- **mgcp**
- **mrrib**
- **ntdomain**
- **ntp**
- **ospf**
- **parser**
- **pim**
- **pix**
- **pptp**
- **radius**
- **rip**
- **rtsp**
- **sdi**
- **sequence**
- **sip**
- **skinny**
- **sntp**
- **sqlnet**
- **ssh**

- ssl
- sunrpc
- tacacs
- timestamps
- vpn-sessiondb
- webvpn
- xdmcp

**例**

次のコマンドでは、認証、アカウントिंग、およびフラッシュメモリについてデバッグをイネーブルにしています。**show debug** コマンドを 3 つの方法で使用して、すべてのデバッグ コンフィギュレーション、特定の機能のデバッグ コンフィギュレーション、および機能のサブセットのデバッグ コンフィギュレーションを表示する方法を示しています。

```
hostname# debug aaa authentication
debug aaa authentication enabled at level 1
hostname# debug aaa accounting
debug aaa accounting enabled at level 1
hostname# debug disk filesystem
debug disk filesystem enabled at level 1
hostname# show debug
debug aaa authentication enabled at level 1
debug aaa accounting enabled at level 1
debug disk filesystem enabled at level 1
hostname# show debug aaa
debug aaa authentication enabled at level 1
debug aaa authorization is disabled.
debug aaa accounting enabled at level 1
debug aaa internal is disabled.
debug aaa vpn is disabled.
hostname# show debug aaa accounting
debug aaa accounting enabled at level 1
hostname#
```

**関連コマンド**

コマンド	説明
debug	すべての debug コマンドを参照してください。

# show dhcpd

DHCP のバインディング、状態、および統計情報を表示するには、特権 EXEC モードまたはグローバル コンフィギュレーション モードで **show dhcpd** コマンドを使用します。

```
show dhcpd {binding [IP_address] | state | statistics}
```

## シンタックスの説明

<b>binding</b>	与えられたサーバの IP アドレスとそれに関連付けられているクライアント ハードウェア アドレスとリース期間に対するバインディング情報を表示します。
<b>IP_address</b>	指定した IP アドレスのバインディング情報を表示します。
<b>state</b>	DHCP サーバの状態を表示します。たとえば、現在のコンテキストでイネーブルになっているかどうか、各インターフェイスでイネーブルになっているかどうかなどです。
<b>statistics</b>	アドレス プール、バインディング、有効期限切れのバインディング、形式が誤っているメッセージ、送信済みメッセージ、および受信済みメッセージの数などの統計情報を表示します。

## 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	透過	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
既存	このコマンドは既存のものです。

## 使用上のガイドライン

**show dhcpd binding** コマンドにオプションの IP アドレスを含めると、その IP アドレスのバインディングのみが表示されます。

**show dhcpd binding | state | statistics** コマンドは、グローバル コンフィギュレーション モードでも使用できます。

## 例

次に、**show dhcpd binding** コマンドの出力例を示します。

```
hostname# show dhcpd binding
IP Address Hardware Address Lease Expiration Type
10.0.1.100 0100.a0c9.868e.43 84985 seconds automatic
```

次に、**show dhcpd state** コマンドの出力例を示します。

```
hostname# show dhcpd state
Context Not Configured for DHCP
Interface outside, Not Configured for DHCP
Interface inside, Not Configured for DHCP
```

次に、**show dhcpd statistics** コマンドの出力例を示します。

```
hostname# show dhcpd statistics
```

```
DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0
```

```
Address pools      1
Automatic bindings 1
Expired bindings   1
Malformed messages 0
```

```
Message           Received
BOOTREQUEST       0
DHCPDISCOVER      1
DHCPREQUEST       2
DHCPDECLINE       0
DHCPRELEASE       0
DHCPINFORM        0
```

```
Message           Sent
BOOTREPLY         0
DHCPOFFER         1
DHCPACK           1
DHCPNAK           1
```

## 関連コマンド

コマンド	説明
<b>clear configure dhcpd</b>	DHCP サーバの設定をすべて削除します。
<b>clear dhcpd</b>	DHCP サーバのバインディングおよび統計情報カウンタを消去します。
<b>dhcpd lease</b>	クライアントに与える DHCP 情報のリース期間を定義します。
<b>show running-config dhcpd</b>	現在の DHCP サーバ コンフィギュレーションを表示します。



# show dhcprelay state

DHCP リレー エージェントの状態を表示するには、特権 EXEC モードまたはグローバル コンフィギュレーション モードで **show dhcprelay state** コマンドを使用します。

**show dhcprelay state**

**シンタックスの説明** このコマンドには、引数もキーワードもありません。

**デフォルト** デフォルトの動作や値はありません。

**コマンド モード** 次の表は、このコマンドを入力できるモードを示しています。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	透過	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
	既存	このコマンドは既存のものです。

**使用上のガイドライン** このコマンドは、現在のコンテキストおよび各インターフェイスの DHCP リレー エージェントの状態情報を表示します。

**例** 次に、**show dhcprelay state** コマンドの出力例を示します。

```
hostname# show dhcprelay state

Context    Configured as DHCP Relay
Interface  outside, Not Configured for DHCP
Interface  infrastructure, Configured for DHCP RELAY SERVER
Interface  inside, Configured for DHCP RELAY
```

関連コマンド	コマンド	説明
	<b>show dhcpd</b>	DHCP サーバの統計情報と状態情報を表示します。
	<b>show dhcprelay statistics</b>	DHCP リレーの統計情報を表示します。
	<b>show running-config dhcprelay</b>	現在の DHCP リレー エージェント コンフィギュレーションを表示します。

## show dhcprelay statistics

DHCP リレーの統計情報を表示するには、特権 EXEC モードで **show dhcprelay statistics** コマンドを使用します。

### show dhcprelay statistics

**シンタックスの説明** このコマンドには、引数もキーワードもありません。

**デフォルト** デフォルトの動作や値はありません。

**コマンドモード** 次の表は、このコマンドを入力できるモードを示しています。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	透過	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
既存	このコマンドは既存のものです。

**使用上のガイドライン** **show dhcprelay statistics** コマンドの出力は、**clear dhcprelay statistics** コマンドを入力するまでは増分します。

**例** 次に、**show dhcprelay statistics** コマンドの出力例を示します。

```
hostname# show dhcprelay statistics

DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0

Packets Relayed
BOOTREQUEST          0
DHCPDISCOVER         7
DHCPREQUEST          3
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

BOOTREPLY            0
DHCPOFFER            7
DHCPACK              3
DHCPNAK              0
FeralPix(config)#
```

## 関連コマンド

コマンド	説明
<code>clear configure dhcprelay</code>	DHCP リレー エージェントの設定をすべて削除します。
<code>clear dhcprelay statistics</code>	DHCP リレー エージェント統計情報カウンタを消去します。
<code>debug dhcprelay</code>	DHCP リレー エージェントに関するデバッグ情報を表示します。
<code>show dhcprelay state</code>	DHCP リレー エージェントの状態を表示します。
<code>show running-config dhcprelay</code>	現在の DHCP リレー エージェント コンフィギュレーションを表示します。

## show disk

フラッシュ メモリの内容を表示するには、特権 EXEC モードで **show disk** コマンドを使用します。PIX セキュリティ アプライアンスのフラッシュ メモリを表示するには、**show flash** コマンドを参照してください。

```
show disk[0 | 1] [fileys | all]
```

## シンタックスの説明

<b>0   1</b>	内蔵フラッシュ メモリ (0。デフォルト) または外部フラッシュメモリ (1) を指定します。
<b>fileys</b>	コンパクトフラッシュ カードに関する情報を表示します。
<b>all</b>	フラッシュ メモリの内容に加えてファイル システム情報を表示します。

## デフォルト

デフォルトでは、内蔵フラッシュ メモリが表示されます。

## 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	透過	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	このコマンドが導入されました。

## 例

次に、**show disk** コマンドの出力例を示します。

```
hostname# show disk
-#- --length-- ----date/time----- path
 11 1301      Feb 21 2005 18:01:34 test.cfg
 12 1949      Feb 21 2005 20:13:36 test1.cfg
 13 2551      Jan 06 2005 10:07:36 test2.cfg
 14 609223    Jan 21 2005 07:14:18 test3.cfg
 15 1619      Jul 16 2004 16:06:48 test4.cfg
 16 3184      Aug 03 2004 07:07:00 old_running.cfg
 17 4787      Mar 04 2005 12:32:18 test5.cfg
 20 1792      Jan 21 2005 07:29:24 test6.cfg
 21 7765184   Mar 07 2005 19:38:30 test7.cfg
 22 1674      Nov 11 2004 02:47:52 test8.cfg
 23 1863      Jan 21 2005 07:29:18 test9.cfg
 24 1197      Jan 19 2005 08:17:48 test10.cfg
 25 608554    Jan 13 2005 06:20:54 backupconfig.cfg
 26 5124096   Feb 20 2005 08:49:28 cdisk1
 27 5124096   Mar 01 2005 17:59:56 cdisk2
 28 2074      Jan 13 2005 08:13:26 test11.cfg
 29 5124096   Mar 07 2005 19:56:58 cdisk3
 30 1276      Jan 28 2005 08:31:58 lead
 31 7756788   Feb 24 2005 12:59:46 asdmfile.dbg
 32 7579792   Mar 08 2005 11:06:56 asdmfile1.dbg
 33 7764344   Mar 04 2005 12:17:46 asdmfile2.dbg
 34 5124096   Feb 24 2005 11:50:50 cdisk4
 35 15322     Mar 04 2005 12:30:24 hs_err.log

10170368 bytes available (52711424 bytes used)
```

次に、**show disk fileys** コマンドの出力例を示します。

```
hostname# show disk fileys
***** Flash Card Geometry/Format Info *****

COMPACT FLASH CARD GEOMETRY
  Number of Heads:          4
  Number of Cylinders       978
  Sectors per Cylinder     32
  Sector Size               512
  Total Sectors             125184

COMPACT FLASH CARD FORMAT
  Number of FAT Sectors     61
  Sectors Per Cluster       8
  Number of Clusters        15352
  Number of Data Sectors    122976
  Base Root Sector         123
  Base FAT Sector           1
  Base Data Sector          155
```

## 関連コマンド

コマンド	説明
<b>dir</b>	ディレクトリの内容を表示します。
<b>show flash</b>	内蔵フラッシュメモリの内容を表示します。

## show dns-hosts

DNS キャッシュを表示するには、特権 EXEC モードで **show dns-hosts** コマンドを使用します。DNS キャッシュには、DNS サーバから動的にラーニングしたエントリと共に、**name** コマンドを使用して手作業で入力した名前および IP アドレスが保持されています。

### show dns-hosts

**シンタックスの説明** このコマンドには、引数もキーワードもありません。

**デフォルト** デフォルトの動作や値はありません。

**コマンドモード** 次の表は、このコマンドを入力できるモードを示しています。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	透過	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)	このコマンドが導入されました。

**使用上のガイドライン** 表示される出力については、「例」の項を参照してください。

**例** 次に、**show dns-hosts** コマンドの出力例を示します。

```
hostname# show dns-hosts
Host                Flags      Age  Type  Address(es)
ns2.example.com    (temp, OK) 0    IP    10.102.255.44
ns1.example.com    (temp, OK) 0    IP    192.168.241.185
snowmass.example.com (temp, OK) 0    IP    10.94.146.101
server.example.com (temp, OK) 0    IP    10.94.146.80
```

表 26-1 に、各フィールドの説明を示します。

表 26-1 show dns-hosts のフィールド

フィールド	説明
Host	ホスト名を表示します。
Flags	次のフラグを組み合わせて、エントリのステータスを表示します。 <ul style="list-style-type: none"> <li>temp：このエントリは、DNS サーバから取得した一時的なものです。セキュリティ アプライアンスは、非アクティブ状態が 72 時間を過ぎるとこのエントリを削除します。</li> <li>perm：このエントリは、<b>name</b> コマンドで追加された永続的なものです。</li> <li>OK：このエントリは有効です。</li> <li>??：このエントリは問題のある可能性があり、再確認が必要です。</li> <li>EX：このエントリは、有効期限が切れています。</li> </ul>
Age	このエントリが最後に参照された時点からの経過時間を表示します。
Type	DNS レコードのタイプを表示します。この値は、常に IP です。
Address(es)	IP アドレス。

#### 関連コマンド

コマンド	説明
<b>clear dns-hosts</b>	DNS キャッシュを消去します。
<b>dns domain-lookup</b>	セキュリティ アプライアンスがネーム ルックアップを実行できるようにします。
<b>dns name-server</b>	DNS サーバのアドレスを設定します。
<b>dns retries</b>	セキュリティ アプライアンスが応答を受信しないときに、一連の DNS サーバへのアクセスを再試行する回数を指定します。
<b>dns timeout</b>	次の DNS サーバを試すまでに待つ時間を指定します。

# show failover

装置のフェールオーバー ステータスに関する情報を表示するには、特権 EXEC モードで **show failover** コマンドを使用します。

```
show failover [group num | history | interface | state | statistics]
```

## シンタックスの説明

<b>group</b>	指定したフェールオーバー グループの動作状態を表示します。
<b>history</b>	フェールオーバーの履歴を表示します。フェールオーバーの履歴には、過去のフェールオーバーの状態変化、および状態変化の理由が表示されます。デバイスがリブートされると、履歴情報は消去されます。
<b>interface</b>	フェールオーバー コマンドとステートフル リンクの情報を表示します。
<b>num</b>	フェールオーバー グループの番号。
<b>state</b>	両方のフェールオーバー装置のフェールオーバー状態を表示します。表示される情報には、装置のプライマリ状態またはセカンダリ状態、装置の Active/Standby ステータス、および最後に報告されたフェールオーバーの理由が含まれます。障害の原因が解決した場合でも、出力には障害理由が保持されます。
<b>statistics</b>	フェールオーバー コマンド インターフェイスの送信パケットと受信パケットの数を表示します。

## 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	透過	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)	このコマンドが変更されました。出力に含まれる情報を追加しています。

## 使用上のガイドライン

**show failover** コマンドは、ダイナミック フェールオーバーの情報、インターフェイスのステータス、およびステートフル フェールオーバーの統計情報を表示します。Stateful Failover Logical Update Statistics の出力は、ステートフル フェールオーバーがイネーブルになっている場合のみ表示されます。「xerr」値と「rerr」値は、フェールオーバーのエラーではなく、パケットの送信エラーまたは受信エラーの数を示します。



### (注)

ステートフル フェールオーバー (ステートフル フェールオーバー統計出力) は、ASA 5505 シリーズ適応型セキュリティ アプライアンスでは使用できません。

**show failover** コマンドの出力で、Stateful Failover フィールドに表示される値は次のとおりです。

- Stateful Obj には、次の値が表示されます。
  - xmit : 送信したパケット数を示します。
  - xerr : 送信エラーの数を示します。
  - rcv : 受信したパケット数を示します。
  - rerr : 受信エラーの数を示します。
- 各行は、次に示す特定オブジェクトのスタティック カウント用です。
  - General : ステートフル オブジェクト全部の合計を示します。
  - sys cmd : 論理アップデート システム コマンド、たとえば、**login** または **stay alive** を参照します。
  - up time : アクティブ セキュリティ アプライアンスがスタンバイ セキュリティ アプライアンスに渡すセキュリティ アプライアンス アップタイムの値を示します。
  - RPC services : リモート プロシージャ コール接続の情報。
  - TCP conn : ダイナミック TCP 接続の情報。
  - UDP conn : ダイナミック UDP 接続の情報。
  - ARP tbl : ダイナミック ARP テーブルの情報。
  - Xlate\_Timeout : 接続変換タイムアウトの情報を示します。
  - VPN IKE upd : IKE 接続の情報。
  - VPN IPSEC upd : IPSec 接続の情報。
  - VPN CTCP upd : cTCP トンネル接続の情報。
  - VPN SDI upd : SDI AAA 接続の情報。
  - VPN DHCP upd : トンネリングされた DHCP 接続の情報。

フェールオーバー IP アドレスを入力していなければ、**show failover** コマンドは IP アドレスに対して 0.0.0.0 を表示し、インターフェイスのモニタリングは、「waiting」状態のままになります。フェールオーバーが動作するためには、フェールオーバー IP アドレスを設定する必要があります。

マルチ コンフィギュレーション モードでは、セキュリティ コンテキストで使用できるのは **show failover** コマンドのみです。オプションのキーワードは入力できません。



例 次に、Active/Standby フェールオーバーでの **show failover** コマンドの出力例を示します。セキュリティ アプライアンスは ASA 5500 シリーズ適応型セキュリティ アプライアンスです。詳細に示されているように、各セキュリティ アプライアンスのロット 1 にはそれぞれ CSC SSM が搭載されています。

```
hostname# show failover

Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: fover Ethernet2 (up)
Unit Poll frequency 1 seconds, holdtime 3 seconds
Interface Poll frequency 15 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
failover replication http
Last Failover at: 22:44:03 UTC Dec 8 2004
  This host: Primary - Active
    Active time: 13434 (sec)
    slot 0: ASA5520 hw/sw rev (1.0/7.1(0)10) status (Up Sys)
      Interface inside (10.130.9.3): Normal
      Interface outside (10.132.9.3): Normal
    slot 1: ASA-SSM-20 hw/sw rev (1.0/CSC-SSM 5.0 (Build#1176)) status
  (Up/Up)
    Logging port IP: 10.0.0.3/24
    CSC-SSM, 5.0 (Build#1176)
  Other host: Secondary - Standby Ready
    Active time: 0 (sec)
    slot 0: ASA5520 hw/sw rev (1.0/7.1(0)10) status (Up Sys)
      Interface inside (10.130.9.4): Normal
      Interface outside (10.132.9.4): Normal
    slot 1: ASA-SSM-20 hw/sw rev (1.0/CSC-SSM 5.0 (Build#1176)) status
  (Up/Up)
    Logging port IP: 10.0.0.4/24
    CSC-SSM, 5.0 (Build#1176)

Stateful Failover Logical Update Statistics
Link : fover Ethernet2 (up)
Stateful Obj   xmit   xerr   rcv    rerr
General        0       0       0       0
sys cmd       1733    0     1733    0
up time        0       0       0       0
RPC services   0       0       0       0
TCP conn       6       0       0       0
UDP conn       0       0       0       0
ARP tbl       106     0       0       0
Xlate Timeout  0       0       0       0
VPN IKE upd    15      0       0       0
VPN IPSEC upd  90      0       0       0
VPN CTCP upd   0       0       0       0
VPN SDI upd    0       0       0       0
VPN DHCP upd   0       0       0       0

Logical Update Queue Information
          Cur   Max   Total
Recv Q:   0     2    1733
Xmit Q:   0     2   15225
```

次に、Active/Active フェールオーバーでの **show failover** コマンドの出力例を示します。

```
hostname# show failover

Failover On
Failover unit Primary
Failover LAN Interface: third GigabitEthernet0/2 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 4 seconds
Interface Policy 1
Monitored Interfaces 8 of 250 maximum
failover replication http
Group 1 last failover at: 13:40:18 UTC Dec 9 2004
Group 2 last failover at: 13:40:06 UTC Dec 9 2004

This host:      Primary
Group 1        State:          Active
               Active time:    2896 (sec)
Group 2        State:          Standby Ready
               Active time:    0 (sec)

slot 0: ASA-5530 hw/sw rev (1.0/7.0(0)79) status (Up Sys)
slot 1: SSM-IDS-20 hw/sw rev (1.0/5.0(0.11)S91(0.11)) status (Up)
admin Interface outside (10.132.8.5): Normal
admin Interface third (10.132.9.5): Normal
admin Interface inside (10.130.8.5): Normal
admin Interface fourth (10.130.9.5): Normal
ctx1 Interface outside (10.1.1.1): Normal
ctx1 Interface inside (10.2.2.1): Normal
ctx2 Interface outside (10.3.3.2): Normal
ctx2 Interface inside (10.4.4.2): Normal

Other host:    Secondary
Group 1        State:          Standby Ready
               Active time:    190 (sec)
Group 2        State:          Active
               Active time:    3322 (sec)

slot 0: ASA-5530 hw/sw rev (1.0/7.0(0)79) status (Up Sys)
slot 1: SSM-IDS-20 hw/sw rev (1.0/5.0(0.1)S91(0.1)) status (Up)
admin Interface outside (10.132.8.6): Normal
admin Interface third (10.132.9.6): Normal
admin Interface inside (10.130.8.6): Normal
admin Interface fourth (10.130.9.6): Normal
ctx1 Interface outside (10.1.1.2): Normal
ctx1 Interface inside (10.2.2.2): Normal
ctx2 Interface outside (10.3.3.1): Normal
ctx2 Interface inside (10.4.4.1): Normal

Stateful Failover Logical Update Statistics
Link : third GigabitEthernet0/2 (up)
Stateful Obj  xmit      xerr      rcv        rerr
General       0            0          0          0
sys cmd       380          0          380        0
up time       0            0          0          0
RPC services  0            0          0          0
TCP conn      1435         0          1450       0
UDP conn      0            0          0          0
ARP tbl       124          0          65         0
Xlate_Timeout 0            0          0          0
VPN IKE upd   15           0          0          0
VPN IPSEC upd 90           0          0          0
VPN CTCP upd  0            0          0          0
VPN SDI upd   0            0          0          0
VPN DHCP upd  0            0          0          0

Logical Update Queue Information
                Cur      Max      Total
Recv Q:         0        1      1895
Xmit Q:         0        0      1940
```

次に、ASA 5505 適応型セキュリティ アプライアンスでの **show failover** コマンドの出力例を示します。

```
Failover On
Failover unit Primary
Failover LAN Interface: fover Vlan150 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 4 of 250 maximum
Version: Ours 7.2(0)55, Mate 7.2(0)55
Last Failover at: 19:59:58 PST Apr 6 2006

    This host: Primary - Active
        Active time: 34 (sec)
        slot 0: ASA5505 hw/sw rev (1.0/7.2(0)55) status (Up Sys)
            Interface inside (192.168.1.1): Normal
            Interface outside (192.168.2.201): Normal
            Interface dmz (172.16.0.1): Normal
            Interface test (172.23.62.138): Normal
        slot 1: empty

    Other host: Secondary - Standby Ready
        Active time: 0 (sec)
        slot 0: ASA5505 hw/sw rev (1.0/7.2(0)55) status (Up Sys)
            Interface inside (192.168.1.2): Normal
            Interface outside (192.168.2.211): Normal
            Interface dmz (172.16.0.2): Normal
            Interface test (172.23.62.137): Normal
        slot 1: empty
```

次に、**show failover state** コマンドの出力例を示します。

```
hostname# show failover state

====My State====
Primary | Active |
====Other State====
Secondary | Standby |
====Configuration State====
    Sync Done
====Communication State====
    Mac set
=====Failed Reason=====
My Fail Reason:
Other Fail Reason:
    Service Card Failure
```

表 26-2 に **show failover state** コマンドの出力を示します。

**表 26-2 show failover state 出力の説明**

フィールド	説明
My State	装置の Primary/Secondary ステータスおよび Active/Standby ステータスを表示します。
Other State	ピア装置の Primary/Secondary ステータスおよび Active/Standby ステータスを表示します。

表 26-2 show failover state 出力の説明 (続き)

フィールド	説明
Configuration State	<p>コンフィギュレーションの同期化の状態を表示します。</p> <p>次に、スタンバイ装置について表示される可能性のあるコンフィギュレーション状態を示します。</p> <ul style="list-style-type: none"> <li>• <b>Config Syncing - STANDBY</b> : コンフィギュレーションの同期化の実行中に設定されます。</li> <li>• <b>Sync Done - STANDBY</b> : スタンバイ装置がアクティブ装置からのコンフィギュレーションの同期化を完了したときに設定されます。</li> </ul> <p>次に、アクティブ装置について表示される可能性のあるコンフィギュレーション状態を示します。</p> <ul style="list-style-type: none"> <li>• <b>Config Syncing</b> : アクティブ装置がスタンバイ装置へのコンフィギュレーションの同期化を実行中に、アクティブ装置に設定されます。</li> <li>• <b>Sync Done</b> : アクティブ装置がスタンバイ装置へのコンフィギュレーションの同期化を正常に終了したときに設定されます。</li> <li>• <b>Ready for Config Sync</b> : スタンバイ装置がコンフィギュレーションの同期化を受信する準備ができたという信号を送信したときに、アクティブ装置に設定されます。</li> </ul>
Communication State	<p>MAC アドレスの同期化の状態を表示します。</p> <ul style="list-style-type: none"> <li>• <b>Mac set</b> : MAC アドレスがピア装置からこの装置に同期されました。</li> <li>• <b>Updated Mac</b> : MAC アドレスが更新され、他の装置と同期する必要がある場合に使用されます。また、この装置がピア装置から同期されたローカル MAC アドレスを更新している移行期間中にも使用されます。</li> </ul>
Failed Reason	<p>最後に報告された障害の原因を表示します。障害状態が解決した場合でも、この情報は消去されません。この情報は、フェールオーバーが発生した場合にのみ変更されます。</p> <p>次に、障害を引き起こす可能性のある原因を示します。</p> <ul style="list-style-type: none"> <li>• <b>Ifc Failure</b> : 障害が発生したインターフェイスの数がフェールオーバー基準を満たした結果、フェールオーバーが発生した。</li> <li>• <b>Comm Failure</b> : フェールオーバー リンクに障害が発生したか、またはピアがダウンしている。</li> <li>• <b>Service card Failure</b> : SSM カードに障害が発生した (ASA のみ)。</li> </ul>

次に、**show failover history** コマンドの出力例を示します。

```
hostname# show failover history

=====
From State          To State          Reason
=====
Not Detected        Negotiation       No Error

Negotiation         Cold Standby      Detected an Active mate

Cold Standby        Sync Config       Detected an Active mate

Sync Config         Sync File System  Detected an Active mate

Sync File System    Bulk Sync         Detected an Active mate

Bulk Sync           Standby Ready     Detected an Active mate

Standby Ready       Just Active       Set by the CI config cmd

Just Active         Active Drain      Set by the CI config cmd

Active Drain        Active Applying Config Set by the CI config cmd

Active Applying Config Active Config Applied Set by the CI config cmd

Active Config Applied Active            Set by the CI config cmd

Active             Disabled          Set by the CI config cmd

=====
```

各エントリは、状態変化が発生した日時、最初の状態、最終の状態、および状態変化の原因を示します。最新のエントリは、下部に表示されます。古いエントリは上部に表示されます。最大 60 のエントリを表示できます。エントリが最大数に達すると、最も古いエントリが出力の上部から削除され、新しいエントリが下部に追加されます。

表 26-3 にフェールオーバーの状態を示します。状態には、安定状態と過渡状態の 2 種類があります。安定状態は、障害などによって状態変化が発生するまで装置が維持できる状態です。過渡状態は、装置が安定状態に到達する途上にある状態です。

表 26-3 フェールオーバーの状態

状態	説明
Initialization	この装置はプラットフォームの機能およびコンフィギュレーションをチェックし、フェールオーバー通信チャネルの準備をしています。これは過渡状態です。
Disabled	フェールオーバーはディセーブルになっています。これは安定状態です。
Negotiation	この装置はピアとの接続を確立し、ピアとネゴシエートしてソフトウェアバージョンの互換性および Active/Standby ロールを判断します。ネゴシエーションされているロールに応じて、この装置は Standby Unit States または Active Unit States に移行するか、または障害が発生した状態に入ります。これは過渡状態です。
Failed	この装置は、障害が発生した状態です。これは安定状態です。
<b>Standby Unit States</b>	
Cold Standby	この装置は、ピアが Active 状態になるのを待っています。ピア装置が Active 状態になると、この装置は Standby Config 状態に進みます。これは過渡状態です。

表 26-3 フェールオーバーの状態 (続き)

状態	説明
Sync Config	この装置は、ピア装置に実行コンフィギュレーションを要求しています。コンフィギュレーションの同期化中にエラーが発生した場合、この装置は Initialization 状態に戻ります。これは過渡状態です。
Sync File System	この装置は、ピア装置とファイルシステムを同期しています。これは過渡状態です。
Bulk Sync	この装置は、ピア装置から状態の情報を受信しています。この状態が発生するのは、ステートフル フェールオーバーがイネーブルになっている場合のみです。これは過渡状態です。
Standby Ready	この装置は、アクティブ装置に障害が発生した場合に引き継ぐ準備ができています。これは安定状態です。
<b>Active Unit States</b>	
Just Active	この装置がアクティブ装置になったときの最初の状態。この状態のとき、メッセージがピアに送信され、この装置がアクティブになり、IP アドレスと MAC アドレスがインターフェイス用に設定されたことがピアに通知されます。これは過渡状態です。
Active Drain	ピアのキューメッセージは廃棄されます。これは過渡状態です。
Active Applying Config	この装置は、システム コンフィギュレーションを適用しています。これは過渡状態です。
Active Config Applied	この装置は、システム コンフィギュレーションの適用を終了しました。これは過渡状態です。
Active	この装置はアクティブで、トラフィックを処理しています。これは安定状態です。

各状態変化の後に、状態変化の原因が示されます。通常、状態変化の原因は、装置が過渡状態から安定状態へ移行する原因と同じです。次に、状態変化をもたらす可能性のある原因を示します。

- エラーなし
- CI config cmd によって設定されている
- フェールオーバー状態チェック
- フェールオーバー インターフェイスの準備ができた
- HELLO が受信されない
- 他の装置のソフトウェアバージョンが異なっている
- 他の装置の動作モードが異なっている
- 他の装置のライセンスが異なっている
- 他の装置のシャーシ設定が異なっている
- 他の装置のカード設定が異なっている
- 他の装置が、この装置にアクティブ状態になるよう要求した
- 他の装置が、この装置にスタンバイ状態になるよう要求した
- 他の装置が、この装置に障害が発生したことを報告した
- 他の装置が、その装置自体に障害が発生したことを報告した
- コンフィギュレーションのミスマッチ
- アクティブ装置が検出された
- アクティブ装置が検出されなかった
- コンフィギュレーションの同期化が行われた

- 通信障害から回復した
- 他の装置の VLAN コンフィギュレーションが異なっている
- VLAN コンフィギュレーションを確認できない
- コンフィギュレーションの同期化が不完全である
- コンフィギュレーションの同期化に失敗した
- インターフェイス チェック
- この装置で通信に障害が発生した
- ACK がフェールオーバー メッセージを受信しなかった
- 他の装置が、同期化後にラーニング状態で動作しなくなった
- ピアの電源が検出されなかった
- フェールオーバー ケーブルがない
- HA 状態の移行に失敗した
- サービス カード障害が検出された
- 他の装置のサービス カードに障害が発生した
- この装置のサービス カードがピアと同様である
- LAN インターフェイスが未設定状態になった
- ピア装置がリロードされた
- シリアル ケーブルから LAN ベース fover に切り替わった
- コンフィギュレーションの同期化の状態を確認できない
- 原因不明

---

**関連コマンド**

コマンド	説明
<code>show running-config failover</code>	現在のコンフィギュレーション内の <code>failover</code> コマンドを表示します。

---

## show file

ファイル システムに関する情報を表示するには、特権 EXEC モードで **show file** コマンドを使用します。

**show file descriptors | system | information filename**

### シンタックスの説明

<b>descriptors</b>	開かれているファイル記述子をすべて表示します。
<b>information</b>	特定のファイルに関する情報を表示します。
<b>filename</b>	ファイル名を指定します。
<b>system</b>	ディスク ファイル システムについて、サイズ、利用可能なバイト数、メディアのタイプ、フラグ、およびプレフィックス情報を表示します。

### 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	透過	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)	このコマンドが導入されました。

### 例

次の例は、ファイル システムに関する情報を表示する方法を示しています。

```
hostname# show file descriptors
No open file descriptors
hostname# show file system
File Systems:
  Size (b)    Free (b)    Type  Flags  Prefixes
* 60985344   60973056   disk  rw     disk:
```

### 関連コマンド

コマンド	説明
<b>dir</b>	ディレクトリの内容を表示します。
<b>pwd</b>	現在の作業ディレクトリを表示します。



# show firewall

現在のファイアウォール モード（ルーテッドまたは透過）を表示するには、特権 EXEC モードで **show firewall** コマンドを使用します。

**show firewall**

**シンタックスの説明** このコマンドには、引数もキーワードもありません。

**デフォルト** デフォルトの動作や値はありません。

**コマンド モード** 次の表は、このコマンドを入力できるモードを示しています。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	透過	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)	このコマンドが導入されました。

**例** 次に、**show firewall** コマンドの出力例を示します。

```
hostname# show firewall
Firewall mode: Router
```

**関連コマンド**

コマンド	説明
<b>firewall transparent</b>	ファイアウォール モードを設定します。
<b>show mode</b>	現在のコンテキスト モード（シングルまたはマルチ）を表示します。

# show flash

内蔵フラッシュ メモリの内容を表示するには、特権 EXEC モードで **show flash:** コマンドを使用します。

**show flash:**



(注) ASA 5500 シリーズでは、*flash* キーワードは *disk0* のエイリアスです。

## シンタックスの説明

このコマンドには、引数もキーワードもありません。

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	透過	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
既存	このコマンドは既存のものです。

## 例

次の例は、内蔵フラッシュ メモリの内容を表示する方法を示しています。

```
hostname# show flash:
-#- --length-- -----date/time----- path
 11 1301      Feb 21 2005 18:01:34 test.cfg
 12 1949      Feb 21 2005 20:13:36 pepsi.cfg
 13 2551      Jan 06 2005 10:07:36 Leo.cfg
 14 609223    Jan 21 2005 07:14:18 rr.cfg
 15 1619      Jul 16 2004 16:06:48 hackers.cfg
 16 3184      Aug 03 2004 07:07:00 old_running.cfg
 17 4787      Mar 04 2005 12:32:18 admin.cfg
 20 1792      Jan 21 2005 07:29:24 Marketing.cfg
 21 7765184   Mar 07 2005 19:38:30 asdmfile-RLK
 22 1674      Nov 11 2004 02:47:52 potts.cfg
 23 1863      Jan 21 2005 07:29:18 r.cfg
 24 1197      Jan 19 2005 08:17:48 tst.cfg
 25 608554    Jan 13 2005 06:20:54 500kconfig
 26 5124096   Feb 20 2005 08:49:28 cdisk70102
 27 5124096   Mar 01 2005 17:59:56 cdisk70104
 28 2074      Jan 13 2005 08:13:26 negateACL
 29 5124096   Mar 07 2005 19:56:58 cdisk70105
 30 1276      Jan 28 2005 08:31:58 steel
 31 7756788   Feb 24 2005 12:59:46 asdmfile.50074.dbg
 32 7579792   Mar 08 2005 11:06:56 asdmfile.gusingh
 33 7764344   Mar 04 2005 12:17:46 asdmfile.50075.dbg
 34 5124096   Feb 24 2005 11:50:50 cdisk70103
 35 15322     Mar 04 2005 12:30:24 hs_err_pid2240.log

10170368 bytes available (52711424 bytes used)
```

## 関連コマンド

コマンド	説明
<b>dir</b>	ディレクトリの内容を表示します。
<b>show disk0</b>	内蔵フラッシュメモリの内容を表示します。
<b>show disk1</b>	外部フラッシュメモリカードの内容を表示します。

# show fragment

IP フラグメント再構成モジュールの運用データを表示するには、特権 EXEC モードで **show fragment** コマンドを入力します。

**show fragment** [*interface*]

**シンタックスの説明** *interface* (オプション)セキュリティ アプライアンスのインターフェイスを指定します。

**デフォルト** *interface* が指定されていない場合、このコマンドはすべてのインターフェイスに適用されます。

**コマンドモード** 次の表は、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	透過	シングル	マルチ	
				コンテキスト	システム
イネーブル EXEC モード	•	•	•	•	•

コマンド履歴	リリース	変更内容
	7.0(1)	コンフィギュレーションデータを運用データから分離するために、コマンドが <b>show fragment</b> と <b>show running-config fragment</b> の 2 つのコマンドに分割されました。

**例** 次の例は、IP フラグメント再構成モジュールの運用データを表示する方法を示しています。

```
hostname# show fragment
Interface: inside
  Size: 200, Chain: 24, Timeout: 5, Threshold: 133
  Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: outside1
  Size: 200, Chain: 24, Timeout: 5, Threshold: 133
  Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: test1
  Size: 200, Chain: 24, Timeout: 5, Threshold: 133
  Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: test2
  Size: 200, Chain: 24, Timeout: 5, Threshold: 133
  Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
```

関連コマンド	コマンド	説明
	<b>clear configure fragment</b>	IP フラグメント再構成コンフィギュレーションを消去し、デフォルトにリセットします。
	<b>clear fragment</b>	IP フラグメント再構成モジュールの運用データを消去します。
	<b>fragment</b>	特別なパケット フラグメント化の管理を提供して、NFS との互換性を改善します。
	<b>show running-config fragment</b>	IP フラグメント再構成コンフィギュレーションを表示します。

# show gc

ガーベッジ コレクション プロセスに関する統計情報を表示するには、特権 EXEC モードで **show gc** コマンドを使用します。

**show gc**

**シンタックスの説明** このコマンドには、引数もキーワードもありません。

**デフォルト** デフォルトの動作や値はありません。

**コマンド モード** 次の表は、このコマンドを入力できるモードを示しています。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	透過	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
	既存	このコマンドは既存のものです。

**例** 次に、**show gc** コマンドの出力例を示します。

```
hostname# show gc
```

```
Garbage collection process stats:
Total tcp conn delete response      :          0
Total udp conn delete response      :          0
Total number of zombie cleaned     :          0
Total number of embryonic conn cleaned :          0
Total error response                :          0
Total queries generated             :          0
Total queries with conn present response :          0
Total number of sweeps              :         946
Total number of invalid vcid        :          0
Total number of zombie vcid         :          0
```

関連コマンド	コマンド	説明
	<b>clear gc</b>	ガーベッジ コレクション プロセスに関する統計情報を削除します。

## show h225

セキュリティ アプライアンスを越えて確立されている H.225 セッションの情報を表示するには、特権 EXEC モードで **show h225** コマンドを使用します。

**show h225**

**シンタックスの説明** このコマンドには、引数もキーワードもありません。

**デフォルト** デフォルトの動作や値はありません。

**コマンド モード** 次の表は、このコマンドを入力できるモードを示しています。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	透過	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
既存	このコマンドは既存のものです。

**使用上のガイドライン** **show h225** コマンドは、セキュリティ アプライアンスを越えて確立されている H.225 セッションの情報を表示します。 **debug h323 h225 event**、**debug h323 h245 event**、および **show local-host** コマンドと共に、このコマンドは、H.323 検査エンジンの問題のトラブルシューティングに使用されます。

**show h225**、**show h245**、または **show h323-ras** コマンドを使用する前に、**pager** コマンドを設定することを推奨します。多くのセッション レコードが存在し、**pager** コマンドが設定されていない場合、**show** コマンドの出力が最後まで到達するには、しばらく時間がかかることがあります。異常なほど多くの接続が存在する場合は、デフォルトのタイムアウト値または設定した値に基づいてセッションがタイムアウトしているかどうか確認します。タイムアウトしていなければ問題があるので、調査が必要です。

**例** 次に、**show h225** コマンドの出力例を示します。

```
hostname# show h225
Total H.323 Calls: 1
1 Concurrent Call(s) for
  | Local: | 10.130.56.3/1040 | Foreign: 172.30.254.203/1720
  | 1. CRV 9861
  | Local: | 10.130.56.3/1040 | Foreign: 172.30.254.203/1720
0 Concurrent Call(s) for
  | Local: | 10.130.56.4/1050 | Foreign: 172.30.254.205/1720
```

この出力は、現在セキュリティ アプライアンスを通過しているアクティブ H.323 コールが 1 つ、ローカル エンドポイント 10.130.56.3 と外部のホスト 172.30.254.203 の間にあることを示しています。また、これらの特定のエンドポイントの間に、同時コールが 1 つあり、そのコールの CRV (Call Reference Value) が 9861 であることを示しています。

ローカルエンドポイント 10.130.56.4 と外部ホスト 172.30.254.205 に対して、同時コールは 0 です。つまり H.225 セッションがまだ存在しているものの、このエンドポイント間にはアクティブ コールがないことを意味します。この状況は、**show h225** コマンドを実行したときに、コールはすでに終了しているが、H.225 セッションがまだ削除されていない場合に発生する可能性があります。または、2 つのエンドポイントが、「maintainConnection」を TRUE に設定しているため、TCP 接続をまだ開いたままにしていることを意味する可能性もあります。したがって、「maintainConnection」を再度 FALSE に設定するまで、またはコンフィギュレーション内の H.225 タイムアウト値に基づくセッションのタイムアウトが起こるまで、セッションは開いたままになります。

#### 関連コマンド

コマンド	説明
<b>debug h323</b>	H.323 のデバッグ情報の表示をイネーブルにします。
<b>inspect h323</b>	H.323 アプリケーション検査をイネーブルにします。
<b>show h245</b>	スロースタートを使用しているエンドポイントがセキュリティ アプライアンスを越えて確立した H.245 セッションの情報を表示します。
<b>show h323-ras</b>	セキュリティ アプライアンスを越えて確立された H.323 RAS セッションの情報を表示します。
<b>timeout h225   h323</b>	H.225 シグナリング接続または H.323 制御接続が終了するまでのアイドル時間を設定します。

## show h245

スロー スタートを使用しているエンドポイントによって、セキュリティ アプライアンスを越えて確立されている H.245 セッションの情報を表示するには、特権 EXEC モードで **show h245** コマンドを使用します。

**show h245**

**シンタックスの説明** このコマンドには、引数もキーワードもありません。

**デフォルト** デフォルトの動作や値はありません。

**コマンドモード** 次の表は、このコマンドを入力できるモードを示しています。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	透過	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
既存	このコマンドは既存のものです。

**使用上のガイドライン** **show h245** コマンドは、スロースタートを使用しているエンドポイントがセキュリティ アプライアンスを越えて確立した H.245 セッションの情報を表示します（スロースタートは、コールの 2 つのエンドポイントが H.245 用の別の TCP コントロール チャネルを開いた場合です。ファースト スタートは、H.245 メッセージが H.225 コントロール チャネル上の H.225 メッセージの一部として交換された場合です）。**debug h323 h245 event**、**debug h323 h225 event**、および **show local-host** コマンドと共に、このコマンドは、H.323 検査エンジンの問題のトラブルシューティングに使用されます。

**例** 次に、**show h245** コマンドの出力例を示します。

```
hostname# show h245
Total: 1
  | LOCAL | TPKT | FOREIGN | TPKT
1 | 10.130.56.3/1041 | 0 | 172.30.254.203/1245 | 0
  | MEDIA: LCN 258 Foreign 172.30.254.203 RTP 49608 RTCP 49609
  | Local | 10.130.56.3 RTP 49608 RTCP 49609
  | MEDIA: LCN 259 Foreign 172.30.254.203 RTP 49606 RTCP 49607
  | Local | 10.130.56.3 RTP 49606 RTCP 49607
```

セキュリティ アプライアンスを越えているアクティブな H.245 コントロールセッションが、現在 1 つあります。ローカルエンドポイントは、10.130.56.3 であり、TPKT 値が 0 であることから、このエンドポイントからの次のパケットには TPKT ヘッダーがあると予測します（TKTP ヘッダーは、各 H.225/H.245 メッセージの前に送られる 4 バイトのヘッダーです。このヘッダーで、この 4 バイトのヘッダーを含むメッセージの長さが分かります）。外部のホストのエンドポイントは、172.30.254.203 であり、TPKT 値が 0 であることから、このエンドポイントからの次のパケットには TPKT ヘッダーがあると予測します。



これらのエンドポイント間でネゴシエートされたメディアには、258 という LCN (論理チャネル番号) があり、外部に 172.30.254.203/49608 という RTP IP アドレス / ポートペアと 172.30.254.203/49609 という RTCP IP アドレス / ポートペアを持ち、ローカルに 10.130.56.3/49608 という RTP IP アドレス / ポートペアと 49609 という RTCP ポートを持っています。

259 という 2 番目の LCN には、外部に 172.30.254.203/49606 という RTP IP アドレス / ポートペアと 172.30.254.203/49607 という RTCP IP アドレス / ポートペアがあり、ローカルに 10.130.56.3/49606 という RTP IP アドレス / ポートペアと 49607 という RTCP ポートを持っています。

#### 関連コマンド

コマンド	説明
<b>debug h323</b>	H.323 のデバッグ情報の表示をイネーブルにします。
<b>inspect h323</b>	H.323 アプリケーション検査をイネーブルにします。
<b>show h245</b>	スロースタートを使用しているエンドポイントがセキュリティ アプライアンスを越えて確立した H.245 セッションの情報を表示します。
<b>show h323-ras</b>	セキュリティ アプライアンスを越えて確立された H.323 RAS セッションの情報を表示します。
<b>timeout h225   h323</b>	H.225 シグナリング接続または H.323 制御接続が終了するまでのアイドル時間を設定します。

## show h323-ras

ゲートキーパーとその H.323 エンドポイントの間でセキュリティ アプライアンスを越えて確立されている H.323 RAS セッションの情報を表示するには、特権 EXEC モードで **show h323-ras** コマンドを使用します。

**show h323-ras**

**シンタックスの説明** このコマンドには、引数もキーワードもありません。

**デフォルト** デフォルトの動作や値はありません。

**コマンドモード** 次の表は、このコマンドを入力できるモードを示しています。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	透過	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
既存	このコマンドは既存のものです。

**使用上のガイドライン** **show h323-ras** コマンドは、セキュリティ アプライアンスを越えてゲートキーパーとその H.323 エンドポイントの間に確立されている H.323 RAS セッションの情報を表示します。**debug h323 ras event** および **show local-host** コマンドと共に、このコマンドは、H.323 RAS 検査エンジンの問題のトラブルシューティングに使用されます。

**show h323-ras** コマンドは、H.323 検査エンジンの問題のトラブルシューティングに使用される接続情報を表示します。詳細については、**inspect protocol h323 {h225 | ras}** コマンドのページを参照してください。

**例** 次に、**show h323-ras** コマンドの出力例を示します。

```
hostname# show h323-ras
Total: 1
 | GK | Caller
 | 172.30.254.214 10.130.56.14
hostname#
```

この出力は、ゲートキーパー 172.30.254.214 とそのクライアント 10.130.56.14 の間にアクティブな登録が 1 つあることを示しています。

## 関連コマンド

コマンド	説明
<b>debug h323</b>	H.323 のデバッグ情報の表示をイネーブルにします。
<b>inspect h323</b>	H.323 アプリケーション検査をイネーブルにします。
<b>show h245</b>	スロースタートを使用しているエンドポイントがセキュリティ アプライアンスを越えて確立した H.245 セッションの情報を表示します。
<b>show h323-ras</b>	セキュリティ アプライアンスを越えて確立された H.323 RAS セッションの情報を表示します。
<b>timeout h225   h323</b>	H.225 シグナリング接続または H.323 制御接続が終了するまでのアイドル時間を設定します。

## show history

以前に入力したコマンドを表示するには、ユーザ EXEC モードで **show history** コマンドを使用します。

```
show history
```

## シンタックスの説明

このコマンドには、引数もキーワードもありません。

## デフォルト

デフォルトの動作や値はありません。

## コマンドモード

次の表は、このコマンドを入力できるモードを示しています。

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

## コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

## 使用上のガイドライン

**show history** コマンドを使用すると、以前に入力したコマンドを表示できます。上矢印キーと下矢印キーを使用したり、**^p** を入力して入力済みの行を表示したり、**^n** を入力して次の行を表示したりして、コマンドを個々に調べることができます。

## 例

次の例は、以前に入力したコマンドをユーザ EXEC モードに入っているときに表示する方法を示しています。

```
hostname> show history
show history
help
show history
```

次の例は、以前に入力したコマンドを特権 EXEC モードに入っているときに表示する方法を示しています。

```
hostname# show history
show history
help
show history
enable
show history
```

次の例は、以前に入力したコマンドをグローバル コンフィギュレーション モードに入っているときに表示する方法を示しています。

```
hostname(config)# show history
show history
help
show history
enable
show history
config t
show history
```

#### 関連コマンド

コマンド	説明
help	指定したコマンドのヘルプを表示します。

# show icmp

ICMP コンフィギュレーションを表示するには、特権 EXEC モードで **show icmp** コマンドを使用します。

## show icmp

**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	透過	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
既存	このコマンドは既存のものです。

**使用上のガイドライン** **show icmp** コマンドは、ICMP コンフィギュレーションを表示します。

**例** 次の例では、ICMP コンフィギュレーションを表示しています。

```
hostname# show icmp
```

**関連コマンド**

<b>clear configure icmp</b>	ICMP コンフィギュレーションを消去します。
<b>debug icmp</b>	ICMP に関するデバッグ情報の表示をイネーブルにします。
<b>icmp</b>	セキュリティ アプライアンス インターフェイスで終端する ICMP トラフィックに対して、アクセス規則を設定します。
<b>inspect icmp</b>	ICMP 検査エンジンをイネーブルまたはディセーブルにします。
<b>timeout icmp</b>	ICMP のアイドル タイムアウトを設定します。

# show idb

インターフェイス記述子ブロックのステータスに関する情報を表示するには、特権 EXEC モードで **show idb** コマンドを使用します。

**show idb**

**シンタックスの説明** このコマンドには、引数もキーワードもありません。

**デフォルト** デフォルトの動作や値はありません。

**コマンドモード** 次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴	リリース	変更内容
	7.0(1)	このコマンドが導入されました。

**使用上のガイドライン** IDB は、インターフェイスのリソースを表現するための内部データ構造です。表示される出力については、「例」の項を参照してください。

## 例

次に、**show idb** コマンドの出力例を示します。

```
hostname# show idb
Maximum number of Software IDBs 280. In use 23.

                HWIDBs      SWIDBs
                Active 6      21
                Inactive 1      2
                Total IDBs 7      23
                Size each (bytes) 116      212
                Total bytes 812      4876

HWIDB# 1 0xbb68ebc Control0/0
HWIDB# 2 0xcd47d84 GigabitEthernet0/0
HWIDB# 3 0xcd4c1dc GigabitEthernet0/1
HWIDB# 4 0xcd5063c GigabitEthernet0/2
HWIDB# 5 0xcd54a9c GigabitEthernet0/3
HWIDB# 6 0xcd58f04 Management0/0

SWIDB# 1 0x0bb68f54 0x01010001 Control0/0
SWIDB# 2 0x0cd47e1c 0xffffffff GigabitEthernet0/0
SWIDB# 3 0x0cd772b4 0xffffffff GigabitEthernet0/0.1
  PEER IDB# 1 0x0d44109c 0xffffffff 3 GigabitEthernet0/0.1
  PEER IDB# 2 0x0d2c0674 0x00020002 2 GigabitEthernet0/0.1
  PEER IDB# 3 0x0d05a084 0x00010001 1 GigabitEthernet0/0.1
SWIDB# 4 0x0bb7501c 0xffffffff GigabitEthernet0/0.2
SWIDB# 5 0x0cd4c274 0xffffffff GigabitEthernet0/1
SWIDB# 6 0x0bb75704 0xffffffff GigabitEthernet0/1.1
  PEER IDB# 1 0x0cf8686c 0x00020003 2 GigabitEthernet0/1.1
SWIDB# 7 0x0bb75dec 0xffffffff GigabitEthernet0/1.2
  PEER IDB# 1 0x0d2c08ac 0xffffffff 2 GigabitEthernet0/1.2
SWIDB# 8 0x0bb764d4 0xffffffff GigabitEthernet0/1.3
  PEER IDB# 1 0x0d441294 0x00030001 3 GigabitEthernet0/1.3
SWIDB# 9 0x0cd506d4 0x01010002 GigabitEthernet0/2
SWIDB# 10 0x0cd54b34 0xffffffff GigabitEthernet0/3
  PEER IDB# 1 0x0d3291ec 0x00030002 3 GigabitEthernet0/3
  PEER IDB# 2 0x0d2c0aa4 0x00020001 2 GigabitEthernet0/3
  PEER IDB# 3 0x0d05a474 0x00010002 1 GigabitEthernet0/3
SWIDB# 11 0x0cd58f9c 0xffffffff Management0/0
  PEER IDB# 1 0x0d05a65c 0x00010003 1 Management0/0
```

表 26-4 に、各フィールドの説明を示します。

表 26-4 show idb stats のフィールド

フィールド	説明
HWIDBs	すべての HWIDB の統計情報を表示します。HWIDB は、システムのハードウェアポートごとに作成されます。
SWIDBs	すべての SWIDB の統計情報を表示します。SWIDB は、システムのメインインターフェイスとサブインターフェイスごと、およびコンテキストに割り当てられているインターフェイスごとに作成されます。 他の一部の内部ソフトウェアモジュールも IDB を作成します。
HWIDB#	ハードウェアインターフェイスのエントリを示します。IDB シーケンス番号、アドレス、およびインターフェイス名が各行に表示されます。
SWIDB#	ソフトウェアインターフェイスのエントリを示します。IDB シーケンス番号、アドレス、対応する vPif ID、およびインターフェイス名が各行に表示されます。
PEER IDB#	コンテキストに割り当てられているインターフェイスを示します。IDB シーケンス番号、アドレス、対応する vPif ID、コンテキスト ID、およびインターフェイス名が各行に表示されます。

## 関連コマンド

コマンド	説明
<b>interface</b>	インターフェイスを設定し、インターフェイス コンフィギュレーションモードに入ります。
<b>show interface</b>	インターフェイスのランタイム ステータスと統計情報を表示します。



# show igmp groups

セキュリティ アプライアンスに直接接続し、IGMP によってラーニングされたレシーバーがあるマルチキャスト グループを表示するには、特権 EXEC モードで **show igmp groups** コマンドを使用します。

```
show igmp groups [[reserved | group] [if_name] [detail]] | summary]
```

## シンタックスの説明

<i>detail</i>	(オプション) 送信元の詳細な説明を表示します。
<i>group</i>	(オプション) IGMP グループのアドレス。このオプション引数を指定すると、表示される情報は指定したグループに関するものだけになります。
<i>if_name</i>	(オプション) 指定したインターフェイスのグループ情報を表示します。
<i>reserved</i>	(オプション) 予約済みグループに関する情報を表示します。
<i>summary</i>	(オプション) グループ加入の要約情報を表示します。

## 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	透過	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)	このコマンドが導入されました。

## 使用上のガイドライン

オプションの引数とキーワードをすべて省略した場合、**show igmp groups** コマンドは、直接接続しているすべてのマルチキャスト グループをグループ アドレス、インターフェイス タイプ、およびインターフェイス番号別に表示します。

## 例

次に、**show igmp groups** コマンドの出力例を示します。

```
hostname#show igmp groups
```

```
IGMP Connected Group Membership
Group Address      Interface      Uptime      Expires      Last Reporter
224.1.1.1          inside         00:00:53    00:03:26    192.168.1.6
```

## 関連コマンド

コマンド	説明
<b>show igmp interface</b>	インターフェイスのマルチキャスト情報を表示します。

# show igmp interface

インターフェイスのマルチキャスト情報を表示するには、特権 EXEC モードで **show igmp interface** コマンドを使用します。

```
show igmp interface [if_name]
```

## シンタックスの説明

*if\_name* (オプション) 選択したインターフェイスの IGMP グループ情報を表示します。

## 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	透過	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)	このコマンドが変更されました。 <i>detail</i> キーワードが削除されました。

## 使用上のガイドライン

オプションの *if\_name* 引数を省略した場合、**show igmp interface** コマンドはすべてのインターフェイスの情報を表示します。

## 例

次に、**show igmp interface** コマンドの出力例を示します。

```
hostname# show igmp interface inside

inside is up, line protocol is up
Internet address is 192.168.37.6, subnet mask is 255.255.255.0
IGMP is enabled on interface
IGMP query interval is 60 seconds
Inbound IGMP access group is not set
Multicast routing is enabled on interface
Multicast TTL threshold is 0
Multicast designated router (DR) is 192.168.37.33
No multicast groups joined
```

## 関連コマンド

コマンド	説明
<b>show igmp groups</b>	セキュリティアプライアンスに直接接続されている受信者、および IGMP を通じてラーニングされた受信者を持つマルチキャストグループを表示します。

# show igmp traffic

IGMP トラフィックに関する統計情報を表示するには、特権 EXEC モードで **show igmp traffic** コマンドを使用します。

**show igmp traffic**

**シンタックスの説明** このコマンドには、引数もキーワードもありません。

**デフォルト** デフォルトの動作や値はありません。

**コマンドモード** 次の表は、このコマンドを入力できるモードを示しています。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	透過	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)	このコマンドが導入されました。

**例** 次に、**show igmp traffic** コマンドの出力例を示します。

```
hostname# show igmp traffic

IGMP Traffic Counters
Elapsed time since counters cleared: 00:02:30

```

	Received	Sent
Valid IGMP Packets	3	6
Queries	2	6
Reports	1	0
Leaves	0	0
Mtrace packets	0	0
DVMRP packets	0	0
PIM packets	0	0

```

Errors:
Malformed Packets          0
Martian source             0
Bad Checksums              0

```

**関連コマンド**

コマンド	説明
<b>clear igmp counters</b>	すべての IGMP 統計情報カウンタを消去します。
<b>clear igmp traffic</b>	IGMP トラフィック カウンタを消去します。

# show interface

インターフェイスに関する統計情報を表示するには、ユーザ EXEC モードで **show interface** コマンドを使用します。

```
show interface [physical_interface[.subinterface] | mapped_name | interface_name | vlan number]
[stats | detail]
```

## シンタックスの説明

<b>detail</b>	(オプション) インターフェイスの詳細な情報を表示します。この情報には、インターフェイスが追加された順序、設定されている状態、実際の状態が含まれ、非対称ルーティングが <b>asr-group</b> コマンドによってイネーブルになっている場合は、非対称ルーティングの統計情報も含まれています。すべてのインターフェイスを表示する場合、SSM 用の内部インターフェイスが ASA 5500 シリーズ適応型セキュリティ アプライアンスにインストールされているときは、それらのインターフェイスに関する情報が表示されます。内部インターフェイスは、ユーザが設定することはできません。この情報は、デバッグのみを目的としたものです。
<b>interface_name</b>	(オプション) <b>nameif</b> コマンドで設定したインターフェイス名を指定します。
<b>mapped_name</b>	(オプション) マルチ コンテキスト モードで、マッピング名を <b>allocate-interface</b> コマンドを使用して割り当てた場合、その名前を指定します。
<b>physical_interface</b>	(オプション) インターフェイス ID ( <b>gigabitethernet0/1</b> など) を指定します。使用できる値については、 <b>interface</b> コマンドを参照してください。
<b>stats</b>	(デフォルト) インターフェイスに関する情報と統計情報を表示します。このキーワードはデフォルトであるため、入力を省略できます。
<b>subinterface</b>	(オプション) 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。
<b>vlan number</b>	(オプション) 組み込みスイッチを持つ ASA 5505 適応型セキュリティ アプライアンスなどのモデルに対して、VLAN インターフェイスを指定します。

## デフォルト

オプションを指定しない場合は、すべてのインターフェイスに関する基本的な統計情報が表示されます。

## 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	透過	シングル	マルチ コンテキスト	システム
ユーザ EXEC	•	•	•	•	•

## コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが、新しいインターフェイス番号付け方式を取り入れるように修正され、明示的な指定をするための <b>stats</b> キーワード、および <b>detail</b> キーワードが追加されました。
7.0(4)	このコマンドに 4GE SSM インターフェイスのサポートが追加されました。
7.2(1)	このコマンドにスイッチ インターフェイスのサポートが追加されました。

**使用上のガイドライン**

インターフェイスが複数のコンテキストで共有されている場合は、コンテキスト内でこのコマンドを入力すると、セキュリティ アプライアンスは現在のコンテキストに関する統計情報のみ表示します。このコマンドをシステム実行スペースで物理インターフェイスに関して入力すると、セキュリティ アプライアンスはすべてのコンテキストの合算統計情報を表示します。

サブインターフェイスに関して表示される統計情報の数は、物理インターフェイスに関して表示される統計情報の数のサブセットです。

インターフェイス名をシステム実行スペースで使用することはできません。これは、**nameif** コマンドはコンテキスト内でのみ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でのみ使用できます。**allocate-interface** コマンドで **visible** キーワードを設定した場合、セキュリティ アプライアンスは **show interface** コマンドの出力にインターフェイスの ID を表示します。

表示される出力については、「例」の項を参照してください。

**例**

次に、**show interface** コマンドの出力例を示します。

```
hostname> show interface
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
    Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
    MAC address 000b.fcf8.c44e, MTU 1500
    IP address 10.86.194.60, subnet mask 255.255.254.0
    1328522 packets input, 124426545 bytes, 0 no buffer
    Received 1215464 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    9 L2 decode drops
    124606 packets output, 86803402 bytes, 0 underruns
    0 output errors, 0 collisions
    0 late collisions, 0 deferred
    input queue (curr/max blocks): hardware (0/7) software (0/0)
    output queue (curr/max blocks): hardware (0/13) software (0/0)
  Traffic Statistics for "outside":
    1328509 packets input, 99873203 bytes
    124606 packets output, 84502975 bytes
    524605 packets dropped
Interface GigabitEthernet0/1 "inside", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps
    Auto-Duplex, Auto-Speed
    MAC address 000b.fcf8.c44f, MTU 1500
    IP address 10.10.0.1, subnet mask 255.255.0.0
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 L2 decode drops
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions
    0 late collisions, 0 deferred
    input queue (curr/max blocks): hardware (0/0) software (0/0)
    output queue (curr/max blocks): hardware (0/0) software (0/0)
  Traffic Statistics for "inside":
    0 packets input, 0 bytes
    0 packets output, 0 bytes
    0 packets dropped
Interface GigabitEthernet0/2 "faillink", is administratively down, line protocol is
down
```

```

Hardware is i82546GB rev03, BW 1000 Mbps
  Auto-Duplex, Auto-Speed
  Description: LAN/STATE Failover Interface
  MAC address 000b.fcf8.c450, MTU 1500
  IP address 192.168.1.1, subnet mask 255.255.255.0
  0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 L2 decode drops
  0 packets output, 0 bytes, 0 underruns
  0 output errors, 0 collisions
  0 late collisions, 0 deferred
  input queue (curr/max blocks): hardware (0/0) software (0/0)
  output queue (curr/max blocks): hardware (0/0) software (0/0)
Traffic Statistics for "faillink":
  0 packets input, 0 bytes
  1 packets output, 28 bytes
  0 packets dropped
Interface GigabitEthernet0/3 "", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps
    Auto-Duplex, Auto-Speed
    Available but not configured via nameif
    MAC address 000b.fcf8.c451, MTU not set
    IP address unassigned
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 L2 decode drops
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions
    0 late collisions, 0 deferred
    input queue (curr/max blocks): hardware (0/0) software (0/0)
    output queue (curr/max blocks): hardware (0/0) software (0/0)
Interface Management0/0 "", is administratively down, line protocol is down
  Hardware is i82557, BW 100 Mbps
    Auto-Duplex, Auto-Speed
    Available but not configured via nameif
    MAC address 000b.fcf8.c44d, MTU not set
    IP address unassigned
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 L2 decode drops
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collisions, 0 deferred
    0 lost carrier, 0 no carrier
    input queue (curr/max blocks): hardware (128/128) software (0/0)
    output queue (curr/max blocks): hardware (0/0) software (0/0)

```

表 26-5 に、各フィールドの説明を示します。

表 26-5 show interface のフィールド

フィールド	説明
Interface ID	インターフェイス ID。コンテキスト内では、 <b>allocate-interface</b> コマンドで <b>visible</b> キーワードを設定しない限り、セキュリティ アプライアンスはマッピング名（設定されている場合）を表示します。
"interface_name"	<b>nameif</b> コマンドで設定したインターフェイス名。システム内でこの名前を設定することはできないため、システム実行スペースでは、このフィールドは空白です。名前を設定していない場合は、 <b>Hardware</b> 行の後に次のメッセージが表示されます。  Available but not configured via nameif

表 26-5 show interface のフィールド (続き)

フィールド	説明
is state	管理状態。次のいずれかです。 <ul style="list-style-type: none"> <li>• up : インターフェイスはシャットダウンされていません。</li> <li>• administratively down : インターフェイスは <b>shutdown</b> コマンドでシャットダウンされています。</li> </ul>
Line protocol is state	回線の状態。次のいずれかです。 <ul style="list-style-type: none"> <li>• up : 使用しているケーブルがネットワーク インターフェイスに接続されています。</li> <li>• down : ケーブルが誤っているか、インターフェイス コネクタに接続されていません。</li> </ul>
VLAN identifier	サブインターフェイスの VLAN ID。
Hardware	インターフェイスのタイプ、最大帯域幅、デュプレックス方式、および速度。リンクがダウンしている場合は、デュプレックス方式と速度は設定値が表示されます。リンクが動作している場合、これらのフィールドには実際の設定がカッコ ( ) で囲まれて設定値と共に表示されます。次に、一般的なハードウェアタイプを示します。 <ul style="list-style-type: none"> <li>• i82542 : PIX プラットフォームで使用される Intel PCI ファイバ ギガビットカード</li> <li>• i82543 : PIX プラットフォームで使用される Intel PCI-X ファイバ ギガビットカード</li> <li>• i82546GB : ASA プラットフォームで使用される Intel PCI-X 銅線ギガビット</li> <li>• i82547GI : ASA プラットフォームでバックプレーンとして使用される Intel CSA 銅線ギガビット</li> <li>• i82557 : ASA プラットフォームで使用される Intel PCI 銅線ファーストイーサネット</li> <li>• i82559 : PIX プラットフォームで使用される Intel PCI 銅線ファーストイーサネット</li> </ul> VCS7380 : SSM-4GE で使用される Vitesse Four Port ギガビットスイッチ
Media-type	(4GE SSM インターフェイスのみ) インターフェイスが RJ-45 または SFP のいずれとして設定されているかを表示します。
message area	特定の状況下で、メッセージが表示されることがあります。次の例を参照してください。 <ul style="list-style-type: none"> <li>• システム実行スペースでは、次のメッセージが表示されることがあります。 Available for allocation to a context</li> <li>• 名前を設定していない場合は、次のメッセージが表示されます。 Available but not configured via nameif</li> </ul>
MAC address	インターフェイスの MAC アドレス。
MTU	このインターフェイスで許容されるパケットの最大サイズ (バイト単位)。インターフェイス名を設定していない場合、このフィールドには「MTU not set」と表示されます。

表 26-5 show interface のフィールド (続き)

フィールド	説明
IP address	<b>ip address</b> コマンドを使用して設定した、または DHCP サーバから受信したインターフェイス IP アドレス。システム内で IP アドレスを設定することはできないため、システム実行スペースでは、このフィールドに「IP address unassigned」と表示されます。
Subnet mask	IP アドレスのサブネット マスク。
Packets input	このインターフェイスで受信されたパケット数。
Bytes	このインターフェイスで受信されたバイト数。
No buffer	メイン システムのバッファ スペースがなかったために、廃棄された受信済みパケットの数。この数を、無視された数と比較してください。イーサネット ネットワーク上のブロードキャスト ストームは、多くの場合、入力バッファ イベントがないことに原因があります。
Received:	
Broadcasts	受信されたブロードキャストの数。
Runts	最小限のパケット サイズ (64 バイト) よりも小さいために廃棄されたパケットの数。ラントの原因は、通常は衝突です。不適切な配線や電気干渉が原因となって発生することもあります。
Giants	最大パケット サイズを超えているために廃棄されたパケットの数。たとえば、1,518 バイトを超えるイーサネット パケットはすべてジャイアントと見なされます。
Input errors	下に示したタイプを含めた、入力エラーの総数。入力に関係しているこの他のエラーも、入力エラーの数が増加する原因になります。また、一部のデータグラムは複数のエラーを包含していることもあります。したがって、この合計数は下に示したタイプについて表示されるエラーの数を超える場合があります。
CRC	巡回冗長検査エラーの数。ステーションは、フレームを送信するときにフレーム末尾に CRC を付加します。この CRC は、フレームに含まれているデータに基づいて、アルゴリズムに従って生成されます。送信元と宛先の間でフレームが改変された場合、セキュリティ アプライアンスは、CRC が一致しないことを指摘します。CRC の値が大きくなる原因は、通常は衝突か、不良データを転送しているステーションです。
Frame	フレーム エラーの数。不良フレームには、長さが不適切なパケット、またはフレーム チェックサムが正しくないパケットが含まれています。このエラーが発生する原因は、通常は衝突か、故障しているイーサネット デバイスです。
Overrun	入力レートがセキュリティ アプライアンスのデータ処理能力を超えたために、受信したデータをセキュリティ アプライアンスがハードウェア バッファに渡すことができなかった回数。
Ignored	インターフェイス ハードウェアの内部バッファが不足したために、インターフェイスによって無視された受信パケットの数。これらのバッファは、バッファの説明で前に述べたシステム バッファとは別のものです。無視される数は、ブロードキャスト ストームとバースト雑音が原因となって増加する場合もあります。
Abort	このフィールドは使用されません。この値は常に 0 です。
L2 decode drops	名前が ( <b>nameif</b> コマンドで) 設定されていないため、または無効な VLAN ID を持つフレームを受信したために、ドロップされたパケットの数。



表 26-5 show interface のフィールド (続き)

フィールド	説明
Packets output	このインターフェイスで送信されたパケット数。
Bytes	このインターフェイスで送信されたバイト数。
Underruns	トランスミッタの動作速度がセキュリティ アプライアンスの処理速度を上回った回数。
Output Errors	衝突が設定されている最大数を越えたために伝送されなかったフレーム数。このカウンタは、ネットワーク トラフィックが大きい間は増加します。
Collisions	イーサネット衝突 (1 つまたは複数の衝突) が原因で、再送されたメッセージ数。これは、通常、拡張しすぎた LAN (イーサネット ケーブルまたはトランシーバ ケーブルが長すぎる、ステーション間にリピータが 3 つ以上ある、またはカスケード接続されたマルチポート トランシーバが多すぎる) で発生します。衝突したパケットは、出力パケットによって一度だけカウントされます。
Interface resets	インターフェイスがリセットされた回数。インターフェイスが 3 秒間伝送できない場合、セキュリティ アプライアンスはインターフェイスをリセットして、伝送を再開します。この間隔の間も、接続状態は保持されます。インターフェイスのリセットは、インターフェイスがループバックされた場合、またはシャットダウンされた場合にも起こります。
Babbles	未使用 (「babble」は、トランスミッタがインターフェイス上に留まっている時間が、最大長のフレームの伝送に要する時間を越えたことを意味します)。
Late collisions	衝突が表示される通常のウィンドウに表示されない衝突が発生したために伝送されなかったフレーム数。遅延衝突は、パケットの伝送で遅れて検出される衝突です。通常は、このようなことは起こらないようになっています。2 つのイーサネット ホストが同時に伝送を試みた場合、両ホストが早期にパケットの衝突を起こして両方がバックオフするか、2 番目のホストが 1 番目のホストの伝送に気付いて待機します。  遅延衝突が発生した場合、デバイスが割り込んでイーサネット上でパケットの送信を試み、同時にセキュリティ アプライアンスがパケットの送信を一部終了します。セキュリティ アプライアンスは、パケットの最初の部分が入ったバッファをすでに解放してしまっている可能性があるため、パケットを再送信しません。ネットワークング プロトコルは、パケットを再送信することで衝突に対処するように設計されているため、これは大きな問題ではありません。しかし、遅延衝突はネットワークに問題が存在することを示します。よくある問題は、リピータを何台も使用して拡張したネットワーク、および仕様範囲外で動作しているイーサネット ネットワークです。
Deferred	リンク上のアクティビティが原因で、伝送前に延期されたフレーム数。
Rate limit drops	(4GE SSM インターフェイスのみ) 転送速度がギガビットではないインターフェイスを設定して、10Mbps を超える速度で転送しようとした場合に、ドロップされたパケットの数。
Lost carrier	伝送中に搬送信号が消失した回数。
No carrier	未使用。
Input queue (curr/max blocks):	入力キューに入っているパケットの数 (現在値と最大値)。
Hardware	ハードウェア キュー内のパケットの数。
Software	ソフトウェア キュー内のパケットの数。

表 26-5 show interface のフィールド (続き)

フィールド	説明
Output queue (curr/max blocks):	出力キューに入っているパケットの数 (現在値と最大値)。
Hardware	ハードウェア キュー内のパケットの数。
Software	ソフトウェア キュー内のパケットの数。
Traffic Statistics:	受信、送信、またはドロップされたパケットの数。
Packets input	受信されたパケットの数とバイトの数。
Packets output	送信されたパケットの数とバイトの数。
Packets dropped	ドロップしたパケットの数。


次に、ASA 5505 適応型セキュリティ アプライアンスでの **show interface** コマンドの出力例を示します。スイッチ ポートが含まれます。

```
hostname# show interface
Interface Vlan1 "inside", is up, line protocol is up
  Hardware is EtherSVI
    MAC address 00d0.2bff.449f, MTU 1500
    IP address 1.1.1.1, subnet mask 255.0.0.0
  Traffic Statistics for "inside":
    0 packets input, 0 bytes
    0 packets output, 0 bytes
    0 packets dropped
    1 minute input rate 0 pkts/sec, 0 bytes/sec
    1 minute output rate 0 pkts/sec, 0 bytes/sec
    1 minute drop rate, 0 pkts/sec
    5 minute input rate 0 pkts/sec, 0 bytes/sec
    5 minute output rate 0 pkts/sec, 0 bytes/sec
    5 minute drop rate, 0 pkts/sec

Interface Ethernet0/0 "", is up, line protocol is up
  Hardware is 88E6095, BW 100 Mbps
    Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
    Available but not configured via nameif
    MAC address 00d0.2bfd.6ec5, MTU not set
    IP address unassigned
    407 packets input, 53587 bytes, 0 no buffer
    Received 103 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 L2 decode drops
    43 switch ingress policy drops
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collisions, 0 deferred
    0 lost carrier, 0 no carrier
    0 rate limit drops
    0 switch egress policy drops
```

表 26-6 に、ASA 5505 適応型セキュリティ アプライアンスなどのスイッチ インターフェイスに関する **show interface** コマンドの各フィールドの説明を示します。**show interface** コマンドで表示されるフィールドについては、表 26-5 を参照してください。

表 26-6 スイッチ インターフェイスに関する **show interface** のフィールド

フィールド	説明
switch ingress policy drops	<p>このドロップは通常、ポートが正常に設定されていない場合に表示されます。このドロップは、デフォルトまたはユーザ定義のスイッチ ポート設定の結果として、パケットがスイッチ ポート内で正常に転送されない場合に増分します。次のようなコンフィギュレーションがこのドロップの原因と考えられます。</p> <ul style="list-style-type: none"> <li>• <b>nameif</b> コマンドが VLAN インターフェイスで設定されませんでした。</li> </ul> <p> (注) 同じ VLAN のインターフェイスとして、<b>nameif</b> コマンドが設定されていなかった場合でも、VLAN 内でスイッチングが正常であれば、このカウンタは増分しません。</p> <ul style="list-style-type: none"> <li>• VLAN がシャットダウンします。</li> <li>• アクセス ポートが 802.1Q タグ付きパケットを受信しました。</li> <li>• トランク ポートが、許可されていないタグ、またはタグ付きでないパケットを受信しました。</li> </ul>
switch egress policy drops	現在使用されていません。

次に、**show interface detail** コマンドの出力例を示します。次の例では、すべてのインターフェイスに関する詳細なインターフェイス統計情報を表示しています。この情報には、内部インターフェイス（プラットフォームに存在する場合）が含まれ、非対称ルーティングが **asr-group** コマンドによってイネーブルになっている場合は、非対称ルーティングの統計情報も含まれています。

```
hostname> show interface detail
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
    Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
    MAC address 000b.fcf8.c44e, MTU 1500
    IP address 10.86.194.60, subnet mask 255.255.254.0
    1330214 packets input, 124580214 bytes, 0 no buffer
    Received 1216917 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    9 L2 decode drops
    124863 packets output, 86956597 bytes, 0 underruns
    0 output errors, 0 collisions
    0 late collisions, 0 deferred
    input queue (curr/max blocks): hardware (0/7) software (0/0)
    output queue (curr/max blocks): hardware (0/13) software (0/0)
  Traffic Statistics for "outside":
    1330201 packets input, 99995120 bytes
    124863 packets output, 84651382 bytes
    525233 packets dropped
  Control Point Interface States:
    Interface number is 1
    Interface config status is active
    Interface state is active
Interface Internal-Data0/0 "", is up, line protocol is up
  Hardware is i82547GI rev00, BW 1000 Mbps
    (Full-duplex), (1000 Mbps)
    MAC address 0000.0001.0002, MTU not set
    IP address unassigned
    6 packets input, 1094 bytes, 0 no buffer
    Received 6 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 L2 decode drops, 0 demux drops
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions
    0 late collisions, 0 deferred
    input queue (curr/max blocks): hardware (0/2) software (0/0)
    output queue (curr/max blocks): hardware (0/0) software (0/0)
  Control Point Interface States:
    Interface number is unassigned
...
```

表 26-7 に、`show interface detail` コマンドの各フィールドの説明を示します。`show interface` コマンドで表示されるフィールドについては、表 26-5 を参照してください。

表 26-7 show interface detail のフィールド

フィールド	説明
Demux drops	(内部データ インターフェイスのみ) SSM インターフェイスからのパケットをセキュリティ アプライアンスが逆多重化できなかったために、ドロップされたパケットの数。SSM インターフェイスは、バックプレーンを経由してネイティブ インターフェイスと通信し、どの SSM インターフェイスからのパケットもバックプレーン上で多重化されます。
Control Point Interface States:	
Interface number	このインターフェイスが作成された順序を示す、デバッグに使用される番号。0 から開始されます。
Interface config status	管理状態。次のいずれかです。 <ul style="list-style-type: none"> <li>• active : インターフェイスはシャットダウンされていません。</li> <li>• not active : インターフェイスは <b>shutdown</b> コマンドでシャットダウンされています。</li> </ul>
Interface state	インターフェイスの実際の状態。ほとんどの場合、この状態は上の config status と一致しています。ハイ アベイラビリティを設定した場合には、セキュリティ アプライアンスは必要に応じてインターフェイスを起動またはシャットダウンするため、一致しない場合があります。
Asymmetrical Routing Statistics:	
Received X1 packets	このインターフェイスで受信された ASR パケット数。
Transmitted X2 packets	このインターフェイスで送信された ASR パケット数。
Dropped X3 packets	このインターフェイスでドロップされた ASR パケット数。パケットがドロップされるのは、パケットを転送しようとしたときにインターフェイスがダウンしている場合です。

#### 関連コマンド

コマンド	説明
<code>allocate-interface</code>	セキュリティ コンテキストにインターフェイスおよびサブインターフェイスを割り当てます。
<code>clear interface</code>	<code>show interface</code> コマンドのカウンタを消去します。
<code>interface</code>	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に入ります。
<code>nameif</code>	インターフェイス名を設定します。
<code>show interface ip brief</code>	インターフェイスの IP アドレスとステータスを表示します。

## show interface ip brief

インターフェイスの IP アドレスとステータスを表示するには、特権 EXEC モードで **show interface ip brief** コマンドを使用します。

```
show interface [physical_interface[.subinterface] | mapped_name | interface_name | vlan number] ip
brief
```

### シンタックスの説明

<i>interface_name</i>	(オプション) <b>nameif</b> コマンドで設定したインターフェイス名を指定します。
<i>mapped_name</i>	(オプション) マルチ コンテキスト モードで、マッピング名を <b>allocate-interface</b> コマンドを使用して割り当てた場合、その名前を指定します。
<i>physical_interface</i>	(オプション) インターフェイス ID ( <b>gigabitethernet0/1</b> など) を指定します。使用できる値については、 <b>interface</b> コマンドを参照してください。
<i>subinterface</i>	(オプション) 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。
<i>vlan number</i>	(オプション) 組み込みスイッチを持つ ASA 5505 適応型セキュリティ アプライアンスなどのモデルに対して、VLAN インターフェイスを指定します。

### デフォルト

インターフェイスを指定しない場合、セキュリティ アプライアンスはすべてのインターフェイスを表示します。

### 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	透過 <sup>1</sup>	シングル	マルチ コンテキスト	システム
特権 EXEC	•	•	•	•	—

1. Management 0/0 インターフェイスまたはサブインターフェイスに対してのみ使用可能。

### コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	このコマンドに、VLAN インターフェイスのサポート、および Management 0/0 インターフェイスまたはサブインターフェイスのサポート (透過モード) が追加されました。

### 使用上のガイドライン

マルチ コンテキスト モードで、**allocate-interface** コマンドを使用してインターフェイス ID をマッピングした場合、そのマッピング名またはインターフェイス名はコンテキスト内でのみ指定できます。

表示される出力については、「例」の項を参照してください。

## 例

次に、**show interface ip brief** コマンドの出力例を示します。

```
hostname# show interface ip brief
Interface                IP-Address      OK? Method  Status
Protocol
Control0/0               127.0.1.1      YES CONFIG  up          up
GigabitEthernet0/0      209.165.200.226 YES CONFIG  up          up
GigabitEthernet0/1      unassigned     YES unset   administratively down down
GigabitEthernet0/2      10.1.1.50      YES manual  administratively down down
GigabitEthernet0/3      192.168.2.6    YES DHCP   administratively down down
Management0/0           209.165.201.3  YES CONFIG  up          up
```

表 26-8 に、各フィールドの説明を示します。

表 26-8 show interface ip brief のフィールド

フィールド	説明
Interface	インターフェイス ID。マルチ コンテキスト モードで、 <b>allocate-interface</b> コマンドを使用してマッピング名を設定した場合は、その名前。すべてのインターフェイスを表示する場合、AIP SSM 用の内部インターフェイスが ASA 適応型セキュリティ アプライアンスにインストールされているときは、それらのインターフェイスに関する情報も表示されます。内部インターフェイスは、ユーザが設定することはできません。この情報は、デバッグのみを目的としたものです。
IP-Address	インターフェイスの IP アドレス。
OK?	このカラムは、現在は使用されていません。常に「Yes」が表示されます。
Method	インターフェイスが IP アドレスを受信したときの方法。値には、次のものがあります。 <ul style="list-style-type: none"> <li>unset : IP アドレスが設定されていません。</li> <li>manual : 実行コンフィギュレーションを設定しました。</li> <li>CONFIG : スタートアップ コンフィギュレーションからロードしました。</li> <li>DHCP : DHCP サーバから受信しました。</li> </ul>
Status	管理状態。次のいずれかです。 <ul style="list-style-type: none"> <li>up : インターフェイスはシャットダウンされていません。</li> <li>administratively down : インターフェイスは <b>shutdown</b> コマンドでシャットダウンされています。</li> </ul>
Protocol	回線の状態。次のいずれかです。 <ul style="list-style-type: none"> <li>up : 使用しているケーブルがネットワーク インターフェイスに接続されています。</li> <li>down : ケーブルが誤っているか、インターフェイス コネクタに接続されていません。</li> </ul>

## 関連コマンド

コマンド	説明
<b>allocate-interface</b>	セキュリティ コンテキストにインターフェイスおよびサブインターフェイスを割り当てます。
<b>interface</b>	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
<b>ip address</b>	インターフェイスの IP アドレスを設定します。または、透過ファイアウォールの管理 IP アドレスを設定します。
<b>nameif</b>	インターフェイス名を設定します。
<b>show interface</b>	インターフェイスのランタイム ステータスと統計情報を表示します。

# show inventory

ネットワーク デバイスにインストールされ、製品 ID (PID)、バージョン ID (VID)、シリアル番号 (SN) を割り当てられているすべてのシスコ製品に関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show inventory** コマンドを使用します。シスコ エンティティに PID が割り当てられていない場合、そのエンティティは取得されず、表示されません。

**show inventory [slot]**

## シンタックスの説明

**slot** (オプション) SSM スロット番号を指定します (システムはスロット 0)。

## デフォルト

インベントリを表示するスロットを指定しない場合は、次のように処理されます。

- 電源を含めて、すべての SSM のインベントリ情報が表示されます。

## 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	透過	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	•	•	—	—	•

## コマンド履歴

リリース	変更内容
7.0(1)	セマンティックの小さな変更。

## 使用上のガイドライン

**show inventory** コマンドは、各シスコ製品のインベントリ情報を UDI 形式で取得し、表示します。UDI は、製品 ID (PID)、バージョン ID (VID)、シリアル番号 (SN) という 3 つの別個のデータ要素を結合したものです。

PID は、製品をご注文いただく際の名称で、従来は「製品名」または「製品番号」と呼ばれていたものです。これは、交換部品を間違いなくご注文いただくために使用する識別子です。

VID は、製品のバージョンです。製品が改良されると、VID が増分します。VID は、製品変更通知 (PCN) について規定した業界ガイドラインである Telcordia GR-209-CORE に基づいた、厳格なプロセスに従って増分されます。

SN は、製品に対するベンダー独自の連続番号です。製造される各製品は、製造時に割り当てられる一意のシリアル番号を保持しており、この番号は現場では変更できません。この番号は、製品の特定のインスタンスを個々に識別するための手段です。

UDI では、各製品をエンティティと呼びます。シャーシなどの一部のエンティティは、スロットなどの下位エンティティを保持しています。各エンティティは、シスコ エンティティ別に階層構造で整理された論理的な表示順に従って、1 行に 1 つずつ表示されます。

**show inventory** コマンドをオプションなしで使用すると、ネットワーク デバイスにインストールされた、PID を割り当てられているシスコ エンティティのリストが表示されます。



**例** 次に、キーワードと引数を指定しない場合の **show inventory** コマンドの出力例を示します。この出力例では、ルータにインストールされた、PID を割り当てられているシスコ エンティティのリストが表示されています。

```
ciscoasa# show inventory
Name:"Chassis", DESCR:"ASA 5540 Adaptive Security Appliance"
PID:ASA5540          , VID:V01 , SN:P3000000998

Name:"slot 1", DESCR:"ASA 5500 Series Security Services Module-20"
PID:ASA-SSM-20      , VID:V01 , SN:P0000000999

Name:"power supply", DESCR:"ASA 5500 Series 180W AC Power Supply"
PID:ASA-180W-PWR-AC , VID:V01 , SN:123456789AB

ciscoasa# show inventory 0
Name:"Chassis", DESCR:"ASA 5540 Adaptive Security Appliance"
PID:ASA5540          , VID:V01 , SN:P3000000998

ciscoasa# show inventory 1
Name:"slot 1", DESCR:"ASA 5500 Series Security Services Module-20"
PID:ASA-SSM-20      , VID:V01 , SN:P0000000999
```

表 26-9 は、この出力に表示されるフィールドについて説明しています。

**表 26-9 show inventory のフィールドの説明**

フィールド	説明
Name	シスコ エンティティに割り当てられている物理名 (テキスト文字列)。たとえば、デバイスの物理コンポーネント名前付けシンタックスに基づいた、「1」などのコンソール番号または単純なコンポーネント番号 (ポート番号やモジュール番号) です。RFC 2737 の entPhysicalName MIB 変数に相当します。
DESCR	オブジェクトの特徴を示す、シスコ エンティティの物理的な説明。RFC 2737 の entPhysicalDesc MIB 変数に相当します。
PID	エンティティの製品 ID。RFC 2737 の entPhysicalModuleName MIB 変数に相当します。
VID	エンティティのバージョン ID。RFC 2737 の entPhysicalHardwareRev MIB 変数に相当します。
SN	製品のシリアル番号。RFC 2737 の entPhysicalSerialNum MIB 変数に相当します。

#### 関連コマンド

コマンド	説明
<b>show diag</b>	ネットワーク デバイスについて、コントローラ、インターフェイス プロセッサ、ポート アダプタの診断情報を表示します。
<b>show tech-support</b>	ルータが問題を報告したときに、ルータに関する一般情報を表示します。

## show ip address

インターフェイスの IP アドレスまたは透過モードの管理 IP アドレスを表示するには、特権 EXEC モードで **show ip address** コマンドを使用します。

```
show ip address [physical_interface[.subinterface]] | mapped_name | interface_name | vlan number]
```

### シンタックスの説明

<i>interface_name</i>	(オプション) <b>nameif</b> コマンドで設定したインターフェイス名を指定します。
<i>mapped_name</i>	(オプション) マルチ コンテキスト モードで、マッピング名を <b>allocate-interface</b> コマンドを使用して割り当てた場合、その名前を指定します。
<i>physical_interface</i>	(オプション) インターフェイス ID ( <b>gigabitethernet0/1</b> など) を指定します。使用できる値については、 <b>interface</b> コマンドを参照してください。
<i>subinterface</i>	(オプション) 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。
<i>vlan number</i>	(オプション) 組み込みスイッチを持つ ASA 5505 適応型セキュリティ アプライアンスなどのモデルに対して、VLAN インターフェイスを指定します。

### デフォルト

インターフェイスを指定しない場合、セキュリティ アプライアンスはすべてのインターフェイスの IP アドレスを表示します。

### 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	透過	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
7.2(1)	このコマンドに VLAN インターフェイスのサポートが追加されました。

### 使用上のガイドライン

ハイ アベイラビリティを設定した場合は、現在の IP アドレスと共にプライマリ IP アドレス (表示には「System」と示されます) が表示されます。装置がアクティブになっている場合、システム IP アドレスと現在の IP アドレスは一致します。装置がスタンバイになっている場合、現在の IP アドレスにはスタンバイ アドレスが表示されます。

## 例

次に、**show ip address** コマンドの出力例を示します。

```
hostname# show ip address
System IP Addresses:
Interface          Name          IP address      Subnet mask      Method
GigabitEthernet0/0 mgmt          10.7.12.100     255.255.255.0    CONFIG
GigabitEthernet0/1 inside        10.1.1.100      255.255.255.0    CONFIG
GigabitEthernet0/2.40 outside      209.165.201.2   255.255.255.224  DHCP
GigabitEthernet0/3 dmz          209.165.200.225 255.255.255.224  manual
Current IP Addresses:
Interface          Name          IP address      Subnet mask      Method
GigabitEthernet0/0 mgmt          10.7.12.100     255.255.255.0    CONFIG
GigabitEthernet0/1 inside        10.1.1.100      255.255.255.0    CONFIG
GigabitEthernet0/2.40 outside      209.165.201.2   255.255.255.224  DHCP
GigabitEthernet0/3 dmz          209.165.200.225 255.255.255.224  manual
```

表 26-10 に、各フィールドの説明を示します。

表 26-10 show ip address のフィールド

フィールド	説明
Interface	インターフェイス ID。マルチ コンテキスト モードで、 <b>allocate-interface</b> コマンドを使用してマッピング名を設定した場合は、その名前。
Name	<b>nameif</b> コマンドで設定したインターフェイス名。
IP address	インターフェイスの IP アドレス。
Subnet mask	IP アドレスとサブネット マスク。
Method	インターフェイスが IP アドレスを受信したときの方法。値には、次のものがあります。 <ul style="list-style-type: none"> <li>unset : IP アドレスが設定されていません。</li> <li>manual : 実行コンフィギュレーションを設定しました。</li> <li>CONFIG : スタートアップ コンフィギュレーションからロードしました。</li> <li>DHCP : DHCP サーバから受信しました。</li> </ul>

## 関連コマンド

コマンド	説明
<b>allocate-interface</b>	セキュリティ コンテキストにインターフェイスおよびサブインターフェイスを割り当てます。
<b>interface</b>	インターフェイスを設定し、インターフェイス コンフィギュレーションモードに入ります。
<b>nameif</b>	インターフェイス名を設定します。
<b>show interface</b>	インターフェイスのランタイム ステータスと統計情報を表示します。
<b>show interface ip brief</b>	インターフェイスの IP アドレスとステータスを表示します。

# show ip address dhcp

インターフェイスの DHCP リースまたは DHCP サーバに関する詳細情報を表示するには、特権 EXEC モードで **show ip address dhcp** コマンドを使用します。

```
show ip address {physical_interface[.subinterface] | mapped_name | interface_name} dhcp {lease | server}
```

## シンタックスの説明

<i>interface_name</i>	<b>nameif</b> コマンドで設定したインターフェイス名を指定します。
<i>lease</i>	DHCP リースに関する情報を表示します。
<i>mapped_name</i>	マルチ コンテキスト モードで、マッピング名を <b>allocate-interface</b> コマンドを使用して割り当てた場合、その名前を指定します。
<i>physical_interface</i>	インターフェイス ID ( <b>gigabitethernet0/1</b> など) を指定します。使用できる値については、 <b>interface</b> コマンドを参照してください。
<i>server</i>	DHCP サーバに関する情報を表示します。
<i>subinterface</i>	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	透過 <sup>1</sup>	シングル	マルチ コンテキスト	システム
特権 EXEC	•	•	•	•	—

1. Management 0/0 インターフェイスまたはサブインターフェイスに対してのみ使用可能。

## コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、新しいサーバ機能に対応するための <b>lease</b> キーワードと <b>server</b> キーワードを含むように変更されました。
7.2(1)	このコマンドに、VLAN インターフェイスのサポート、および Management 0/0 インターフェイスまたはサブインターフェイスのサポート（透過モード）が追加されました。

## 使用上のガイドライン

表示される出力については、「例」の項を参照してください。

## 例

次に、`show ip address dhcp lease` コマンドの出力例を示します。

```
hostname# show ip address outside dhcp lease
Temp IP Addr:209.165.201.57 for peer on interface:outside
Temp sub net mask:255.255.255.224
  DHCP Lease server:209.165.200.225, state:3 Bound
  DHCP Transaction id:0x4123
  Lease:259200 secs, Renewal:129600 secs, Rebind:226800 secs
  Temp default-gateway addr:209.165.201.1
  Temp ip static route0: dest 10.9.0.0 router 10.7.12.255
  Next timer fires after:111797 secs
  Retry count:0, Client-ID:cisco-0000.0000.0000-outside
  Proxy: TRUE Proxy Network: 10.1.1.1
  Hostname: device1
```

表 26-11 に、各フィールドの説明を示します。

表 26-11 show ip address dhcp lease のフィールド

フィールド	説明
Temp IP Addr	インターフェイスに割り当てられている IP アドレス。
Temp sub net mask	インターフェイスに割り当てられているサブネットマスク。
DHCP Lease server	DHCP サーバのアドレス。
state	DHCP リースの状態。次のいずれかです。 <ul style="list-style-type: none"> <li>• <b>Initial</b> : 初期化状態。セキュリティ アプライアンスがリース取得プロセスを開始します。この状態は、リースが終了したときとリースのネゴシエーションが失敗したときも表示されます。</li> <li>• <b>Selecting</b> : セキュリティ アプライアンスは、1 つまたはそれ以上の DHCP サーバから DHCP OFFER メッセージを受信して、いずれかを選択できる状態になるのを待っています。</li> <li>• <b>Requesting</b> : セキュリティ アプライアンスは、要求の送信先となったサーバからの応答を待っています。</li> <li>• <b>Purging</b> : セキュリティ アプライアンスは、クライアントが IP アドレスを解放したか、その他の何らかのエラーが発生したために、リースを削除しています。</li> <li>• <b>Bound</b> : セキュリティ アプライアンスは有効なリースを保持し、正常に動作しています。</li> <li>• <b>Renewing</b> : セキュリティ アプライアンスは、リースを更新しようとしています。DHCP REQUEST メッセージを現在の DHCP サーバに定期的送信して、応答を待ちます。</li> <li>• <b>Rebinding</b> : セキュリティ アプライアンスは元のサーバとの間でリースの更新に失敗したため、いずれかのサーバから応答があるか、リースが終了するまで DHCP REQUEST メッセージを送信します。</li> <li>• <b>Holddown</b> : セキュリティ アプライアンスは、リースを削除するプロセスを開始しました。</li> <li>• <b>Releasing</b> : セキュリティ アプライアンスは、IP アドレスが不要になったことを示す解放メッセージをサーバに送信します。</li> </ul>
DHCP transaction id	クライアントが選択したランダムな数値。要求メッセージに関連付けるためにクライアントとサーバが使用します。
Lease	DHCP サーバが指定した、インターフェイスがこの IP アドレスを使用できる期間。

表 26-11 show ip address dhcp lease のフィールド (続き)

フィールド	説明
Renewal	インターフェイスがこのリースを自動的に更新しようとするまでの期間。
Rebind	セキュリティ アプライアンスが DHCP サーバに再バインドしようとするまでの期間。再バインドが発生するのは、セキュリティ アプライアンスが元の DHCP サーバと通信できないまま、リース期間の 87.5% が経過した場合です。この場合、セキュリティ アプライアンスは DHCP 要求をブロードキャストして、使用可能ないずれかの DHCP サーバと通信しようとします。
Temp default-gateway addr	DHCP サーバが提供したデフォルト ゲートウェイ アドレス。
Temp ip static route0	デフォルトのスタティック ルート。
Next timer fires after	内部タイマーが始動するまでの秒数。
Retry count	セキュリティ アプライアンスがリースを確立しようとしている場合、このフィールドはセキュリティ アプライアンスが DHCP メッセージの送信を試行した回数を示しています。たとえば、セキュリティ アプライアンスが <b>Selecting</b> 状態になっている場合、この値はセキュリティ アプライアンスが検出メッセージを送信した回数を示しています。セキュリティ アプライアンスが <b>Requesting</b> 状態になっている場合は、セキュリティ アプライアンスが要求メッセージを送信した回数を示しています。
Client-ID	サーバとのすべての通信で使用されるクライアント ID。
Proxy	このインターフェイスが、VPN クライアントのプロキシ DHCP クライアントであるかどうかを示します (True または False)。
Proxy Network	要求されたネットワーク。
Hostname	クライアントのホスト名。

次に、**show ip address dhcp server** コマンドの出力例を示します。

```
hostname# show ip address outside dhcp server

DHCP server: ANY (255.255.255.255)
Leases: 0
Offers: 0      Requests: 0      Acks: 0      Naks: 0
Declines: 0    Releases: 0      Bad: 0

DHCP server: 40.7.12.6
Leases: 1
Offers: 1      Requests: 17     Acks: 17     Naks: 0
Declines: 0    Releases: 0      Bad: 0
DNS0: 171.69.161.23,  DNS1: 171.69.161.24
WINS0: 172.69.161.23,  WINS1: 172.69.161.23
Subnet: 255.255.0.0   DNS Domain: cisco.com
```

表 26-12 に、各フィールドの説明を示します。

表 26-12 show ip address dhcp server のフィールド

フィールド	説明
DHCP server	このインターフェイスがリースを取得した DHCP サーバのアドレス。最初のエントリ（「ANY」）はデフォルトサーバで、常に表示されます。
Leases	サーバから取得したリースの数。インターフェイスの場合、リースの数は通常は 1 です。VPN のプロキシとして動作しているインターフェイスに対してサーバがアドレスを提供している場合は、リースが複数になります。
Offers	サーバからのオファーの数。
Requests	サーバに送信した要求の数。
Acks	サーバから受信した確認応答の数。
Naks	サーバから受信した否定応答の数。
Declines	サーバから受信した辞退の数。
Releases	サーバに送信したリリースの数。
Bad	サーバから受信した不良パケットの数。
DNS0	DHCP サーバから取得したプライマリ DNS サーバアドレス。
DNS1	DHCP サーバから取得したセカンダリ DNS サーバアドレス。
WINS0	DHCP サーバから取得したプライマリ WINS サーバアドレス。
WINS1	DHCP サーバから取得したセカンダリ WINS サーバアドレス。
Subnet	DHCP サーバから取得したサブネットアドレス。
DNS Domain	DHCP サーバから取得したドメイン。

#### 関連コマンド

コマンド	説明
<b>interface</b>	インターフェイスを設定し、インターフェイス コンフィギュレーションモードに入ります。
<b>ip address dhcp</b>	DHCP サーバから IP アドレスを取得するようにインターフェイスを設定します。
<b>nameif</b>	インターフェイス名を設定します。
<b>show interface ip brief</b>	インターフェイスの IP アドレスとステータスを表示します。
<b>show ip address</b>	インターフェイスの IP アドレスを表示します。

## show ip address pppoe

PPPoE 接続に関する詳細情報を表示するには、特権 EXEC モードで **show ip address pppoe** コマンドを実行します。

```
show ip address {physical_interface[,subinterface] | mapped_name | interface_name | vlan number}
pppoe
```

### シンタックスの説明

<i>interface_name</i>	<b>nameif</b> コマンドで設定したインターフェイス名を指定します。
<i>mapped_name</i>	マルチ コンテキスト モードで、マッピング名を <b>allocate-interface</b> コマンドを使用して割り当てた場合、その名前を指定します。
<i>physical_interface</i>	インターフェイス ID ( <b>gigabitethernet0/1</b> など) を指定します。使用できる値については、 <b>interface</b> コマンドを参照してください。
<i>subinterface</i>	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。
<i>vlan number</i>	(オプション) 組み込みスイッチを持つ ASA 5505 適応型セキュリティ アプライアンスなどのモデルに対して、VLAN インターフェイスを指定します。

### 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	透過 <sup>1</sup>	シングル	マルチ コンテキスト	システム
特権 EXEC	•	•	•	•	—

1. Management 0/0 インターフェイスまたはサブインターフェイスに対してのみ使用可能。

### コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

### 使用上のガイドライン

表示される出力については、「例」の項を参照してください。

### 例

次に、**show ip address pppoe** コマンドの出力例を示します。

```
hostname# show ip address outside pppoe
```



表 26-13 に、各フィールドの説明を示します。

表 26-13 show ip address dhcp lease のフィールド

フィールド	説明
	•

#### 関連コマンド

コマンド	説明
<b>interface</b>	インターフェイスを設定し、インターフェイス コンフィギュレーションモードに入ります。
<b>ip address pppoe</b>	PPPoE サーバから IP アドレスを取得するようにインターフェイスを設定します。
<b>nameif</b>	インターフェイス名を設定します。
<b>show interface ip brief</b>	インターフェイスの IP アドレスとステータスを表示します。
<b>show ip address</b>	インターフェイスの IP アドレスを表示します。

## show ip audit count

インターフェイスに監査ポリシーを適用した場合に、一致したシグニチャの数を表示するには、特権 EXEC モードで **show ip audit count** コマンドを使用します。

```
show ip audit count [global | interface interface_name
```

### シンタックスの説明

<b>global</b>	(デフォルト) すべてのインターフェイスについて、一致した件数を表示します。
<b>interface interface_name</b>	(オプション) 指定したインターフェイスについて、一致した件数を表示します。

### デフォルト

キーワードを指定しない場合は、すべてのインターフェイスについて一致件数が表示されます (*global*)。

### 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	透過	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
既存	このコマンドは既存のものです。

### 使用上のガイドライン

監査ポリシーを作成するには **ip audit name** コマンドを使用し、ポリシーを適用するには **ip audit interface** コマンドを使用します。

例 次に、**show ip audit count** コマンドの出力例を示します。

```
hostname# show ip audit count
IP AUDIT GLOBAL COUNTERS

1000 I Bad IP Options List          0
1001 I Record Packet Route          0
1002 I Timestamp                    0
1003 I Provide s,c,h,tcc            0
1004 I Loose Source Route           0
1005 I SATNET ID                    0
1006 I Strict Source Route          0
1100 A IP Fragment Attack           0
1102 A Impossible IP Packet        0
1103 A IP Teardrop                  0
2000 I ICMP Echo Reply              0
2001 I ICMP Unreachable             0
2002 I ICMP Source Quench          0
2003 I ICMP Redirect                0
2004 I ICMP Echo Request            10
2005 I ICMP Time Exceed             0
2006 I ICMP Parameter Problem      0
2007 I ICMP Time Request            0
2008 I ICMP Time Reply              0
2009 I ICMP Info Request            0
2010 I ICMP Info Reply              0
2011 I ICMP Address Mask Request    0
2012 I ICMP Address Mask Reply      0
2150 A Fragmented ICMP              0
2151 A Large ICMP                   0
2154 A Ping of Death                0
3040 A TCP No Flags                 0
3041 A TCP SYN & FIN Flags Only     0
3042 A TCP FIN Flag Only            0
3153 A FTP Improper Address         0
3154 A FTP Improper Port            0
4050 A Bomb                          0
4051 A Snork                         0
4052 A Chargen                       0
6050 A DNS Host Info                 0
6051 A DNS Zone Xfer                 0
6052 A DNS Zone Xfer High Port      0
6053 A DNS All Records               0
6100 I RPC Port Registration         0
6101 I RPC Port Unregistration       0
6102 I RPC Dump                      0
6103 A Proxied RPC                   0
6150 I ypserv Portmap Request        0
6151 I ypbind Portmap Request        0
6152 I yppasswdd Portmap Request     0
6153 I ypserv Portmap Request        0
6154 I ypxfrd Portmap Request        0
6155 I mountd Portmap Request        0
6175 I rexd Portmap Request          0
6180 I rexd Attempt                  0
6190 A statd Buffer Overflow         0

IP AUDIT INTERFACE COUNTERS: inside
...
```

## 関連コマンド

コマンド	説明
<code>clear ip audit count</code>	監査ポリシーのシグニチャー致件数を消去します。
<code>ip audit interface</code>	インターフェイスに監査ポリシーを割り当てます。
<code>ip audit name</code>	パケットが攻撃シグニチャーまたは情報シグニチャー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。
<code>show running-config ip audit attack</code>	<code>ip audit attack</code> コマンドのコンフィギュレーションを表示します。

# show ip verify statistics

Unicast RPF 機能によってドロップされたパケットの数を表示するには、特権 EXEC モードで **show ip verify statistics** コマンドを使用します。Unicast RPF をイネーブルにするには、**ip verify reverse-path** コマンドを使用します。

```
show ip verify statistics [interface interface_name]
```

<b>シンタックスの説明</b>	<i>interface</i>	(オプション) 指定したインターフェイスに関する統計情報を表示します。
	<i>interface_name</i>	

**デフォルト** このコマンドは、すべてのインターフェイスに関する統計情報を表示します。

**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	透過	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
	既存	このコマンドは既存のものです。

**例** 次に、**show ip verify statistics** コマンドの出力例を示します。

```
hostname# show ip verify statistics
interface outside: 2 unicast rpf drops
interface inside: 1 unicast rpf drops
interface intf2: 3 unicast rpf drops
```

関連コマンド	コマンド	説明
	<b>clear configure ip verify reverse-path</b>	<b>ip verify reverse-path</b> コンフィギュレーションを消去します。
	<b>clear ip verify statistics</b>	Unicast RPF の統計情報を消去します。
	<b>ip verify reverse-path</b>	Unicast Reverse Path Forwarding 機能をイネーブルにして IP スプーフィングを防止します。
	<b>show running-config ip verify reverse-path</b>	<b>ip verify reverse-path</b> コンフィギュレーションを表示します。

## show ipsec sa

IPSec SA のリストを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show ipsec sa** コマンドを使用します。このコマンドの別の形式である、**show crypto ipsec sa** を使用することもできます。

```
show ipsec sa [entry | identity | map map-name | peer peer-addr] [detail]
```

### シンタックスの説明

<i>detail</i>	(オプション) 表示対象に関する詳細なエラー情報を表示します。
<i>entry</i>	(オプション) IPSec SA をピアアドレスでソートして表示します。
<i>identity</i>	(オプション) IPSec SA を ID でソートして、ESP を除いて表示します。これは圧縮された形式です。
<i>map map-name</i>	(オプション) 指定した暗号マップの IPSec SA を表示します。
<i>peer peer-addr</i>	(オプション) 指定したピア IP アドレスの IPSec SA を表示します。

### 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	透過	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	•	•	•	—	—
特権 EXEC	•	•	•	—	—

### コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

**例** グローバル コンフィギュレーション モードで入力した次の例では、IPSec SA を表示しています。

```
hostname(config)# show ipsec sa
interface: outside2
  Crypto map tag: def, local addr: 10.132.0.17

  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (172.20.0.21/255.255.255.255/0/0)
  current_peer: 172.20.0.21
  dynamic allocated peer ip: 10.135.1.5

  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
  #pkts decaps: 1145, #pkts decrypt: 1145, #pkts verify: 1145
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
  #pre-frag successes: 2, #pre-frag failures: 1, #fragments created: 10
  #PMTUs sent: 5, #PMTUs rcvd: 2, #decapstulated frags needing reassembly: 1
  #send errors: 0, #recv errors: 0

  local crypto endpt.: 10.132.0.17, remote crypto endpt.: 172.20.0.21

  path mtu 1500, ipsec overhead 60, media mtu 1500
  current outbound spi: DC15BF68

inbound esp sas:
  spi: 0x1E8246FC (511854332)
    transform: esp-3des esp-md5-hmac
    in use settings ={RA, Tunnel, }
    slot: 0, conn_id: 3, crypto-map: def
    sa timing: remaining key lifetime (sec): 548
    IV size: 8 bytes
    replay detection support: Y
outbound esp sas:
  spi: 0xDC15BF68 (3692412776)
    transform: esp-3des esp-md5-hmac
    in use settings ={RA, Tunnel, }
    slot: 0, conn_id: 3, crypto-map: def
    sa timing: remaining key lifetime (sec): 548
    IV size: 8 bytes
    replay detection support: Y

Crypto map tag: def, local addr: 10.132.0.17

  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
hostname(config)#
```



**(注)**

断片化の統計は、IPSec 処理前に断片化が発生することを IPSec SA ポリシーが記述している場合は、断片化前の統計になります。断片化後の統計は、IPSec 処理後に断片化が発生することを SA ポリシーが記述している場合に表示されます。

グローバル コンフィギュレーション モードで入力した次の例では、def という暗号マップの IPSec SA を表示しています。

```

hostname(config)# show ipsec sa map def
cryptomap: def
  Crypto map tag: def, local addr: 172.20.0.17

  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
  current_peer: 10.132.0.21
  dynamic allocated peer ip: 90.135.1.5

  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
  #pkts decaps: 1146, #pkts decrypt: 1146, #pkts verify: 1146
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
  #send errors: 0, #recv errors: 0

  local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

  path mtu 1500, ipsec overhead 60, media mtu 1500
  current outbound spi: DC15BF68

inbound esp sas:
  spi: 0x1E8246FC (511854332)
    transform: esp-3des esp-md5-hmac
    in use settings ={RA, Tunnel, }
    slot: 0, conn_id: 3, crypto-map: def
    sa timing: remaining key lifetime (sec): 480
    IV size: 8 bytes
    replay detection support: Y
outbound esp sas:
  spi: 0xDC15BF68 (3692412776)
    transform: esp-3des esp-md5-hmac
    in use settings ={RA, Tunnel, }
    slot: 0, conn_id: 3, crypto-map: def
    sa timing: remaining key lifetime (sec): 480
    IV size: 8 bytes
    replay detection support: Y

Crypto map tag: def, local addr: 172.20.0.17

  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
  current_peer: 10.135.1.8
  dynamic allocated peer ip: 0.0.0.0

  #pkts encaps: 73672, #pkts encrypt: 73672, #pkts digest: 73672
  #pkts decaps: 78824, #pkts decrypt: 78824, #pkts verify: 78824
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 73672, #pkts comp failed: 0, #pkts decomp failed: 0
  #send errors: 0, #recv errors: 0

  local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

  path mtu 1500, ipsec overhead 60, media mtu 1500
  current outbound spi: 3B6F6A35

inbound esp sas:
  spi: 0xB32CF0BD (3006066877)
    transform: esp-3des esp-md5-hmac
    in use settings ={RA, Tunnel, }
    slot: 0, conn_id: 4, crypto-map: def
    sa timing: remaining key lifetime (sec): 263
    IV size: 8 bytes
    replay detection support: Y
outbound esp sas:
  spi: 0x3B6F6A35 (997157429)
    transform: esp-3des esp-md5-hmac

```



```

    in use settings ={RA, Tunnel, }
    slot: 0, conn_id: 4, crypto-map: def
    sa timing: remaining key lifetime (sec): 263
    IV size: 8 bytes
    replay detection support: Y
hostname(config)#

```

グローバル コンフィギュレーション モードで入力した次の例では、キーワード **entry** を指定して IPsec SA を表示しています。

```

hostname(config)# show ipsec sa entry
peer address: 10.132.0.21
  Crypto map tag: def, local addr: 172.20.0.17

    local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
    current_peer: 10.132.0.21
    dynamic allocated peer ip: 90.135.1.5

    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
    #send errors: 0, #recv errors: 0

    local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

    path mtu 1500, ipsec overhead 60, media mtu 1500
    current outbound spi: DC15BF68

inbound esp sas:
  spi: 0x1E8246FC (511854332)
    transform: esp-3des esp-md5-hmac
    in use settings ={RA, Tunnel, }
    slot: 0, conn_id: 3, crypto-map: def
    sa timing: remaining key lifetime (sec): 429
    IV size: 8 bytes
    replay detection support: Y
outbound esp sas:
  spi: 0xDC15BF68 (3692412776)
    transform: esp-3des esp-md5-hmac
    in use settings ={RA, Tunnel, }
    slot: 0, conn_id: 3, crypto-map: def
    sa timing: remaining key lifetime (sec): 429
    IV size: 8 bytes
    replay detection support: Y

peer address: 10.135.1.8
  Crypto map tag: def, local addr: 172.20.0.17

    local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
    current_peer: 10.135.1.8
    dynamic allocated peer ip: 0.0.0.0

    #pkts encaps: 73723, #pkts encrypt: 73723, #pkts digest: 73723
    #pkts decaps: 78878, #pkts decrypt: 78878, #pkts verify: 78878
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 73723, #pkts comp failed: 0, #pkts decomp failed: 0
    #send errors: 0, #recv errors: 0

    local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

    path mtu 1500, ipsec overhead 60, media mtu 1500
    current outbound spi: 3B6F6A35

```

```

inbound esp sas:
  spi: 0xB32CF0BD (3006066877)
  transform: esp-3des esp-md5-hmac
  in use settings ={RA, Tunnel, }
  slot: 0, conn_id: 4, crypto-map: def
  sa timing: remaining key lifetime (sec): 212
  IV size: 8 bytes
  replay detection support: Y
outbound esp sas:
  spi: 0x3B6F6A35 (997157429)
  transform: esp-3des esp-md5-hmac
  in use settings ={RA, Tunnel, }
  slot: 0, conn_id: 4, crypto-map: def
  sa timing: remaining key lifetime (sec): 212
  IV size: 8 bytes
  replay detection support: Y
hostname(config)#

```

グローバル コンフィギュレーション モードで入力した次の例では、キーワード *entry detail* を指定して IPSec SA を表示しています。

```

hostname(config)# show ipsec sa entry detail
peer address: 10.132.0.21
  Crypto map tag: def, local addr: 172.20.0.17

  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
  current_peer: 10.132.0.21
  dynamic allocated peer ip: 90.135.1.5

  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
  #pkts decaps: 1148, #pkts decrypt: 1148, #pkts verify: 1148
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
  #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
  #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
  #pkts invalid prot (rcv): 0, #pkts verify failed: 0
  #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
  #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
  #pkts replay failed (rcv): 0
  #pkts internal err (send): 0, #pkts internal err (rcv): 0

  local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

  path mtu 1500, ipsec overhead 60, media mtu 1500
  current outbound spi: DC15BF68

inbound esp sas:
  spi: 0x1E8246FC (511854332)
  transform: esp-3des esp-md5-hmac
  in use settings ={RA, Tunnel, }
  slot: 0, conn_id: 3, crypto-map: def
  sa timing: remaining key lifetime (sec): 322
  IV size: 8 bytes
  replay detection support: Y
outbound esp sas:
  spi: 0xDC15BF68 (3692412776)
  transform: esp-3des esp-md5-hmac
  in use settings ={RA, Tunnel, }
  slot: 0, conn_id: 3, crypto-map: def
  sa timing: remaining key lifetime (sec): 322
  IV size: 8 bytes
  replay detection support: Y

```

```
peer address: 10.135.1.8
Crypto map tag: def, local addr: 172.20.0.17

local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
current_peer: 10.135.1.8
dynamic allocated peer ip: 0.0.0.0

#pkts encaps: 73831, #pkts encrypt: 73831, #pkts digest: 73831
#pkts decaps: 78989, #pkts decrypt: 78989, #pkts verify: 78989
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 73831, #pkts comp failed: 0, #pkts decomp failed: 0
#pkts no sa (send): 0, #pkts invalid sa (rcv): 0
#pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
#pkts invalid prot (rcv): 0, #pkts verify failed: 0
#pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
#pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
#pkts replay failed (rcv): 0
#pkts internal err (send): 0, #pkts internal err (rcv): 0

local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

path mtu 1500, ipsec overhead 60, media mtu 1500
current outbound spi: 3B6F6A35

inbound esp sas:
spi: 0xB32CF0BD (3006066877)
transform: esp-3des esp-md5-hmac
in use settings ={RA, Tunnel, }
slot: 0, conn_id: 4, crypto-map: def
sa timing: remaining key lifetime (sec): 104
IV size: 8 bytes
replay detection support: Y
outbound esp sas:
spi: 0x3B6F6A35 (997157429)
transform: esp-3des esp-md5-hmac
in use settings ={RA, Tunnel, }
slot: 0, conn_id: 4, crypto-map: def
sa timing: remaining key lifetime (sec): 104
IV size: 8 bytes
replay detection support: Y
hostname(config)#
```

次の例では、キーワード *identity* を指定して IPsec SA を表示しています。

```
hostname(config)# show ipsec sa identity
interface: outside2
  Crypto map tag: def, local addr: 172.20.0.17

  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
  current_peer: 10.132.0.21
  dynamic allocated peer ip: 90.135.1.5

  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
  #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
  #send errors: 0, #recv errors: 0

  local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

  path mtu 1500, ipsec overhead 60, media mtu 1500
  current outbound spi: DC15BF68

Crypto map tag: def, local addr: 172.20.0.17

  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
  current_peer: 10.135.1.8
  dynamic allocated peer ip: 0.0.0.0

  #pkts encaps: 73756, #pkts encrypt: 73756, #pkts digest: 73756
  #pkts decaps: 78911, #pkts decrypt: 78911, #pkts verify: 78911
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 73756, #pkts comp failed: 0, #pkts decomp failed: 0
  #send errors: 0, #recv errors: 0

  local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

  path mtu 1500, ipsec overhead 60, media mtu 1500
  current outbound spi: 3B6F6A35
```

次の例では、キーワード *identity* と *detail* を指定して IPsec SA を表示しています。

```
hostname(config)# show ipsec sa identity detail
interface: outside2
  Crypto map tag: def, local addr: 172.20.0.17

  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
  current_peer: 10.132.0.21
  dynamic allocated peer ip: 90.135.1.5

  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
  #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
  #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
  #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
  #pkts invalid prot (rcv): 0, #pkts verify failed: 0
  #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
  #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
  #pkts replay failed (rcv): 0
  #pkts internal err (send): 0, #pkts internal err (rcv): 0

  local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

  path mtu 1500, ipsec overhead 60, media mtu 1500
  current outbound spi: DC15BF68

Crypto map tag: def, local addr: 172.20.0.17

  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
  current_peer: 10.135.1.8
  dynamic allocated peer ip: 0.0.0.0

  #pkts encaps: 73771, #pkts encrypt: 73771, #pkts digest: 73771
  #pkts decaps: 78926, #pkts decrypt: 78926, #pkts verify: 78926
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 73771, #pkts comp failed: 0, #pkts decomp failed: 0
  #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
  #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
  #pkts invalid prot (rcv): 0, #pkts verify failed: 0
  #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
  #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
  #pkts replay failed (rcv): 0
  #pkts internal err (send): 0, #pkts internal err (rcv): 0

  local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

  path mtu 1500, ipsec overhead 60, media mtu 1500
  current outbound spi: 3B6F6A35
```

## 関連コマンド

コマンド	説明
<b>clear configure isakmp</b>	すべての ISAKMP コンフィギュレーションを消去します。
<b>clear configure isakmp policy</b>	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
<b>clear isakmp sa</b>	IKE ランタイム SA データベースを消去します。
<b>isakmp enable</b>	IPsec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
<b>show running-config isakmp</b>	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

# show ipsec sa summary

IPSec SA の要約を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show ipsec sa summary** コマンドを使用します。

```
show ipsec sa summary
```

**シンタックスの説明** このコマンドには、引数も変数もありません。

**デフォルト** デフォルトの動作や値はありません。

**コマンドモード** 次の表は、このコマンドを入力できるモードを示しています。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	透過	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	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴	リリース	変更内容
	7.0(1)	このコマンドが導入されました。

**例** グローバル コンフィギュレーション モードで入力した次の例では、次の接続タイプごとに IPSec SA の要約を表示しています。

- IPSec
- IPSec over UDP
- IPSec over NAT-T
- IPSec over TCP
- IPSec VPN ロードバランシング

```
hostname(config)# show ipsec sa summary
```

```
Current IPSec SA's:          Peak IPSec SA's:
IPSec                       :    2          Peak Concurrent SA   :   14
IPSec over UDP              :    2          Peak Concurrent L2L  :    0
IPSec over NAT-T           :    4          Peak Concurrent RA   :   14
IPSec over TCP              :    6
IPSec VPN LB                :    0
Total                       :   14
hostname(config)#
```

関連コマンド	コマンド	説明
	<b>clear ipsec sa</b>	IPSec SA 全体を削除します。または、指定したパラメータに基づいて削除します。
	<b>show ipsec sa</b>	IPSec SA のリストを表示します。
	<b>show ipsec stats</b>	IPSec に関する一連の統計情報を表示します。

# show ipsec stats

一連の IPSec 統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show ipsec stats** コマンドを使用します。

**show ipsec stats**

**シンタックスの説明** このコマンドには、キーワードも変数もありません。

**デフォルト** デフォルトの動作や値はありません。

**コマンド モード** 次の表は、このコマンドを入力できるモードを示しています。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	透過	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	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴	リリース	変更内容
	7.0(1)	このコマンドが導入されました。

例 グローバル コンフィギュレーション モードで入力した次の例では、IPSec 統計情報を表示していません。

```
hostname(config)# show ipsec stats

IPsec Global Statistics
-----
Active tunnels: 2
Previous tunnels: 9
Inbound
  Bytes: 4933013
  Decompressed bytes: 4933013
  Packets: 80348
  Dropped packets: 0
  Replay failures: 0
  Authentications: 80348
  Authentication failures: 0
  Decryptions: 80348
  Decryption failures: 0
  Decapsulated fragments needing reassembly: 0
Outbound
  Bytes: 4441740
  Uncompressed bytes: 4441740
  Packets: 74029
  Dropped packets: 0
  Authentications: 74029
  Authentication failures: 0
  Encryptions: 74029
  Encryption failures: 0
  Fragmentation successes: 3
    Pre-fragmentation successes: 2
    Post-fragmentation successes: 1
  Fragmentation failures: 2
    Pre-fragmentation failures: 1
    Post-fragmentation failures: 1
  Fragments created: 10
  PMTUs sent: 1
  PMTUs recvd: 2
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
hostname(config)#
```

#### 関連コマンド

コマンド	説明
<b>clear ipsec sa</b>	IPSec SA またはカウンタを、指定したパラメータに基づいて消去します。
<b>crypto ipsec transform-set</b>	トランスフォームセットを定義します。
<b>show ipsec sa</b>	指定したパラメータに基づいて IPSec SA を表示します。
<b>show ipsec sa summary</b>	IPSec SA の要約を表示します。



# show ipv6 access-list

IPv6 アクセス リストを表示するには、特権 EXEC モードで **show ipv6 access-list** コマンドを使用します。IPv6 アクセス リストは、どの IPv6 トラフィックがセキュリティ アプライアンスを通過できるかを規定するものです。

```
show ipv6 access-list [id [source-ipv6-prefix/prefix-length | any | host source-ipv6-address]]
```

## シンタックスの説明

<i>any</i>	(オプション) IPv6 プレフィックス ::/0 の短縮形です。
<i>host source-ipv6-address</i>	(オプション) 特定のホストの IPv6 アドレス。指定した場合は、指定したホストに関するアクセス規則のみが表示されます。
<i>id</i>	(オプション) アクセス リスト名。指定した場合は、指定したアクセス リストのみが表示されます。
<i>source-ipv6-prefix /prefix-length</i>	(オプション) IPv6 ネットワーク アドレスとプレフィックス。指定した場合は、指定した IPv6 ネットワークに関するアクセス規則のみが表示されます。

## デフォルト

すべての IPv6 アクセス リストを表示します。

## 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	透過	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)	このコマンドが導入されました。

## 使用上のガイドライン

**show ipv6 access-list** コマンドは、IPv6 固有のものであることを除けば、**show ip access-list** コマンドと同様の出力を提供します。

## 例

次に、**show ipv6 access-list** コマンドの出力例を示します。inbound、tcptraffic、および outbound という名前の IPv6 アクセス リストが表示されています。

```
hostname# show ipv6 access-list
IPv6 access list inbound
  permit tcp any any eq bgp reflect tcptraffic (8 matches) sequence 10
  permit tcp any any eq telnet reflect tcptraffic (15 matches) sequence 20
  permit udp any any reflect udptraffic sequence 30
IPv6 access list tcptraffic (reflexive) (per-user)
  permit tcp host 2001:0DB8:1::1 eq bgp host 2001:0DB8:1::2 eq 11000 timeout 300
(time
  left 243) sequence 1
  permit tcp host 2001:0DB8:1::1 eq telnet host 2001:0DB8:1::2 eq 11001 timeout 300
  (time left 296) sequence 2
IPv6 access list outbound
  evaluate udptraffic
  evaluate tcptraffic
```

## 関連コマンド

コマンド	説明
ipv6 access-list	IPv6 アクセス リストを作成します。

## show ipv6 interface

IPv6 用に設定されているインターフェイスのステータスを表示するには、特権 EXEC モードで **show ipv6 interface** コマンドを使用します。

```
show ipv6 interface [brief] [if_name] [prefix]
```

## シンタックスの説明

<i>brief</i>	各インターフェイスの IPv6 ステータスとコンフィギュレーションについて、簡単な要約を表示します。
<i>if_name</i>	(オプション) <b>nameif</b> コマンドによって指定される内部インターフェイス名または外部インターフェイス名。指定したインターフェイスについてのみ、ステータスとコンフィギュレーションが表示されます。
<i>prefix</i>	(オプション) ローカル IPv6 プレフィックス プールから生成されたプレフィックス。

## デフォルト

すべての IPv6 インターフェイスを表示します。

## 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	透過	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)	このコマンドが導入されました。

## 使用上のガイドライン

**show ipv6 interface** コマンドは、IPv6 固有のものであることを除けば、**show interface** コマンドと同様の出力を提供します。インターフェイス ハードウェアが使用可能な場合、そのインターフェイスは *up* とマークされます。インターフェイスが双方向通信を提供できる場合、回線プロトコルは *up* とマークされます。

インターフェイス名を指定しない場合は、すべての IPv6 インターフェイスに関する情報が表示されます。インターフェイス名を指定すると、指定したインターフェイスに関する情報が表示されます。

## 例

次に、**show ipv6 interface** コマンドの出力例を示します。

```
hostname# show ipv6 interface outside
interface ethernet0 "outside" is up, line protocol is up
  IPv6 is enabled, link-local address is 2001:0DB8::/29 [TENTATIVE]
  Global unicast address(es):
    2000::2, subnet is 2000::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF11:6770
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
```

次に、**brief** キーワードを指定して入力した **show ipv6 interface** コマンドの出力例を示します。

```
hostname# show ipv6 interface brief
outside [up/up]
  unassigned
inside [up/up]
  fe80::20d:29ff:fe1d:69f0
  fec0::a:0:0:a0a:a70
vlan101 [up/up]
  fe80::20d:29ff:fe1d:69f0
  fec0::65:0:0:a0a:6570
dmz-ca [up/up]
  unassigned
```

次に、**show ipv6 interface** コマンドの出力例を示します。アドレスからプレフィックスを生成したインターフェイスの特性が表示されています。

```
hostname# show ipv6 interface inside prefix
IPv6 Prefix Advertisements inside
Codes: A - Address, P - Prefix-Advertisement, O - Pool
       U - Per-user prefix, D - Default           N - Not advertised, C - Calendar

AD      fec0:0:0:a::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
```

# show ipv6 neighbor

IPv6 近隣探索キャッシュ情報を表示するには、特権 EXEC モードで **show ipv6 neighbor** コマンドを使用します。

```
show ipv6 neighbor [if_name | address]
```

## シンタックスの説明

<i>address</i>	(オプション) 指定した IPv6 アドレスの近隣探索キャッシュ情報だけを表示します。
<i>if_name</i>	(オプション) 指定したインターフェイス名 ( <b>nameif</b> コマンドによって設定) のキャッシュ情報だけを表示します。

## 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	透過	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)	このコマンドが導入されました。

## 使用上のガイドライン

次に、**show ipv6 neighbor** コマンドによって提供される情報を示します。

- **IPv6 Address** : ネイバーまたはインターフェイスの IPv6 アドレス。
- **Age** : アドレスが到達可能と確認された時点からの経過時間 (分単位)。ハイフン (-) は、スタティック エントリであることを示します。
- **Link-layer Addr** : MAC アドレス。アドレスが不明な場合は、ハイフン (-) が表示されます。
- **State** : 近隣キャッシュ エントリの状態。



(注) 到達可能性の検出は、IPv6 近隣探索キャッシュのスタティック エントリには適用されません。したがって、**INCOMP** (不完全) 状態と **REACH** (到達可能) 状態の説明は、ダイナミック キャッシュ エントリとスタティック キャッシュ エントリで異なります。

次に、IPv6 近隣探索キャッシュのダイナミック エントリについて表示される可能性のある状態を示します。

- **INCOMP** : (不完全) このエントリのアドレス解決を実行中です。ネイバー送信要求メッセージがターゲットの送信要求ノードマルチキャストアドレスに送信されましたが、対応するネイバーアダプタイズメントメッセージをまだ受信していません。
- **REACH** : (到達可能) ネイバーへの転送パスが正常に機能していることを示す肯定確認が、直近の **ReachableTime** ミリ秒以内に受信されました。**REACH** 状態になっている間は、パケットが送信されるときにデバイスは特に操作を実行しません。

- **STALE** : 転送パスが正常に機能していることを示す最後の肯定確認を受信してから、ReachableTime ミリ秒を超える時間が経過しました。**STALE** 状態になっている間は、パケットが送信されるまで、デバイスは操作を一切実行しません。
- **DELAY** : 転送パスが正常に機能していることを示す最後の肯定確認を受信してから、ReachableTime ミリ秒を超える時間が経過しました。パケットは、直近の DELAY\_FIRST\_PROBE\_TIME 秒以内に送信されました。**DELAY** 状態に入ってから DELAY\_FIRST\_PROBE\_TIME 秒以内に到達可能性確認を受信できない場合は、ネイバー送信要求メッセージが送信され、状態が **PROBE** に変更されます。
- **PROBE** : 到達可能性確認を受信されるまで、RetransTime ミリ秒ごとにネイバー送信要求メッセージを再送信して、到達可能性確認を要求し続けます。
- **????** : 不明な状態。

次に、IPv6 近隣探索キャッシュのスタティック エントリについて表示される可能性のある状態を示します。

- **INCMP** : (不完全) このエントリのインターフェイスはダウンしています。
- **REACH** : (到達可能) このエントリのインターフェイスは動作しています。

- Interface

アドレスに到達可能であったインターフェイス。

**例** 次に、インターフェイスを指定して入力した **show ipv6 neighbor** コマンドの出力例を示します。

```
hostname# show ipv6 neighbor inside
IPv6 Address                               Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e REACH inside
FE80::203:A0FF:FED6:141E                    0 0003.a0d6.141e REACH inside
3001:1::45a                                  - 0002.7d1a.9472 REACH inside
```

次に、IPv6 アドレスを指定して入力した **show ipv6 neighbor** コマンドの出力例を示します。

```
hostname# show ipv6 neighbor 2000:0:0:4::2
IPv6 Address                               Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e REACH inside
```

### 関連コマンド

コマンド	説明
<b>clear ipv6 neighbors</b>	IPv6 近隣探索キャッシュのすべてのエントリを、スタティック エントリを除いて削除します。
<b>ipv6 neighbor</b>	IPv6 近隣探索キャッシュ内にスタティック エントリを設定します。

# show ipv6 route

IPv6 ルーティング テーブルの内容を表示するには、特権 EXEC モードで **show ipv6 route** コマンドを使用します。

**show ipv6 route**

**シンタックスの説明** このコマンドには、引数もキーワードもありません。

**デフォルト** デフォルトの動作や値はありません。

**コマンド モード** 次の表は、このコマンドを入力できるモードを示しています。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	透過	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)	このコマンドが導入されました。

**使用上のガイドライン** **show ipv6 route** コマンドは、情報が IPv6 固有のものであることを除けば、**show route** コマンドと同様の出力を提供します。

次に、IPv6 ルーティング テーブルに表示される情報を示します。

- **Codes** : ルートを生成したプロトコルを示します。表示される値は次のとおりです。
  - **C** : 接続済み
  - **L** : ローカル
  - **S** : スタティック
  - **R** : RIP 生成
  - **B** : BGP 生成
  - **I1** : ISIS L1 : 統合 IS-IS Level 1 生成
  - **I2** : ISIS L2 : 統合 IS-IS Level 2 生成
  - **IA** : ISIS エリア間 : 統合 IS-IS エリア間生成
- **fe80::/10** : リモート ネットワークの IPv6 プレフィックスを示します。
- **[0/0]** : カッコ内の最初の数値は、情報ソースの管理ディスタンスです。2 番目の数値はルート  
のメトリックです。
- **via ::** : リモート ネットワークに到達するための次のルータのアドレスを示します。
- **inside** : 示されているネットワークへの次のルータに到達できるインターフェイスを示します。

## 例

次に、**show ipv6 route** コマンドの出力例を示します。

```
hostname# show ipv6 route

IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
L   fe80::/10 [0/0]
    via ::, inside
    via ::, vlan101
L   fec0::a:0:0:a0a:a70/128 [0/0]
    via ::, inside
C   fec0:0:0:a::/64 [0/0]
    via ::, inside
L   fec0::65:0:0:a0a:6570/128 [0/0]
    via ::, vlan101
C   fec0:0:0:65::/64 [0/0]
    via ::, vlan101
L   ff00::/8 [0/0]
    via ::, inside
    via ::, vlan101
S   ::/0 [0/0]
    via fec0::65:0:0:a0a:6575, vlan101
```

## 関連コマンド

コマンド	説明
<b>debug ipv6 route</b>	IPv6 のルーティング テーブル アップデートおよびルート キャッシュ アップデートに関するデバッグ情報を表示します。
<b>ipv6 route</b>	IPv6 ルーティング テーブルにスタティック エントリを追加します。

# show ipv6 routers

オンライン ルータから受信した IPv6 ルータ アドバタイズメント情報を表示するには、特権 EXEC モードで **show ipv6 routers** コマンドを使用します。

```
show ipv6 routers [if_name]
```

## シンタックスの説明

*if\_name* (オプション) 情報を表示する対象となる、**nameif** コマンドによって指定される内部インターフェイス名または外部インターフェイス名。

## デフォルト

デフォルトの動作や値はありません。

## コマンドモード

次の表は、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	透過	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)	このコマンドが導入されました。

## 使用上のガイドライン

インターフェイス名を指定しない場合は、すべての IPv6 インターフェイスに関する情報が表示されます。インターフェイス名を指定すると、指定したインターフェイスに関する情報が表示されません。

## 例

次に、インターフェイス名を指定せずに入力した **show ipv6 routers** コマンドの出力例を示します。

```
hostname# show ipv6 routers
Router FE80::83B3:60A4 on outside, last update 3 min
  Hops 0, Lifetime 6000 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 3FFE:C00:8007::800:207C:4E37/96 autoconfig
  Valid lifetime -1, preferred lifetime -1
Router FE80::290:27FF:FE8C:B709 on inside, last update 0 min
  Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
```

## 関連コマンド

コマンド	説明
<b>ipv6 route</b>	IPv6 ルーティング テーブルにスタティック エントリを追加します。



# show ipv6 traffic

IPv6 トラフィックに関する統計情報を表示するには、特権 EXEC モードで **show ipv6 traffic** コマンドを使用します。

**show ipv6 traffic**

**シンタックスの説明** このコマンドには、引数もキーワードもありません。

**デフォルト** デフォルトの動作や値はありません。

**コマンドモード** 次の表は、このコマンドを入力できるモードを示しています。

コマンドモード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	透過	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)	このコマンドが導入されました。

**使用上のガイドライン** トラフィック カウンタを消去するには、**clear ipv6 traffic** コマンドを使用します。

## 例

次に、**show ipv6 traffic** コマンドの出力例を示します。

```
hostname# show ipv6 traffic
IPv6 statistics:
  Rcvd: 545 total, 545 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
        218 fragments, 109 total reassembled
        0 reassembly timeouts, 0 reassembly failures
  Sent: 228 generated, 0 forwarded
        1 fragmented into 2 fragments, 0 failed
        0 encapsulation failed, 0 no route, 0 too big
  Mcast: 168 received, 70 sent

ICMP statistics:
  Rcvd: 116 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
  unreachable: 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, 60 router advert, 0 redirects
        31 neighbor solicit, 25 neighbor advert
  Sent: 85 output, 0 rate-limited
  unreachable: 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, 18 router advert, 0 redirects
        33 neighbor solicit, 34 neighbor advert

UDP statistics:
  Rcvd: 109 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 37 output

TCP statistics:
  Rcvd: 85 input, 0 checksum errors
  Sent: 103 output, 0 retransmitted
```

## 関連コマンド

コマンド	説明
<b>clear ipv6 traffic</b>	IPv6 トラフィック カウンタを消去します。