show facility-alarm relay コマンド～ show ipsec stats コマンド

show facility-alarm relay

ISA 3000 でアクティブ化された状態のリレーを表示するには、ユーザ EXEC モードで**show facility-alarm relay** コマンドを使用します。

show facility-alarm relay

構文の説明

このコマンドには引数またはキーワードはありません。

コマンドデフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

アラーム出力ピンに接続されたリレーは、ドア センサなどの外部センサと、デュアル電源、温度センサなどのような内部センサのアラーム ステータスを伝達します。

例

次に、**show facility-alarm relay** コマンドの出力例を示します。

```
ciscoasa> show facility-alarm relay
Source    Severity   Description                          Relay      Time
ciscoasa  minor      external alarm contact 1 triggered   Energized  06:56:50 UTC Mon Sep
22 2014
```

関連コマンド

コマンド	説明
alarm contact description	アラーム入力の説明を指定します。
alarm contact severity	アラームの重大度を指定します。
alarm contact trigger	1 つまたはすべてのアラーム入力のトリガーを指定します。
alarm facility input-alarm	アラーム入力のロギング オプションと通知オプションを指定します。

コマンド	説明
alarm facility power-supply rps	電源アラームを設定します。
alarm facility temperature	温度アラームを設定します。
alarm facility temperature（上限および下限のしきい値）	温度しきい値の下限または上限を設定します。
show alarm settings	すべてのグローバル アラーム設定を表示します。
show environment alarm-contact	すべての外部アラーム設定を表示します。
show facility-alarm status	トリガーされたすべてのアラームを表示するか、または指定された重大度に基づいてアラームを表示します。
clear facility-alarm output	出力リレーの電源を切り、LED のアラーム状態をクリアします。

show facility-alarm status

ISA 3000 のすべてのアラームを表示するには、ユーザ EXEC モードで **show facility-alarm status** コマンドを使用します。このコマンドには、指定された重大度に基づいてアラームを表示するための引数もあります。

show facility-alarm status {**info** | **major** | **minor**}

構文の説明

info	トリガーされたすべてのアラームを表示します。
major	トリガーされた重大度が高いすべてのアラームを表示します。
minor	トリガーされた重大度が低いすべてのアラームを表示します。

コマンドデフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

アラーム出力ピンに接続されたリレーは、ドア センサなどの外部センサと、デュアル電源、温度センサなどのような内部センサのアラーム ステータスを伝達します。

例

これらすべてのコマンドが次の情報を表示します。

カラム	説明
Source	アラームがトリガーされたデバイス。通常は、デバイスで設定されているホスト名です。
Severity	重大度が高い（major）か、低い（minor）か
Description	トリガーされたアラームのタイプ。たとえば、温度、外部連絡先、冗長電源など
Relay	電源が入っている（energized）か、入っていない（de-energized）か
Time	トリガーされたアラームのタイムスタンプ

次に、**show facility-alarm status** コマンドの出力例を示します。

```
ciscoasa> show facility-alarm status info
ciscoasa minor external alarm contact 1 triggered  Energized     06:56:50 UTC Mon Sep 22
2014
ciscoasa minor Temp below Secondary Threshold      De-energized  06:56:49 UTC Mon Sep 22
2014
ciscoasa major Redundant pwr missing or failed     De-energized  07:00:19 UTC Mon Sep 22
2014
ciscoasa major Redundant pwr missing or failed     De-energized  07:00:19 UTC Mon Sep 22
2014

ciscoasa> show facility-alarm status major
Source    Severity  Description                          Relay         Time
ciscoasa  major     Redundant pwr missing or failed   De-energized  07:00:19 UTC Mon Sep
22 2014
ciscoasa  major     Redundant pwr missing or failed   De-energized  07:00:19 UTC Mon Sep
22 2014


ciscoasa> show facility-alarm status minor
Source    Severity  Description                           Relay         Time
ciscoasa  minor     external alarm contact 1 triggered  Energized     06:56:50 UTC Mon Sep
22 2014
ciscoasa  minor     Temp below Secondary Threshold      De-energized  06:56:49 UTC Mon Sep
22 2014
```

関連コマンド

コマンド	説明
alarm contact description	アラーム入力の説明を指定します。
alarm contact severity	アラームの重大度を指定します。
alarm contact trigger	1 つまたはすべてのアラーム入力のトリガーを指定します。
alarm facility input-alarm	アラーム入力のロギング オプションと通知オプションを指定します。
alarm facility power-supply rps	電源アラームを設定します。
alarm facility temperature	温度アラームを設定します。
alarm facility temperature（上限および下限のしきい値）	温度しきい値の下限または上限を設定します。
show alarm settings	すべてのグローバル アラーム設定を表示します。
show environment alarm-contact	すべての外部アラーム設定を表示します。
show facility-alarm relay	アクティブ化された状態のリレーを表示します。
clear facility-alarm output	出力リレーの電源を切り、LED のアラーム状態をクリアします。

show failover

ユニット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**]

構文の説明

group	指定されたフェールオーバー グループの実行状態を表示します。
history	フェールオーバー履歴を表示します。フェールオーバー履歴には、過去のフェールオーバーでの状態変更や、状態変更の理由が表示されます。履歴情報はデバイスをリブートするとクリアされます。
interface	フェールオーバーおよびステートフル リンク情報を表示します。
num	フェールオーバー グループの番号。
state	両方のフェールオーバー ユニットのフェールオーバー状態を表示します。表示される情報は、ユニットのプライマリまたはセカンダリ ステータス、ユニットのアクティブ/スタンバイ ステータス、最後にレポートされたフェールオーバーの理由などがあります。障害の理由が解消されても、障害の理由は出力に残ります。
statistics	フェールオーバー コマンド インターフェイスの送信および受信パケット数を表示します。

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

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが変更されました。出力の情報が追加されました。
8.2(2)	このコマンドが変更されました。出力には、ファイアウォール インターフェイスおよびフェールオーバー インターフェイスの IPv6 アドレスが含まれます。ステートフル フェールオーバーの統計情報出力には、IPv6 ネイバー探索テーブル（IPv6 ND tbl）の更新についての情報が含まれます。

使用上のガイドライン

show failover コマンドは、ダイナミック フェールオーバー情報、インターフェイス 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。

IPv4 と IPv6 の両方のアドレスがインターフェイスで設定されている場合は、両方のアドレスが出力に表示されます。インターフェイスには複数の IPv6 アドレスを設定できるため、リンクローカル アドレスのみが表示されます。インターフェイスに IPv4 アドレスが設定されていない場合、出力の IPv4 アドレスは 0.0.0.0 として表示されます。インターフェイスに IPv6 アドレスが設定されていない場合、アドレスは単純に出力から省かれます。

Stateful Failover Logical Update Statistics 出力は、ステートフル フェールオーバーがイネーブルの場合のみ表示されます。「xerr」および「rerr」の値はフェールオーバーのエラーではなく、パケット送受信エラーの数を示します。

(注) ステートフル フェールオーバーは、ASA 5505 では使用できません。したがって、ステートフル フェールオーバーの統計情報出力も使用できません。

show failover コマンド出力で、ステートフル フェールオーバーの各フィールドには次の値があります。

- Stateful Obj の値は次のとおりです。
  - xmit：送信されたパケットの数を示します。
  - xerr：送信エラーの数を示します。
  - rcv：受信したパケットの数を示します。
  - rerr：受信エラーの数を示します。
- 各行は、次に示す特定のオブジェクト スタティック カウントを表します。
  - General：すべてのステートフル オブジェクトの合計を示します。
  - sys cmd：**login** または **stay alive** などの論理的なシステム更新コマンドを示します。
  - up time：ASAのアップ タイムの値（アクティブなASAがスタンバイのASAに渡す）を示します。
  - RPC services：リモート プロシージャ コール接続情報。
  - TCP conn：ダイナミック TCP 接続情報。
  - UDP conn：ダイナミック UDP 接続情報。
  - ARP tbl：ダイナミック ARP テーブル情報。
  - Xlate_Timeout：接続変換タイムアウト情報を示します。
  - IPv6 ND tbl：IPv6 ネイバー探索テーブル情報。
  - VPN IKE upd：IKE 接続情報。
  - VPN IPSEC upd：IPSec 接続情報。
  - VPN CTCP upd：cTCP トンネル接続情報。
  - VPN SDI upd：SDI AAA 接続情報。
  - VPN DHCP upd：トンネル型 DHCP 接続情報。
  - SIP Session：SIP シグナリング セッション情報。
  - Route Session：ルート同期アップデートの LU 統計情報

フェールオーバー IP アドレスを入力しない場合、**show failover** コマンドでは IP アドレス 0.0.0.0 が表示され、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。フェールオーバーを機能させる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。

表 7-1 に、フェールオーバーのインターフェイス状態の説明を示します。

表 7-1　フェールオーバー インターフェイス状態

状態	説明
Normal	インターフェイスは稼働中で、ピア ユニットの対応するインターフェイスから hello パケットを受信中です。
Normal (Waiting)	インターフェイスは稼働中ですが、ピア ユニットの対応するインターフェイスから hello パケットをまだ受信していません。インターフェイスのスタンバイ IP アドレスが設定されていること、および 2 つのインターフェイス間の接続が存在することを確認してください。
Normal (Not-Monitored)	インターフェイスは動作中ですが、フェールオーバー プロセスによってモニタされていません。モニタされていないインターフェイスの障害によってフェールオーバーはトリガーされません。
No Link	物理リンクがダウンしています。
No Link (Waiting)	物理リンクがダウンし、インターフェイスはピア ユニットの対応するインターフェイスから hello パケットをまだ受信していません。リンクが復元した後、スタンバイ IP アドレスがそのインターフェイスに設定されているかどうか、および 2 つのインターフェイス間が接続されているかどうかを確認します。
No Link (Not-Monitored)	物理リンクがダウンしていますが、フェールオーバー プロセスによってモニタされていません。モニタされていないインターフェイスの障害によってフェールオーバーはトリガーされません。
Link Down	物理リンクは動作中ですが、インターフェイスは管理上ダウンしています。
Link Down (Waiting)	物理リンクは動作中ですが、インターフェイスは管理上ダウンしており、インターフェイスはピア ユニットの対応するインターフェイスから hello パケットをまだ受信していません。インターフェイスを動作状態にした後（インターフェイス コンフィギュレーション モードで **no shutdown** コマンドを使用）、スタンバイ IP アドレスがそのインターフェイスに設定されているかどうか、および 2 つのインターフェイス間が接続されているかどうかを確認します。
Link Down (Not-Monitored)	物理リンクは動作中ですが、インターフェイスは管理上ダウンしており、フェールオーバー プロセスによってモニタされていません。モニタされていないインターフェイスの障害によってフェールオーバーはトリガーされません。
Testing	ピア ユニットの対応するインターフェイスから hello パケットが届かないため、インターフェイスはテスト モードです。
Failed	インターフェイスのテストに失敗し、インターフェイスは障害が発生したとしてマークされます。インターフェイスの障害によってフェールオーバー基準が満たされた場合、インターフェイスの障害によって、セカンダリ ユニットまたはフェールオーバー グループへのフェールオーバーが発生します。

マルチ コンテキスト モードでは、**show failover** コマンドのみがセキュリティ コンテキストで使用できます。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。ASA では、フェールオーバー リンク（folink）と inside インターフェイスに IPv6 アドレスを使用しています。

```
ciscoasa# show failover

Failover On
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/4 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 1049 maximum
MAC Address Move Notification Interval not set
Version: Ours 98.1(1)86, Mate 98.1(1)86
Serial Number: Ours JAF1610APKQ, Mate JAF1610ALGM
Last Failover at: 12:52:34 UTC Apr 26 2017
        This host: Primary - Active
                Active time: 87 (sec)
                slot 0: ASA5585-SSP-10 hw/sw rev (2.0/98.1(1)86) status (Up Sys)
                  Interface inside (10.86.118.1): Normal (Monitored)
                  Interface outside (192.168.77.1): No Link (Waiting)
                  Interface dmz (192.168.67.1): No Link (Waiting)
                slot 1: empty
                slot 1: empty
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5585-SSP-10 hw/sw rev (2.0/98.1(1)86) status (Up Sys)
                  Interface inside (10.86.118.2): Normal (Waiting)
                  Interface outside (192.168.77.2): No Link (Waiting)
                  Interface dmz (192.168.67.2): No Link (Waiting)
                slot 1: empty
                slot 1: empty

Stateful Failover Logical Update Statistics
        Link : failover GigabitEthernet0/4 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         22         0          6          0
        sys cmd         6          0          6          0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         14         0          0          0
        Xlate_Timeout   0          0          0          0
        IPv6 ND tbl     0          0          0          0
        VPN IKEv1 SA    0          0          0          0
        VPN IKEv1 P2    0          0          0          0
        VPN IKEv2 SA    0          0          0          0
        VPN IKEv2 P2    0          0          0          0
        VPN CTCP upd    0          0          0          0
        VPN SDI upd     0          0          0          0
        VPN DHCP upd    0          0          0          0
        SIP Session     0          0          0          0
        SIP Tx  0          0          0          0
        SIP Pinhole     0          0          0          0
        Route Session   0          0          0          0
        Router ID       1          0          0          0
        User-Identity   1          0          0          0
        CTS SGTNAME     0          0          0          0
        CTS PAC         0          0          0          0
        TrustSec-SXP    0          0          0          0
        IPv6 Route      0          0          0          0
```

```
        STS Table       0           0           0           0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       5       6
        Xmit Q:         0       27      86
```

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。この例では、管理コンテキストでのみ IPv6 アドレスをインターフェイスに割り当てています。

```
ciscoasa# show failover

Failover On
Failover unit Primary
Failover LAN Interface: folink 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-5545 hw/sw rev (1.0/7.0(0)79) status (Up Sys)
                admin Interface outside (10.132.8.5): Normal
                admin Interface folink (10.132.9.5/fe80::2a0:c9ff:fe03:101): Normal
                admin Interface inside (10.130.8.5/fe80::2a0:c9ff:fe01:101): Normal
                admin Interface fourth (10.130.9.5/fe80::3eff:fe11:6670): 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-5545 hw/sw rev (1.0/7.0(0)79) status (Up Sys)
                admin Interface outside (10.132.8.6): Normal
                admin Interface folink (10.132.9.6/fe80::2a0:c9ff:fe03:102): Normal
                admin Interface inside (10.130.8.6/fe80::2a0:c9ff:fe01:102): Normal
                admin Interface fourth (10.130.9.6/fe80::3eff:fe11:6671): 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
        IPv6 ND tbl     22          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
       SIP Session    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 シリーズのでの **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、アクティブ-アクティブ セットアップでの **show failover state** コマンドの出力例を示します。

```
ciscoasa(config)# show failover state

               State          Last Failure Reason      Date/Time
This host  -   Secondary
    Group 1    Failed         Backplane Failure        03:42:29 UTC Apr 17 2009
    Group 2    Failed         Backplane Failure        03:42:29 UTC Apr 17 2009
Other host -   Primary
    Group 1    Active         Comm Failure             03:41:12 UTC Apr 17 2009
    Group 2    Active         Comm Failure             03:41:12 UTC Apr 17 2009

====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

次に、アクティブ-スタンバイ セットアップでの **show failover state** コマンドの出力例を示します。

```
ciscoasa(config)# show failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
               Active         None
Other host -   Secondary
               Standby Ready  Comm Failure             12:53:10 UTC Apr 26 2017

====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

表 7-2 に、**show failover state** コマンドの出力の説明を示します。

表 7-2　　show failover state の出力の説明

フィールド	説明
Configuration State	コンフィギュレーションの同期化の状態を表示します。 スタンバイ ユニットで可能なコンフィギュレーション状態は、次のとおりです。 • **Config Syncing - STANDBY**：コンフィギュレーションの同期化が実行されているときに設定されます。 • **Interface Config Syncing - STANDBY** • **Sync Done - STANDBY**：スタンバイ ユニットが、アクティブ ユニットと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。 アクティブ ユニットで可能なコンフィギュレーション状態は、次のとおりです。 • **Config Syncing**：スタンバイ ユニットに対してコンフィギュレーションの同期化を実行しているときにアクティブ ユニット上で設定されます。 • **Interface Config Syncing** • **Sync Done**：アクティブ ユニットが、スタンバイ ユニットに対してコンフィギュレーションの同期化を正常に完了したときに設定されます。 • **Ready for Config Sync**：スタンバイ ユニットがコンフィギュレーションの同期化を受信する準備が完了したという信号を送るときにアクティブ ユニット上で設定されます。
Communication State	MAC アドレスの同期化のステータスを表示します。 • **Mac set**：MAC アドレスがピア ユニットからこのユニットに同期化されました。 • **Updated Mac**：MAC アドレスが更新され、他のユニットに対して同期化する必要がある場合に使用されます。また、ユニットが遷移期間中に、ピア ユニットから同期化されたローカル MAC アドレスを更新する場合にも使用されます。
Date/Time	障害の日付およびタイムスタンプを表示します。

表 7-2　　show failover state の出力の説明（続き）

フィールド	説明
Last Failure Reason	最後にレポートされた障害の理由を表示します。この情報は、障害の条件が解消されてもクリアされません。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。 可能な障害の理由は次のとおりです。 • **Ifc Failure**：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、フェールオーバーが発生しました。 • **Comm Failure**：フェールオーバー リンクに障害が発生したか、ピアがダウンしています。 • **Backplane Failure**
State	ユニットの Primary/Secondary および Active/Standby ステータスを表示します。
This host/Other host	This host は、コマンドが実行されたデバイスについての情報を示します。Other host は、フェールオーバーのペアとなる他のデバイスについての情報を示します。

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

```
ciscoasa(config)# show failover history
==============================================================================
Group     From State                To State                  Reason
==============================================================================
...
03:42:29 UTC Apr 17 2009
    0     Sync Config               Failed
Backplane failed

03:42:29 UTC Apr 17 2009
    1     Standby Ready             Failed
Backplane failed

03:42:29 UTC Apr 17 2009
    2     Standby Ready             Failed
Backplane failed

03:44:39 UTC Apr 17 2009
    0     Failed                    Negotiation
Backplane operational

03:44:40 UTC Apr 17 2009
    1     Failed                    Negotiation
Backplane operational

03:44:40 UTC Apr 17 2009
    2     Failed                    Negotiation
Backplane operational

==============================================================================
```

各エントリには、状態変更が発生した時刻および日付、開始状態、結果状態、および状態変更の理由が示されます。最も新しいエントリが表示の末尾に配置されます。古いエントリが上部に表示されます。最大で 60 エントリを表示できます。エントリが最大数に到達した場合、最も古いエントリが出力の上部から削除され、新しいエントリが末尾に追加されます。

表 7-3 に、フェールオーバーの状態を示します。状態には永続的と一時的の 2 つのタイプがあります。永続的な状態とは、障害などの何らかの出来事によって状態変更が発生するまで、ユニットが維持できる状態のことです。一時的な状態とは、ユニットが永続的な状態に到達するまでの間に経過する状態です。

表 7-3　フェールオーバーの状態

States	説明
Disabled	フェールオーバーはディセーブルです。これは安定したステートです。
不合格	ユニットは障害状態です。これは安定したステートです。
Negotiation	ユニット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を判別し、Active/Standby ロールを決定します。ネゴシエートされたロールに基づき、ユニットはスタンバイ ユニット状態またはアクティブ ユニット状態になるか、障害状態になります。これは一時的なステートです。
Not Detected	ASA はピアの存在を検出できません。このことは、フェールオーバーがイネーブルな状態で ASA が起動されたが、ピアが存在しない、またはピアの電源がオフである場合に発生する可能性があります。
スタンバイ ユニット状態	
Cold Standby	ユニットはピアがアクティブ状態に到達するのを待機します。ピア ユニットがアクティブ状態に到達すると、このユニットは Standby Config 状態に進みます。これは一時的なステートです。
Sync Config	ユニットはピア ユニットから実行コンフィギュレーションを要求します。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、ユニットは初期化状態に戻ります。これは一時的なステートです。
Sync File System	ユニットはピア システムとファイル システムを同期化します。これは一時的なステートです。
Bulk Sync	ユニットはピアから状態情報を受信します。この状態は、ステートフル フェールオーバーがイネーブルの場合にのみ発生します。これは一時的なステートです。
Standby Ready	ユニットは、アクティブ ユニットに障害が発生した場合に引き継ぐ準備が完了しています。これは安定したステートです。
アクティブ ユニット状態	
Just Active	ユニットがアクティブ ユニットになったときの最初の状態です。この状態にあるとき、ユニットがアクティブになること、および IP アドレスと MAC アドレスをインターフェイスに設定することをピアに通知するメッセージがピアに送信されます。これは一時的なステートです。
Active Drain	ピアからのキュー メッセージが廃棄されます。これは一時的なステートです。
Active Applying Config	ユニットはシステム コンフィギュレーションを適用します。これは一時的なステートです。
Active Config Applied	ユニットはシステム コンフィギュレーションの適用を完了しました。これは一時的なステートです。
Active	ユニットはアクティブで、トラフィックを処理しています。これは安定したステートです。

それぞれの状態変更の後に状態変更の理由が続きます。この理由は、ユニットが一時的な状態から永続的な状態に進んでも、通常同じままになります。次に、可能性がある状態変更の理由を示します。

- 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
- 他のユニットのソフトウェア バージョンが異なっている
- 他のユニットの動作モードが異なっている
- 他のユニットのライセンスが異なっている
- 他のユニットのシャーシ コンフィギュレーションが異なっている
- 他のユニットのカード コンフィギュレーションが異なっている
- 他のユニットからアクティブ状態を要求された
- 他のユニットからスタンバイ状態を要求された
- 他のユニットが、このユニットに障害があるとレポートした
- 他のユニットが、そのユニットに障害があるとレポートした
- コンフィギュレーションの不一致
- アクティブ ユニットが検出された
- アクティブ ユニット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
- 他のユニットの 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
- このユニットの通信が失敗した
- フェールオーバー メッセージの ACK を受信しなかった
- 同期後の学習状態で他のユニットが動作しなくなった
- ピアの電源が検出されない
- フェールオーバー ケーブルがない
- HA 状態の進行に失敗した
- サービス カード障害が検出された
- 他のユニットのサービス カードに障害が発生した
- このユニットのサービス カードはピアと同様である
- LAN インターフェイスが未設定状態になった
- ピア ユニットがリロードされた

- 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同期化の状態を確認できない
- 自動更新要求
- 原因不明

次に、**show failover interface** コマンドの出力例を示します。デバイスのフェールオーバー インターフェイスに IPv6 アドレスが設定されています。

```
ciscoasa(config)# show failover interface
        interface folink GigabitEthernet0/2
                System IP Address: 2001:a0a:b00::a0a:b70/64
                My IP Address    : 2001:a0a:b00::a0a:b70
                Other IP Address : 2001:a0a:b00::a0a:b71
```

関連コマンド

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

show failover exec

指定したユニットの **failover exec** コマンド モードを表示するには、特権 EXEC モードで **show failover exec** コマンドを使用します。

show failover exec {**active** | **standby** | **mate**}

構文の説明

active	アクティブ ユニットの **failover exec** コマンド モードを表示します。
mate	ピア ユニットの **failover exec** コマンド モードを表示します。
standby	スタンバイ ユニットの **failover exec** コマンド モードを表示します。

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

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

failover exec コマンドは、指定したデバイスとのセッションを確立します。デフォルトでは、このセッションはグローバル コンフィギュレーション モードです。このセッションのコマンド モードは、**failover exec** コマンドを使用して適切なコマンド(**interface** コマンドなど)を送信することによって変更できます。指定されたデバイスの **failover exec** コマンド モードを変更しても、デバイスへのアクセスに使用しているセッションのコマンド モードは変更されません。デバイスとの現在のセッションのコマンド モードを変更しても、**failover exec** コマンドで使用されるコマンド モードには影響しません。

show failover exec コマンドは、**failover exec** コマンドで送信されるコマンドが実行される、指定したデバイス上のコマンド モードを表示します。

例

次に、**show failover exec** コマンドの出力例を示します。この例では、**failover exec** コマンドが入力されるユニットのコマンド モードが、コマンドが実行される **failover exec** コマンド モードと同じである必要がないことを示しています。

この例では、スタンバイ ユニットにログインした管理者が、アクティブ ユニット上のインターフェイスに名前を追加します。この例で、**show failover exec mate** コマンドを 2 回めに入力したとき、ピア デバイスはインターフェイス コンフィギュレーション モードであると表示されます。**failover exec** コマンドでデバイスに送信されるコマンドは、このモードで実行されます。

```
ciscoasa(config)# show failover exec mate

Active unit Failover EXEC is at config mode

! The following command changes the standby unit failover exec mode
! to interface configuration mode.
ciscoasa(config)# failover exec mate interface GigabitEthernet0/1
ciscoasa(config)# show failover exec mate

Active unit Failover EXEC is at interface sub-command mode

! Because the following command is sent to the active unit, it is replicated
! back to the standby unit.
ciscoasa(config)# failover exec mate nameif test
```

関連コマンド

コマンド	説明
failover exec	フェールオーバー ペアの指定されたユニット上で、入力されたコマンドを実行します。

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*

構文の説明

descriptors	開かれているファイル記述子をすべて表示します。
filename	ファイル名を指定します。
情報	パートナー アプリケーション パッケージ ファイルなど、特定のファイルについての情報を表示します。
system	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。

コマンドデフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.2(1)	パートナー アプリケーション パッケージ ファイルについての情報を表示する機能が追加されました。
9.7(1)	**show file descriptor** コマンドは、システム コンテキスト モードで open ファイル記述子からだけ出力をプリントするように更新されました。

使用上のガイドライン

マルチ コンテキスト モードのシステム コンテキストで使用する場合、**show file descriptors** コマンドはすべてのコンテキストにわたって、開いている場合のファイルの記述子の詳細を表示します。コンテキストに open ファイル記述子がある場合、CLI がシステム コンテキストで実行されていれば、その特定のコンテキストの詳細のみが表示されます。システムは、「no file descriptors」のコンテキストのすべての名前は出力しません。open ファイル記述子があるコンテキストのみを表示します。

例

次に、**show firewall** コマンドの出力例を示します。

開いているファイルがない単一コンテキスト

```
ciscoasa(config)# show file descriptors
No open file descriptors
ciscoasa(config)#
```

開いているファイルがある単一のコンテキスト

```
ciscoasa(config)# show file descriptors
FD  Position  Open  PID  Path
0 0 0302  139  disk0:/test1.txt
ciscoasa(config)#
```

システム コンテキストで開いているファイルがないマルチコンテキスト

```
ciscoasa# show file descriptors
ciscoasa#
```

システム コンテキストで開いているファイルがあるマルチコンテキスト

```
ST-Campus-spyc/stby(config)# show file descriptors
Context: CTX1
FD  Position  Open  PID  Path
0 0 0000  180  disk0:/SHARED/anyconnect-linux-3.1.07021-k9.pkg
1 0 0000  180  disk0:/SHARED/anyconnect-win-4.0.02052-k9.pkg
Context: CTX3
FD  Position  Open  PID  Path
0 0 0000  180  disk0:/SHARED/anyconnect-linux-3.1.07021-k9.pkg
1 0 0000  180  disk0:/SHARED/anyconnect-win-4.0.02052-k9.pkg
Context: CTX5
FD  Position  Open  PID  Path
0 0 0000  180  disk0:/SHARED/anyconnect-linux-3.1.07021-k9.pkg
1 0 0000  180  disk0:/SHARED/anyconnect-win-4.0.02052-k9.pkg
```

ユーザ コンテキストで開いているファイルがないマルチコンテキスト

```
ST-Campus-spyc/stby/CTX1(config)# changeto context CTX2
ST-Campus-spyc/act/CTX2(config)# show file descriptors
No open file descriptors
ST-Campus-spyc/act/CTX2(config)#
```

ユーザ コンテキストで開いているファイルがあるマルチコンテキスト

```
ST-Campus-spyc/stby(config)# changeto con CTX1
ST-Campus-spyc/stby/CTX1(config)# show file descriptors
FD  Position  Open  PID  Path
0 0 0000  180  disk0:/SHARED/anyconnect-linux-3.1.07021-k9.pkg
1 0 0000  180  disk0:/SHARED/anyconnect-win-4.0.02052-k9.pkg
ST-Campus-spyc/stby/CTX1(config)#

ciscoasa# show file system
File Systems:
   Size(b)     Free(b)    Type  Flags  Prefixes
* 60985344    60973056    disk    rw     disk:
```

次に、**show file info** コマンドの出力例を示します。

```
ciscoasa# show file info disk0:csc_embd1.0.1000.pkg
type is package (csc)
file size is 17204149 bytes version 1
```

関連コマンド

コマンド	説明
dir	ディレクトリの内容を表示します。
pwd	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(ルーテッドまたはトランスペアレント)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

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、**show firewall** コマンドの出力例を示します。

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

関連コマンド

コマンド	説明
firewall transparent	ファイアウォール モードを設定します。
show mode	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

internal Flash memory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: all | controller | filesys

(注) ASAでは、**flash** キーワードにエイリアス **disk0** が使用されます。

構文の説明

all	すべてのフラッシュの情報を表示します。
controller	ファイル システム コントローラの情報を表示します。
filesys	ファイル システムの情報を表示します。

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。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、**show flash:** コマンドの出力例を示します。

```
ciscoasa# 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
dir	ディレクトリの内容を表示します。
show disk0:	internal Flash memoryの内容を表示します。
show disk1:	external Flash memory cardの内容を表示します。

show flow-export counters

NetFlow データに関連付けられているランタイム カウンタを表示するには、特権 EXEC モードで **show flow-export counters** コマンドを使用します。

show flow-export counters

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
8.1(1)	このコマンドが追加されました。
9.0(1)	送信元ポート割り当ての失敗に対する新しいエラー カウンタが追加されました。

使用上のガイドライン

ランタイム カウンタには、統計データおよびエラー データが含まれます。

例

次に、NetFlow データに関連付けられているランタイム カウンタを表示する **show flow-export counters** コマンドの出力例を示します。

```
ciscoasa# show flow-export counters

destination: inside 209.165.200.224 2055
 Statistics:
  packets sent                      1000
 Errors:
  block allocation failure             0
  invalid interface                    0
  template send failure                0
  no route to collector                0
  source port allocation               0
```

関連コマンド

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

show flow-offload

フロー オフロードについての情報を表示するには、特権 EXEC モードで **show flow-offload** コマンドを使用します。

show flow-offload {**info** [**detail**] | **cpu** | **flow** [**count** | **detail**] | **statistics**}

構文の説明

info [**detail**]	オフロード エンジンに関する基本情報を表示します。ポートの使用状況の要約などの追加情報を取得するには、**detail** キーワードを追加します。
cpu	オフロード コアの負荷のパーセンテージを表示します。
flow [**count**	**detail**]	オフロードされているアクティブなフローに関する情報を表示します。オプションで次のキーワードを追加できます。 • **count**：オフロードされているアクティブなフローと作成済みのオフロードされたフローの数を表示します。 • **detail**：オフロードされているアクティブなフローとそれらの書き換えルールとデータを表示します。
statistics	オフロードされたフローのパケット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

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが導入されました。

使用上のガイドライン

フロー オフロードが有効な場合は、このコマンドを使用して、サービスとオフロードされたフローに関する情報を表示できます。

例

次に、**show flow-offload statistics** コマンドの出力例を示します。出力には、送信（Tx）パケット数、受信（Rx）パケット数、ドロップされたパケット数、および使用された仮想 NIC（VNIC）の統計情報が示されます。

```
ciscoasa# show offload-engine statistics
Packet stats of port : 0
        Tx Packet count                 :        785807566
        Rx Packet count                 :        785807566
        Dropped Packet count            :                0
        VNIC transmitted packet         :        785807566
        VNIC transmitted bytes          :     103726598712
        VNIC Dropped packets            :                0
        VNIC erroneous received         :                0
        VNIC CRC errors                 :                0
        VNIC transmit failed            :                0
        VNIC multicast received         :                0
 Packet stats of port : 1
        Tx Packet count                 :                0
        Rx Packet count                 :                0
        Dropped Packet count            :                0
        VNIC transmitted packet         :                0
        VNIC transmitted bytes          :                0
        VNIC Dropped packets            :                0
        VNIC erroneous received         :                0
        VNIC CRC errors                 :                0
        VNIC transmit failed            :                0
        VNIC multicast received         :                0
```

関連コマンド

コマンド	説明
clear flow-offload	オフロード統計情報またはフローをクリアします。
flow-offload	フロー オフロードを有効にします。
set-connection advanced-options flow-offload	オフロードの対象としてトラフィック フローを指定します。

show fragment

IP フラグメント再構築モジュールの動作データを表示するには、特権 EXEC モードで **show fragment** コマンドを使用します。

show fragment [*interface*]

構文の説明

interface	（任意）ASA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

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、コンフィギュレーション データと動作データを分けるために、**show fragment** および **show running-config fragment** の 2 つのコマンドに分けられました。

例

次に、IP フラグメント再構築モジュールの動作データを表示する方法の例を示します。

```
ciscoasa# 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
clear configure fragment	IP フラグメント再構成コンフィギュレーションをクリアし、デフォルトにリセットします。
clear fragment	IP フラグメント再構成モジュールの動作データをクリアします。

コマンド	説明
fragment	パケット フラグメンテーションを詳細に管理できるようにし、NFS との互換性を高めます。
show running-config fragment	IP フラグメント再構成コンフィギュレーションを表示します。

show gc

ガーベッジ コレクション プロセスの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

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、**show gc** コマンドの出力例を示します。

```
ciscoasa# 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
clear gc	ガーベッジ コレクション プロセスの統計情報を削除します。

show h225

ASAを越えて確立された 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

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

show h225 コマンドは、ASA 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。

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。セッション レコードが多いときに **pager** コマンドが設定されていない場合、**show** コマンドの出力が末端に届くまでに時間がかかる場合があります。

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。

```
ciscoasa# 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、ローカル エンドポイント 10.130.56.3 と外部ホスト 172.30.254.203 との間でASAを通過するアクティブな H.323 コールが 1 つ存在し、これらのエンドポイントの間には、コールの CRV（Call Reference Value）が 9861 の同時コールが 1 つ存在す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 については、同時コールの数は 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
inspect h323	H.323 アプリケーション インスペクションをイネーブルにします。
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ASA間で確立された H.245 セッションの情報を表示します。
show h323 ras	ASA間で確立された H.323 RAS セッションの情報を表示します。
timeout h225 | h323	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がASAを越えて確立した 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

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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ASA 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 スタートでは、コールの 2 つのエンドポイントが H.245 用に別の TCP コントロール チャネルを開きます。ファスト スタートは、H.245 メッセージが H.225 コントロール チャネルで H.225 メッセージの一部として交換された場合です。

例

次に、**show h245** コマンドの出力例を示します。

```
ciscoasa# 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
```

ASAでアクティブな 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 メッセージの先頭の 4 バイト 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わかります)。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るメディアは、論理チャネル番号（LCN）が 258 で、外部の RTP IP アドレス/ポート ペアが 172.30.254.203/49608、RTCP IP アドレス/ポートが 172.30.254.203/49609、ローカルの RTP IP アドレス/ポート ペアが 10.130.56.3/49608、RTCP ポートが 49609 です。

値が 259 の 2 番めの LCN は、外部の RTP IP アドレス/ポート ペアが 172.30.254.203/49606、RTCP IP アドレス/ポート ペアが 172.30.254.203/49607、ローカルの RTP IP アドレス/ポート ペアが 10.130.56.3/49606、RTCP ポートが 49607 です。

関連コマンド

コマンド	説明
inspect h323	H.323 アプリケーション インスペクションをイネーブルにします。
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ASA間で確立された H.245 セッションの情報を表示します。
show h323 ras	ASA間で確立された H.323 RAS セッションの情報を表示します。
timeout h225 | h323	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

H.323 接続の情報を表示するには、特権 EXEC モードで **show h323** コマンドを使用します。

show h323 {ras | gup}

構文の説明

ras	ASA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 セッションを表示します。
gup	H323 ゲートウェイ アップデート プロトコル接続に関する情報を表示します。

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

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

show h323 ras コマンドは、ASA 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。

例

次に、**show h323 ras** コマンドの出力例を示します。

```
ciscoasa# show h323 ras
ciscoasa#
Total: 1
        GK                      Caller
        172.30.254.214 10.130.56.14
```

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
inspect h323	H.323 アプリケーション インスペクションをイネーブルにします。
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ASA間で確立された H.245 セッションの情報を表示します。
timeout h225 | h323	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

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

show history コマンドを使用すると、以前入力したコマンドを表示できます。上矢印と下矢印を使用してコマンドを個別に調べて、**^p** を入力して以前に入力した行を表示するか、**^n** を入力して次の行を表示できます。

例

次に、ユーザ EXEC モードで **show history** コマンドを使用する例を示します。

```
ciscoasa> show history
    show history
    help
    show history
```

次に、特権 EXEC モードで **show history** コマンドを使用する例を示します。

```
ciscoasa# show history
    show history
    help
    show history
    enable
    show history
```

次に、グローバル コンフィギュレーション モードで **show history** コマンドを使用する例を示します。

```
ciscoasa(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情報を表示します。

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

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドはすでに存在していました。

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

次に、ICMP コンフィギュレーションを表示する例を示します。

```
ciscoasa# show icmp
```

関連コマンド

clear configure icmp	ICMP コンフィギュレーションをクリアします。
debug icmp	ICMP のデバッグ情報の表示をイネーブルにします。
icmp	ASAインターフェイスが終端となる ICMP トラフィックのアクセスルールを設定します。
inspect icmp	ICMP インスペクション エンジンをイネーブルまたはディセーブルにします。
timeout icmp	ICMP のアイドル タイムアウトを設定します。

show idb

Interface Descriptor Block のステータスについての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

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

IDB はインターフェイス リソースを表す内部データ構造です。出力の説明については、「例」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。

```
ciscoasa# 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 7-4 に、各フィールドの説明を示します。

表 7-4　show idb stats の各フィールド

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、システム内の各ハードウェア ポートについて作成されます。
SWIDBs	すべての SWIDB の統計情報を表示します。SWIDB は、システム内の各メインおよびサブインターフェイスについて、およびコンテキストに割り当てられている各インターフェイスについて作成されます。 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 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 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
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。

show igmp groups

ASAに直接接続された受信者、および IGMP によって学習された受信者を含むマルチキャスト 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**]

構文の説明

detail	(任意) ソースの詳細説明を出力します。
group	(任意) IGMP グループのアドレス。このオプション引数を含めると、表示は指定されたグループに限定されます。
if_name	(任意) 指定されたインターフェイスについてのグループ情報を表示します。
reserved	(任意) 予約されたグループについての情報を表示します。
summary	(任意) 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

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

オプションの引数およびキーワードをすべて省略すると、**show igmp groups** コマンドは、直接接続されたマルチキャスト 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。

```
ciscoasa# 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
show igmp interface	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*]

構文の説明

if_name	（任意）選択したインターフェイスについての 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

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが変更されました。**detail** 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* 引数を省略すると、**show igmp interface** コマンドはすべてのインターフェイスについて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。

```
ciscoasa# 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
show igmp groups	ASAに直接接続されている受信者、および IGMP を通じて学習された受信者を含むマルチキャスト グループを表示します。

show igmp traffic

IGMP トラフィックの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

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

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

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

show import webvpn

ASAまたは Anyconnect セキュア モビリティ クライアントをカスタマイズおよびローカライズする、フラッシュ メモリ内のファイル、カスタマイゼーション オブジェクト、変換テーブル、またはプラグインを一覧表示するには、特権 EXEC モードで **show import webvpn** コマンドを使用します。

show import webvpn {**AnyConnect-customization** | **customization** | **mst-translation** | **plug-in** | **translation-table** | **url-list** | **webcontent**}[**detailed** | **xml-output**]

構文の説明

AnyConnect-customization	AnyConnect クライアント GUI をカスタマイズする、ASAフラッシュ メモリ内のリソース ファイル、実行可能ファイルおよび MS トランスフォームを表示します。
customization	クライアントレス VPN ポータルをカスタマイズする、ASAフラッシュ メモリ内の XML カスタマイゼーション オブジェクトを表示します(ファイル名は base64 デコード済み)。
mst-translation	AnyConnect クライアント インストーラ プログラムを翻訳する、ASAフラッシュ メモリ内の MS トランスフォームを表示します。
plug-in	ASAフラッシュ メモリ内のプラグイン モジュールを表示します(SSH、VNC、および RDP などのサードパーティの Java ベースのクライアント アプリケーション)。
translation-table	クライアントレス ポータル、Secure Desktop およびプラグインによって表示されるユーザ メッセージの言語を変換する、ASAフラッシュ メモリ内の変換テーブルを表示します。
url-list	クライアントレス ポータルによって使用される、ASAフラッシュ メモリ内の URL の一覧を表示します(ファイル名は base64 デコード済み)。
webcontent	クライアントレス ポータル、クライアントレス アプリケーションおよびプラグインによって、エンド ユーザに表示されるオンライン ヘルプに使用される、ASAフラッシュ メモリ内のコンテンツを表示します。
detailed	フラッシュ メモリ内のファイルおよびハッシュのパスを表示します。
xml-output	ファイルの XML 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

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
8.2(1)	**AnyConnect-customization** キーワードが追加されました。

使用上のガイドライン

show import webvpn コマンドを使用すると、クライアントレス SSL VPN ユーザが使用可能なカスタム データおよび Java ベースのクライアント アプリケーションが識別されます。表示されるリストでは、ASAのフラッシュ メモリにある要求されるすべてのデータ タイプの詳細が表示されます。

例

次に、さまざまな **show import webvpn** コマンドによって表示される WebVPN データの例を示します。

```
ciscoasa# show import webvpn plug
ssh
rdp
vnc
ciscoasa#

ciscoasa#show import webvpn plug detail
post GXN2BIGGOAOkBMibDQsMu2GWZ3Q= Tue, 29 Apr 2008 19:57:03 GMT
rdp fHeyReIOUwDCgAL9HdTsPnjdBOo= Tue, 15 Sep 2009 23:23:56 GMT
rdp2 shw8c22T2SsILLk6zyCd6H6VOz8= Wed, 11 Feb 2009 21:17:54 GMT
ciscoasa# show import webvpn customization
Template
DfltCustomization
ciscoasa#

ciscoasa# show import webvpn translation-table
Translation Tables' Templates:
  AnyConnect
  PortForwarder
  banners
  csd
  customization
  url-list
  webvpn
Translation Tables:
  ru                                              customization
  ua                                              customization
ciscoasa#

ciscoasa# show import webvpn url-list
Template
No bookmarks are currently defined
ciscoasa#

ciscoasa# show import webvpn webcontent
No custom webcontent is loaded
ciscoasa#
```

関連コマンド

コマンド	説明
revert webvpn all	ASAに現在存在するすべての WebVPN データおよびプラグインを削除します。

show interface

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

show interface [{*physical_interface* | **redundant** *number*}[**.***subinterface*] | *mapped_name* | *interface_name* | **vlan** *number* | **vni** *id* [**summary**]] [**stats** | **detail**]

構文の説明

detail	(任意)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、非対称ルーティングの統計情報(**asr-group** コマンドによって非対称ルーティングがイネーブルになっている場合)が含まれます。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、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、ユーザによる設定は不可能です。情報はデバッグだけを目的としています。
interface_name	(任意)**nameif** コマンド内にインターフェイス名のセットを指定します。
mapped_name	(任意)**allocate-interface** コマンドを使用してマッピング名を割り当てた場合、マルチ コンテキスト モードでその名前を指定します。
physical_interface	(任意)**gigabitethernet 0/1** のようなインターフェイス ID を識別します。有効値については、**interface** コマンドを参照してください。
redundant*number*	(任意)**redundant1** のような冗長インターフェイス ID を識別します。
stats	(デフォルト)インターフェイス情報および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、このキーワードはオプションです。
summary	(オプション)VNI インターフェイスの場合は、VNI インターフェイスのパラメータのみを表示します。
subinterface	(任意)論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。
vlan *number*	(オプション)ASA 5505 または ASASM の場合に、VLAN インターフェイスを指定します。
vni *id*	(オプション)VNI インターフェイスのパラメータ、ステータス、および統計情報と、ブリッジされているインターフェイス(設定されている場合)のステータス、ならびに関連付けられている NVE インターフェイスを表示します。

デフォルト

いずれのオプションも識別しない場合、このコマンドはすべてのインターフェイスについての基本的な統計情報を表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、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変更され、明示的に指定するための **stats** キーワード、および **detail** キーワードが追加されました。
7.0(4)	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)	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。
8.0(2)	冗長インターフェイスのサポートが追加されました。また、サブインターフェイス用の遅延が追加されました。入力リセット ドロップと出力リセット ドロップの 2 つの新しいカウンタが追加されました。
8.2(1)	No buffer の数値が、ブロック割り当てからの失敗の数を示すように変更されました。
8.6(1)	ASA 5512-X ～ ASA 5555-X の共有管理インターフェイス、およびソフトウェア モジュールのコントロール プレーン インターフェイスのサポートが追加されました。管理インターフェイスは **show interface detail** コマンドを使用して Internal-Data0/1 として表示され、コントロール プレーン インターフェイスは Internal-Control0/0 として表示されます。
9.4(1)	**vni** インターフェイス タイプが追加されました。
9.5(1)	クラスタリング サイト固有の MAC アドレスが出力に追加されました。

使用上のガイドライン

1 つの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ときに、あるコンテキストでこのコマンドを入力した場合、ASAは現在のコンテキストの統計情報だけを表示します。物理インターフェイスのシステム実行スペース内でこのコマンドを使用すると、ASAはすべてのコンテキストについて組み合わせた統計情報を表示します。

サブインターフェイスについて表示される統計情報の数は、物理インターフェイスについ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は、システム実行スペースでは使用できません。これは、**nameif** コマンドはコンテキスト内だけで使用できるためです。同様に、**allocate-interface** コマンドを使用してインターフェイス ID をマッピング名にマッピングした場合、そのマッピング名はコンテキスト内だけで使用できます。**allocate-interface** コマンドで **visible** キーワードを設定した場合、ASAは **show interface** コマンドの出力にインターフェイス ID を表示します。

(注) Hardware カウントと Traffic Statistics カウントでは、送信または受信されるバイト数が異なります。

Hardware カウントでは、この量はハードウェアから直接取得され、レイヤ 2 パケットのサイズが反映されます。一方、Traffic Statistics では、レイヤ 3 パケットのサイズが反映されます。

カウントの差はインターフェイス カード ハードウェアの設計に基づいて異なります。

たとえば、ファスト イーサネット カードの場合、レイヤ 2 カウントはイーサネット ヘッダーを含むため、トラフィック カウントよりも 14 バイト大きくなります。ギガビット イーサネット カードの場合、レイヤ 2 カウントはイーサネット ヘッダーと CRC の両方を含むため、トラフィック カウントよりも 18 バイト大きくなります。

出力の説明については、「例」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。

```
ciscoasa# show interface
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        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
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/7)
        output queue (curr/max packets): hardware (0/13)
  Traffic Statistics for "outside":
        1328509 packets input, 99873203 bytes
        124606 packets output, 84502975 bytes
        524605 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 GigabitEthernet0/1 "inside", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        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
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/0)
        output queue (curr/max packets): hardware (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 GigabitEthernet0/2 "faillink", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        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
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/0)
        output queue (curr/max packets): hardware (0/0)
  Traffic Statistics for "faillink":
        0 packets input, 0 bytes
        1 packets output, 28 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 GigabitEthernet0/3 "", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
        Active member of Redundant5
        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
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/0)
        output queue (curr/max packets): hardware (0/0)
Interface Management0/0 "", is administratively down, line protocol is down
  Hardware is i82557, BW 100 Mbps, DLY 1000 usec
        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 packets): hardware (128/128) software (0/0)
        output queue (curr/max packets): hardware (0/0) software (0/0)
Interface Redundant1 "", is down, line protocol is down
  Redundancy Information:
        Members unassigned
Interface Redundant5 "redundant", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
        MAC address 000b.fcf8.c451, MTU 1500
        IP address 10.2.3.5, 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
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/0) software (0/0)
```

```
        output queue (curr/max packets): hardware (0/0) software (0/0)
  Traffic Statistics for "redundant":
        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
  Redundancy Information:
        Member GigabitEthernet0/3(Active), GigabitEthernet0/2
        Last switchover at 15:15:26 UTC Oct 24 2006
Interface Redundant5.1 "", is down, line protocol is down
        VLAN identifier none
        Available but not configured with VLAN or via nameif
```

次の出力は、使用している場合のサイト MAC アドレスの使用状況を示しています。

```
ciscoasa# show interface port-channel1.3151
Interface Port-channel1.3151 "inside", is up, line protocol is up
    Hardware is EtherChannel/LACP, BW 1000 Mbps, DLY 10 usec
        VLAN identifier 3151
        MAC address aaaa.1111.1234, MTU 1500
        Site Specific MAC address aaaa.1111.aaaa
        IP address 10.3.1.1, subnet mask 255.255.255.0
    Traffic Statistics for "inside":
        132269 packets input, 6483425 bytes
        1062 packets output, 110448 bytes
        98530 packets dropped
```

表 7-5 に、各フィールドの説明を示します。

表 7-5　show interface の各フィールド

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、**allocate-interface** コマンドで **visible** キーワードを設定しない限り、ASAはマッピング名（設定されている場合）を表示します。
“*interface_name*”	**nameif** コマンドで設定されたインターフェイス名。システム実行スペースでは、システムに名前を設定できないため、このフィールドはブランクです。名前を設定しない場合、Hardware 行の下に次のメッセージが表示されます。 `Available but not configured via nameif`
is *state*	管理ステートは次のとおりです。 • up：インターフェイスはシャットダウンされません。 • administratively down：インターフェイスは、**shutdown** コマンドを使用してシャットダウンされます。
Line protocol is *state*	回線ステータスは次のとおりです。 • up：動作す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。 • down：ケーブルが正しくないか、インターフェイス コネクタに接続されていません。
VLAN identifier	サブインターフェイスの場合、VLAN ID。

表 7-5　show interface の各フィールド(続き)

フィールド	説明
Hardware	インターフェイスのタイプ、最大帯域幅、遅延、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ともに表示されます。次に、一般的なハードウェア タイプを示します。 • 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 • 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 • i82546GB：ASA プラットフォーム上で使用される Intel PCI-X 銅線ギガビット • i82547GI：ASA プラットフォーム上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 • i82557：ASA プラットフォーム上で使用される Intel PCI 銅線ファスト イーサネット • i82559：PIX プラットフォームで使用される Intel PCI 銅線ファスト イーサネット • VCS7380：SSM-4GE で使用される Vitesse 4 ポート ギガビット スイッチ
Media-type	(4GE SSMインターフェイスの場合のみ)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示します。

message area	一部の状況で、メッセージが表示される場合もあります。次の例を参照してください。
	• システム実行スペースで、次のメッセージが表示される場合があります。
	`Available for allocation to a context`
	• 名前を設定しない場合、次のメッセージが表示されます。
	`Available but not configured via nameif`
	• インターフェイスが冗長インターフェイスのメンバの場合、次のメッセージが表示されます。
	`Active member of Redundant5`

MAC address	インターフェイスの MAC アドレス。
Site Specific MAC address	クラスタリングの場合に、使用中のサイト固有の MAC アドレスを表示します。
MTU	このインターフェイス上で許可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ない場合、このフィールドには「MTU not set」と表示されます。
IP address	**ip address** コマンドを使用して設定したか、DHCP サーバから受信したインターフェイスの IP アドレス。システム実行スペースでは、システムに IP アドレスを設定できないため、このフィールドには「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したパケットの数。

表 7-5　　show interface の各フィールド(続き)

フィールド	説明
Bytes	このインターフェイスで受信したバイト数。
No buffer	ブロック割り当てからの失敗の数。
Received:	
Broadcasts	受信したブロードキャストの数。
Input errors	次に示すタイプを含めた入力エラーの総数。入力に関係する他のエラーも入力エラーのカウント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含んでいることもあります。したがって、この合計数は、次に示すタイプについて表示されるエラーの数を超えることがあります。
Runts	最小のパケット 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。ラントは通常、コリジョンによって発生します。不適切な配線や電気干渉によって発生することもあります。
Giants	最大パケット サイズを超えたため廃棄されるパケットの数。たとえば、1518 バイトよりも大きいイーサネット パケットはジャイアントと見なされます。
CRC	巡回冗長検査エラーの数。ステーションがフレームを送信すると、フレームの末尾に CRC を付加します。この CRC は、フレーム内のデータに基づくアルゴリズムから生成されます。送信元と宛先の間でフレームが変更された場合、ASAは CRC が一致しないことを通知します。CRC の数値が高いことは、通常、コリジョンの結果であるか、ステーションが不良データを送信することが原因です。
Frame	フレーム エラーの数。不良フレームには、長さが正しくないパケットや、フレーム チェックサムが正しくないパケットがあります。このエラーは通常、コリジョンまたはイーサネット デバイスの誤動作が原因です。
Overrun	ASAのデータ処理能力を入力レートが超えたため、ASAがハードウェア バッファに受信したデータを処理できなかった回数。
Ignored	このフィールドは使用されません。値は常に 0 です。
Abort	このフィールドは使用されません。値は常に 0 です。
L2 decode drops	名前がまだ設定されていないか(**nameif**コマンド)、無効な VLAN ID を持つフレームが受信されたためにドロップしたパケットの数。冗長インターフェイス コンフィギュレーションのスタンバイ インターフェイスでは、このインターフェイスに名前(**nameif コマンド**)が設定されていないため、カウンタが増加する可能性があります。
Packets output	このインターフェイスに送信されたパケットの数。
Bytes	このインターフェイスに送信されたバイトの数。
Underruns	ASAが処理できるよりも速くトランスミッタが稼働した回数。
Output Errors	設定されたコリジョンの最大数を超えたため送信されなかったフレームの数。このカウンタは、ネットワーク トラフィックが多い場合にのみ増加します。
Collisions	イーサネット コリジョン(単一および複数のコリジョン)が原因で再送信されたメッセージの数。これは通常、過渡に延長した LAN で発生します(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、ステーション間のリピータが 2 つよりも多い、またはマルチポート トランシーバのカスケードが多すぎる場合)。衝突するパケットは、出力パケットによって 1 回だけカウントされます。

表 7-5　　show interface の各フィールド(続き)

フィールド	説明
Interface resets	インターフェイスがリセットされた回数。インターフェイスで 3 秒間送信できない場合、ASAはインターフェイスをリセットして送信を再開します。この間隔では、接続状態が維持されます。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またはシャットダウンする場合も発生します。
Babbles	未使用。(「バブル」は、トランスミッタが最長フレームの送信に要した時間よりも長くインターフェイスに留まっていたことを意味します)。
Late collisions	通常のコリジョン ウィンドウの外側でコリジョンが発生したため、送信されなかったフレームの数。レイト コリジョンは、パケットの送信中に遅れて検出されるコリジョンです。これは通常発生しません。2 つのイーサネット ホストが同時に通信しようとした場合、早期にパケットが衝突して両者がバックオフするか、2 番めのホストが 1 番めのホストの通信状態を確認して待機します。 レイト コリジョンが発生すると、デバイスは割り込みを行ってイーサネット上にパケットを送信しようとしますが、ASAはパケットの送信を部分的に完了しています。ASAは、パケットの最初の部分を保持するバッファを解放した可能性があるため、パケットを再送しません。このことはあまり問題になりません。その理由は、ネットワーキング プロトコルはパケットを再送することでコリジョンを処理する設計になっているためです。ただし、レイト コリジョンはネットワークに問題が存在することを示しています。一般的な問題は、リピータで接続された大規模ネットワーク、および仕様の範囲を超えて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送信前に保留されたフレームの数。
input reset drops	リセットが発生したときに RX リングでドロップしたパケットの数をカウントします。
output reset drops	リセットが発生したときに TX リングでドロップしたパケットの数をカウントします。
Rate limit drops	(4GE SSMインターフェイスの場合だけ)ギガビット以外の速度でインターフェイスを設定して、設定に応じて 10 Mbps または 100 Mbps を超えて送信しようとした場合にドロップされたパケットの数。
Lost carrier	送信中に搬送波信号が消失した回数。
No carrier	未使用。
Input queue (curr/max packets):	入力キュー内のパケットの数(現行値と最大値)。
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。ギガビット イーサネット インターフェイスでは使用できません。
Output queue (curr/max packets):	出力キュー内のパケットの数(現行値と最大値)。
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 7-5　　show interface の各フィールド(続き)

フィールド	説明
input queue (blocks free curr/low)	curr/low エントリは、インターフェイスの受信(入力)記述子リング上の現在のスロットおよび使用可能な all-time-lowest スロットの番号を示します。これらは、メイン CPU によって更新されるため、all-time-lowest(インターフェイス統計情報が削除されるか、またはデバイスがリロードされるまで)の水準点はあまり正確ではありません。
output queue (blocks free curr/low)	curr/low エントリは、インターフェイスの送信(出力)記述子リング上の現在のスロットおよび使用可能な all-time-lowest スロットの番号を示します。これらは、メイン CPU によって更新されるため、all-time-lowest(インターフェイス統計情報が削除されるか、またはデバイスがリロードされるまで)の水準点はあまり正確ではありません。
Traffic Statistics:	受信、送信、またはドロップしたパケットの数。
Packets input	受信したパケットの数とバイトの数。
Packets output	送信し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。このカウンタは通常、高速セキュリティ パス(ASP)上でドロップしたパケットについて増分します(たとえば、アクセスリスト拒否が原因でパケットをドロップした場合など)。 インターフェイス上でドロップが発生する原因については、**show asp drop** コマンドを参照してください。
1 minute input rate	過去 1 分間に受信したパケットの数(パケット/秒およびバイト/秒)。
1 minute output rate	過去 1 分間に送信したパケットの数(パケット/秒およびバイト/秒)。
1 minute drop rate	過去 1 分間にドロップしたパケットの数(パケット/秒)。
5 minute input rate	過去 5 分間に受信したパケットの数(パケット/秒およびバイト/秒)。
5 minute output rate	過去 5 分間に送信したパケットの数(パケット/秒およびバイト/秒)。
5 minute drop rate	過去 5 分間にドロップしたパケットの数(パケット/秒)。
Redundancy Information:	冗長インターフェイスについて、メンバー物理インターフェイスを示します。アクティブ インターフェイスの場合はインターフェイス ID の後に「(Active)」と表示されます。 メンバーをまだ割り当てていない場合、次の出力が表示されます。 `Members unassigned`
Last switchover	冗長インターフェイスの場合、アクティブ インターフェイスがスタンバイ インターフェイスにフェールオーバーした時刻を表示します。

次に、スイッチ ポートを含む ASA 5505 上での **show interface** コマンドの出力例を示します。

```
ciscoasa# show interface
Interface Vlan1 "inside", is up, line protocol is up
  Hardware is EtherSVI, BW 100 Mbps, DLY 100 usec
        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, DLY 1000 usec
            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 7-7 に、ASA 5505 適応型セキュリティ アプライアンスのスイッチ インターフェイスなどのスイッチ インターフェイスに対する **show interface** コマンドの各フィールドの説明を示します。**show interface** コマンドでも表示されるフィールドについては、表 7-6 を参照してください。

表 7-6　スイッチ インターフェイスについての show interface の各フィールド

フィールド	説明
switch ingress policy drops	このドロップは通常、ポートが正しく設定されていないときに表示されます。このドロップは、デフォルトまたはユーザ設定のスイッチ ポート設定の結果としてスイッチ ポート内でパケットが正常に転送できない場合に増分されます。このドロップの原因として、次のコンフィギュレーションが考えられます。 • **nameif** コマンドが VLAN インターフェイス上で設定されていない。 (注)　同じ VLAN 内のインターフェイスに、**nameif** コマンドが設定されていなかった場合でも、VLAN 内のスイッチングは正常で、このカウンタは増分されません。 • VLAN がシャットダウンしている。 • アクセス ポートで 802.1Q タグが付いたパケットを受信した。 • トランク ポートで許可されないタグまたはタグのないパケットを受信した。 • ASAが、イーサネット キープアライブを持つ別のシスコ デバイスに接続されている。たとえば、Cisco IOS ソフトウェアではインターフェイス ヘルス状態を確認するためにイーサネット ループバック パケットを使用します。このパケットは、他のデバイスによって受信されるためのものではなく、パケットをただ送信できることによって、ヘルス状態が確認されます。これらのタイプのパケットはスイッチ ポートでドロップされ、カウンタが増分されます。
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。次に、すべてのインターフェイス（プラットフォームに存在する場合は内部インターフェイスを含む）についての詳細なインターフェイス統計情報および非対称ルーティング統計情報（**asr-group** コマンドでイネーブルにされている場合）を表示する例を示します。

```
ciscoasa# show interface detail
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        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 packets): hardware (0/7)
        output queue (curr/max packets): hardware (0/13)
  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, DLY 1000 usec
        (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 packets): hardware (0/2) software (0/0)
        output queue (curr/max packets): hardware (0/0) software (0/0)
   Control Point Interface States:
        Interface number is unassigned
...
```

表 7-7 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** コマンドでも表示されるフィールドについては、表 7-7 を参照してください。

表 7-7　show interface detail の各フィールド

フィールド	説明
Demux drops	(内部データ インターフェイスのみ)ASAがSSM インターフェイスからのパケットを逆多重化できなかったためドロップしたパケットの数。SSMインターフェイスはバックプレーンを介してネイティブ インターフェイスと通信し、すべての SSM インターフェイスからのパケットはバックプレーン上で多重化されます。
Control Point Interface States:	
Interface number	デバッグに使用される 0 から始まる番号で、このインターフェイスが作成された順番を示します。
Interface config status	管理ステートは次のとおりです。 • active:インターフェイスはシャット ダウンされていません。 • not active:インターフェイスは **shutdown** コマンドでシャット ダウンされています。
Interface state	インターフェイスの実際の状態。この状態は通常、上記の config status と一致します。ハイ アベイラビリティに設定した場合、ASAは必要に応じてインターフェイスを動作状態またはダウン状態にするため、不一致が生じる可能性があります。
Asymmetrical Routing Statistics:	
Received X1 packets	このインターフェイスで受信した ASR パケットの数。
Transmitted X2 packets	このインターフェイスで送信した ASR パケットの数。
Dropped X3 packets	このインターフェイスでドロップした ASR パケットの数。パケットは、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状態の場合にドロップされることがあります。

次に、ASA 5512-X ～ ASA 5555-X 上の **show interface detail** コマンドの出力例を示します。この例では、ASA とソフトウェア モジュールの両方の管理 0/0 インターフェイス（「Internal-Data0/1」として表示）の統計情報を組み合わせて示しています。出力には、Internal-Control0/0 インターフェイスも示されています。これは、ソフトウェア モジュールと ASA間の制御トラフィックに使用されています。

```
Interface Internal-Data0/1 "ipsmgmt", is down, line protocol is up
  Hardware is , BW Unknown Speed-Capability, DLY 1000 usec
        (Full-duplex), (1000 Mbps)
        Input flow control is unsupported, output flow control is unsupported
        MAC address 0100.0100.0000, MTU not set
        IP address 127.0.1.1, 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 pause input, 0 resume input
        0 L2 decode drops
        182 packets output, 9992 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (0/0)
        output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "ipsmgmt":
        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
  Control Point Interface States:
        Interface number is 11
        Interface config status is active
        Interface state is active

Interface Internal-Control0/0 "cplane", is down, line protocol is up
  Hardware is , BW Unknown Speed-Capability, DLY 1000 usec
        (Full-duplex), (1000 Mbps)
        Input flow control is unsupported, output flow control is unsupported
        MAC address 0100.0100.0000, MTU not set
        IP address 127.0.1.1, 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 pause input, 0 resume input
        0 L2 decode drops
        182 packets output, 9992 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (0/0)
        output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "cplane":
        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
  Control Point Interface States:
        Interface number is 11
        Interface config status is active
        Interface state is active
```

show interface vni 1 コマンドについては、次の出力を参照してください。

```
ciscoasa# show interface vni 1
Interface vni1 "vni-inside", is up, line protocol is up
VTEP-NVE 1
Segment-id 5001
Tag-switching: disabled
MTU: 1500
MAC: aaaa.bbbb.1234
IP address 192.168.0.1, subnet mask 255.255.255.0
Multicast group 239.1.3.3
Traffic Statistics for "vni-inside":
235 packets input, 23606 bytes
524 packets output, 32364 bytes
14 packets dropped
1 minute input rate 0 pkts/sec, 0 bytes/sec
1 minute output rate 0 pkts/sec, 2 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
```

show interface vni 1 summary コマンドについては、次の出力を参照してください。

```
ciscoasa# show interface vni 1 summary
Interface vni1 "vni-inside", is up, line protocol is up
VTEP-NVE 1
Segment-id 5001
Tag-switching: disabled
MTU: 1500
MAC: aaaa.bbbb.1234
IP address 192.168.0.1, subnet mask 255.255.255.0
Multicast group not configured
```

関連コマンド

コマンド	説明
allocate-interface	インターフェイスおよびサブインターフェイスをセキュリティ コンテキストに割り当てます。
clear interface	**show interface** コマンドのカウンタをクリアします。
delay	インターフェイスの遅延メトリックを変更します。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
nameif	インターフェイス名を設定します。
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します。

show interface ip brief

インターフェイスの IP アドレスおよび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**

構文の説明

interface_name	（任意）**nameif** コマンド内にインターフェイス名のセットを指定します。
mapped_name	（任意）**allocate-interface** コマンドを使用してマッピング名を割り当てた場合、マルチ コンテキスト モードでその名前を指定します。
physical_interface	（任意）**gigabiternet0/1** などのインターフェイス ID を指定します。有効値については、**interface** コマンドを参照してください。
subinterface	（任意）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。
vlan *number*	（任意）ASA 5505 適応型セキュリティ アプライアンスなど、組み込みスイッチのあるモデルでは、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、ASA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

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント[1]	シングル	コンテキスト	システム
特権 EXEC	• Yes	• Yes	• Yes	• Yes	—

1. 管理 0/0 インターフェイスまたはサブインターフェイスだけで使用可能です。

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(1)	トランスペアレント モードでの VLAN インターフェイスおよび管理 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だけで指定できます。

出力表示の詳細については、「例」を参照してください。

例

次に、**show ip brief** コマンドの出力例を示します。

```
ciscoasa# 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
```

表 7-8 に、各フィールドの説明を示します。

表 7-8　show interface ip brief の各フィールド

フィールド	説明
Interface	**allocate-interface** コマンドを使用して設定した場合の、マルチ コンテキスト モードでのインターフェイス ID またはマッピング名。すべてのインターフェイスを表示すると、AIPSSMの内部インターフェイスが ASA にインストールされている場合は、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、ユーザによる設定は不可能です。情報はデバッグだけを目的としています。
IP-Address	インターフェイスの IP アドレス。
OK?	この列は現在使用されておらず、常に「Yes」と表示されます。
Method	インターフェイスが IP アドレスを受信した方法。値は次のとおりです。 • unset：IP アドレスは設定されていません。 • manual：実行コンフィギュレーションを設定しました。 • 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。 • DHCP：DHCP サーバから受信しました。
Status	管理ステートは次のとおりです。 • up：インターフェイスはシャットダウンされません。 • administratively down：インターフェイスは、**shutdown** コマンドを使用してシャットダウンされます。
Protocol	回線ステータスは次のとおりです。 • up：動作す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。 • down：ケーブルが正しくないか、インターフェイス コネクタに接続されていません。

関連コマンド

コマンド	説明
allocate-interface	インターフェイスおよびサブインターフェイスをセキュリティ コンテキストに割り当てます。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ip address	インターフェイスの IP アドレス、またはトランスペアレント ファイアウォールの管理 IP アドレスを設定します。
nameif	インターフェイス名を設定します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。

show inventory

製品 ID（PID）、バージョン ID（VID）、およびシリアル番号（SN）が割り当てられているネットワーク デバイスにインストールさ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 モードで **show inventory** コマンドを使用します。

show inventory [*mod_id*]

構文の説明

mod_id	（オプション）モジュール ID またはスロット番号（0 ～ 3）を指定します。

デフォルト

項目のインベントリを表示するスロットを指定しない場合は、すべてのモジュール（電源モジュールを含む）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。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
8.4(2)	SSP の出力が追加されました。さらに、デュアル SSP インストールのサポートが追加されました。
8.6(1)	ASA 5512-X、5515-X、5525-X、5545-X および 5555-X（シャーシ、冗長電源、I/O 拡張カード）の出力が追加されました。
9.1(1)	ASA CX モジュールの出力が追加されました。

使用上のガイドライン

show inventory コマンドは、各シスコ製品についてのインベントリ情報を UDI 形式で取得および表示します。UDI 形式とは、製品 ID（PID）、バージョン番号（VID）、およびシリアル番号（SN）という 3 つの別個のデータ要素の組み合わせです。

PID は製品を発注するための名前で、従来は「製品名」または「部品番号」と呼ばれていました。これは、正しい交換部品を発注するために使用する ID です。

VID は製品のバージョンです。製品が変更されると、VID は、製品の変更通知を管理する業界ガイドラインである Telcordia GR-209-CORE から定めた厳格なプロセスに従って増分されます。

SN はベンダー固有の製品の通し番号です。それぞれの製品には工場で割り当てた独自のシリアル番号があり、現場では変更できません。シリアル番号は、製品の個々の固有のインスタンスを識別するための手段です。シリアル番号は、デバイスのさまざまなコンポーネントに応じてその長さが異なる場合があります。

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には、スロットのようなサブエンティティがあります。各エンティティは、シスコ エンティティごとに階層的に配置された論理的な表示順で別々の行に表示されます。

オプションを指定せずに **show inventory** コマンドを使用すると、ネットワーキング デバイスに取り付けられており、PID が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。

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または表示されません。

(注) 2 つの SSP が同じシャーシに取り付けられている場合は、モジュールの番号がシャーシ内でのモジュールの物理的な場所を示します。スロット 0 に取り付けられた SSP が、常にシャーシ マスターとなります。センサーは、SSP が関連付けられている場合にのみ、出力に表示されます。

出力内の用語 *module* は、物理スロットと同等です。SSP 自体の説明においては、物理スロット 0 に取り付けられている場合には出力に module: 0、それ以外の場合は module: 1 が含まれます。ターゲット SSP がシャーシ マスターである場合、**show inventory** コマンドの出力には電源や冷却ファンが含まれます。それ以外の場合、これらのコンポーネントは省略されます。

ASA 5500-X シリーズのハードウェア上の制限により、シリアル番号が表示されない場合があります。これらのモデルの PCI-E I/O（NIC）オプション カードの UDI 表示では、カード タイプは 2 つのみですが、出力はシャーシ タイプに応じて 6 通りになります。これは、指定されたシャーシに応じて異なる PCI-E ブラケット アセンブリが使用されるためです。次に、各 PCI-E I/O カード アセンブリについて予想される出力を示します。たとえば、Silicom SFP NIC カードが検出された場合、UDI 表示はこのカードが取り付けられているデバイスによって決定されます。VID および S/N の値は N/A です。これは、これらの値が電子的に格納されていないためです。

ASA 5512-X または 5515-X 内の 6 ポート SFP イーサネット NIC カードの場合:

```
Name: "module1", DESCR: "ASA 5512-X/5515-X Interface Card 6-port GE SFP, SX/LX"
PID: ASA-IC-6GE-SFP-A    , VID: N/A, SN: N/A
```

ASA 5525-X 内の 6 ポート SFP イーサネット NIC カードの場合:

```
Name: "module1", DESCR: "ASA 5525-X Interface Card 6-port GE SFP, SX/LX"
PID: ASA-IC-6GE-SFP-B    , VID: N/A, SN: N/A
```

ASA 5545-X または 5555-X 内の 6 ポート SFP イーサネット NIC カードの場合:

```
Name: "module1", DESCR: "ASA 5545-X/5555-X Interface Card 6-port GE SFP, SX/LX"
PID: ASA-IC-6GE-SFP-C    , VID: N/A, SN: N/A
```

ASA 5512-X または 5515-X 内の 6 ポート銅線イーサネット NIC カードの場合:

```
Name: "module1", DESCR: "ASA 5512-X/5515-X Interface Card 6-port 10/100/1000, RJ-45"
PID: ASA-IC-6GE-CU-A    , VID: N/A, SN: N/A
```

ASA 5525-X 内の 6 ポート銅線イーサネット NIC カードの場合:

```
Name: "module1", DESCR: "ASA 5525-X Interface Card 6-port 10/100/1000, RJ-45"
PID: ASA-IC-6GE-CU-B    , VID: N/A, SN: N/A
```

ASA 5545-X または 5555-X 内の 6 ポート銅線イーサネット NIC カードの場合:

```
Name: "module1", DESCR: "ASA 5545-X/5555-X Interface Card 6-port 10/100/1000, RJ-45"
PID: ASA-IC-6GE-CU-C    , VID: N/A, SN: N/A
```

例

次に、キーワードや引数を指定していない **show inventory**コマンドの出力例を示します。この出力例は、ASAに取り付けられている、PID が割り当てられている各シスコ エンティティのリストを示しています（ASA CX モジュール用に使用されているストレージ デバイスを含む）。

```
ciscoasa> show inventory
Name: "Chassis", DESCR: "ASA 5555-X with SW, 8 GE Data, 1 GE Mgmt"
PID: ASA5555            , VID: V01     , SN: FGL170441BU

Name: "power supply 1", DESCR: "ASA 5545-X/5555-X AC Power Supply"
PID: ASA-PWR-AC         , VID: N/A     , SN: 2CS1AX

Name: "Storage Device 1", DESCR: "Micron 128 GB SSD MLC, Model Number: C400-MTFDDAC128MAM"
PID: N/A                , VID: N/A     , SN: MXA174201RR
```

次に、デュアル SSP インストールのシャーシ マスター上の **show inventory** コマンドの出力例を示します。

```
ciscoasa> show inventory
Name: "module 0", DESCR: "ASA 5585-X Security Services Processor-40 w 6GE,4 SFP+"
PID: ASA5585-SSP-40     , VID: V01     , SN: JAF1436ACLJ

Name: "Chassis", DESCR: "ASA 5585-X"
PID: ASA5585            , VID: V01     , SN: 123456789AB

Name: "fan", DESCR: "ASA 5585-X Fan Module"
PID: ASA5585-FAN        , VID: V01     , SN: POG1434000G

Name: "power supply 0", DESCR: "ASA 5585-X AC Power Supply"
PID: ASA5585-PWR-AC     , VID: V01     , SN: POG1434002K
```

表 7-9 に、この出力で表示されるフィールドについて説明します。

表 7-9　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た物理名（テキスト ストリング）。たとえば、コンソール、SSP、または「1」などの簡易コンポーネント番号（ポートまたはモジュールの番号）など、デバイスの物理コンポーネント命名構文に応じて異なります。RFC 2737 の entPhysicalName MIB 変数に相当します。
DESCR	オブジェクトを特徴付けるシスコ 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	エンティティ製品 ID。RFC 2737 の entPhysicalModelName MIB 変数に相当します。
VID	エンティティのバージョン番号。RFC 2737 の entPhysicalHardwareRev MIB 変数に相当します。
SN	エンティティのシリアル番号。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
show diag	ネットワーキング デバイスのコントローラ、インターフェイス プロセッサ、およびポート アダプタについての診断情報を表示します。
show tech-support	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 IP アドレス（トランスペアレント モードの場合は管理 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*]

構文の説明

interface_name	（任意）**nameif** コマンド内にインターフェイス名のセットを指定します。
mapped_name	（任意）**allocate-interface** コマンドを使用してマッピング名を割り当てた場合、マルチ コンテキスト モードでその名前を指定します。
physical_interface	（任意）**gigabiternet0/1** などのインターフェイス ID を指定します。有効値については、**interface** コマンドを参照してください。
subinterface	（任意）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。
vlan *number*	（任意）ASA 5505 適応型セキュリティ アプライアンスなど、組み込みスイッチのあるモデルでは、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、ASAはすべてのインターフェイス IP アドレスを表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	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

このコマンドは、ハイ アベイラビリティを設定するときのためのプライマリ IP アドレス（表示では「System」と記載される）と現在の IP アドレスを表示します。ユニットがアクティブの場合、システム IP アドレスと現在の IP アドレスは一致します。ユニットがスタンバイの場合、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。

```
ciscoasa# 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 7-10 に、各フィールドの説明を示します。

表 7-10　　show ip address の各フィールド

フィールド	説明
Interface	**allocate-interface** コマンドを使用して設定した場合の、マルチ コンテキスト モードでのインターフェイス ID またはマッピング名。
Name	**nameif** コマンドで設定され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 アドレスのサブネット マスク。
Method	インターフェイスが IP アドレスを受信した方法。値は次のとおりです。 • unset：IP アドレスは設定されていません。 • manual：実行コンフィギュレーションを設定しました。 • 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。 • DHCP：DHCP サーバから受信しました。

関連コマンド

コマンド	説明
allocate-interface	インターフェイスおよびサブインターフェイスをセキュリティ コンテキストに割り当てます。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
nameif	インターフェイス名を設定します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。
show 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します。

show ip address dhcp

インターフェイスに対する DHCP リースまたは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**}

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

構文の説明

interface_name	**nameif** コマンドを使用して設定されたインターフェイス名を指定します。
lease	DHCP リースに関する情報を表示します。
mapped_name	マルチ コンテキスト モードで、マッピング名を **allocate-interface** 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。
physical_interface	**gigabiternet0/1** などのインターフェイス ID を指定します。有効値については、**interface** コマンドを参照してください。
proxy	IPL テーブル内のプロキシ エントリを表示します。
server	IPL テーブル内のサーバ エントリを表示します。
subinterface	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。
summary	エントリの要約を表示します。

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

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント[1]	シングル	コンテキスト	システム
特権 EXEC	• Yes	—	• Yes	• Yes	—

1. 管理 0/0 インターフェイスまたはサブインターフェイスだけで使用可能です。

コマンド履歴

リリース	変更内容
7.0(1)	新しいサーバ機能に適応するための **lease** キーワードおよび **server** キーワードが追加されました。
7.2(1)	トランスペアレント モードでの VLAN インターフェイスおよび管理 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が追加されました。
9.1(4)	新しいサーバ機能に適応するための **proxy** キーワードおよび **summary** キーワードが追加されました。

使用上のガイドライン　出力の説明については、「例」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。

```
ciscoasa# 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 7-11 に、各フィールドの説明を示します。

表 7-11　show ip address dhcp lease の各フィールド

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 アドレス。
state	DHCP リースの状態で、次のとおりです。 • [Initial]：初期化状態で、ASAがリースを取得するプロセスを開始します。この状態は、リースが終了したか、リースのネゴシエーションに失敗したときにも表示されます。 • [Selecting]：ASAは 1 つ以上の DHCP サーバから DHCPOFFER メッセージを受信することを待機しており、メッセージを選択できます。 • [Requesting]：ASAは、要求を送信した送信先サーバからの応答を待機しています。 • Purging：クライアントが IP アドレスを解放したか、他のエラーが発生したため、ASAはリースを削除します。 • [Bound]：ASAは有効なリースを保持し、正常に動作しています。 • [Renewing]：ASAはリースを更新しようとしています。DHCPREQUEST メッセージを現在の DHCP サーバに定期的に送信し、応答を待機します。 • [Rebinding]：ASAは元のサーバのリースを更新することに失敗したため、いずれかのサーバから応答を受け取るかリースが終了するまで DHCPREQUEST メッセージを送信します。 • [Holddown]：ASAはリースを削除するプロセスを開始しました。 • [Releasing]：ASAは IP アドレスが不要になったことを示すリリース メッセージをサーバに送信します。
DHCP transaction id	クライアントによって選択され、要求メッセージを関連付けるためにクライアントとサーバによって使用される乱数。

表 7-11　　show ip address dhcp lease の各フィールド(続き)

フィールド	説明
Lease	DHCP サーバによって指定される、インターフェイスがこの IP アドレスを使用できる時間の長さ。
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時間の長さ。
Rebind	ASAが DHCP サーバに再バインドしようとするまでの時間の長さ。再バインドが発生するのは、ASAが元の DHCP サーバと通信できず、リース期間の 87.5% を経過した場合です。ASAは、DHCP 要求をブロードキャストすることによって、使用可能な任意の DHCP サーバに接続を試みます。
Temp default-gateway addr	DHCP サーバによって指定されるデフォルト ゲートウェイ アドレス。
Temp ip static route0	デフォルト スタティック ルート。
Next timer fires after	内部タイマーがトリガーするまでの秒数。
Retry count	ASAがリースを設定しようとしているとき、このフィールドは、ASAが DHCP メッセージの送信を試行した回数を示します。たとえば、ASAが Selecting 状態の場合、この値はASAが探索メッセージを送信した回数を示します。ASAが Requesting 状態の場合、この値はASAが要求メッセージを送信した回数を示します。
Client-ID	サーバとのすべての通信に使用したクライアント ID。
Proxy	このインターフェイスが VPN クライアント用のプロキシ DHCP クライアントかどうかを True または False で指定します。
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。

```
ciscoasa# 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 7-12 に、各フィールドの説明を示します。

表 7-12　show ip address dhcp server の各フィールド

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 アドレス。最上位エントリ（「ANY」）はデフォルト サーバで常に存在します。
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、リースの数は一般的に 1 です。VPN 用のプロキシを実行中の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、リースは複数となります。
Offers	サーバからのオファーの数。
Requests	サーバに送信された要求の数。
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拒否の数。
Releases	サーバに送信されたリリースの数。
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
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ip address dhcp	インターフェイスで DHCP サーバから IP アドレスを取得できるように設定します。
nameif	インターフェイス名を設定します。
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します。
show ip address	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** コマンドを使用します。

show ip address {*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name* | **vlan** *number*} **pppoe**

構文の説明

interface_name	**nameif** コマンドを使用して設定されたインターフェイス名を指定します。
mapped_name	マルチ コンテキスト モードで、マッピング名を **allocate-interface** 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。
physical_interface	**gigabiternet0/1** などのインターフェイス ID を指定します。有効値については、**interface** コマンドを参照してください。
subinterface	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。
vlan *number*	（任意）ASA 5505 適応型セキュリティ アプライアンスなど、組み込みスイッチのあるモデルでは、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

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント[1]	シングル	コンテキスト	システム
特権 EXEC	• Yes	• Yes	• Yes	• Yes	—

1. 管理 0/0 インターフェイスまたはサブインターフェイスだけで使用可能です。

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

出力の説明については、「例」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。

```
ciscoasa# show ip address outside pppoe
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ip address ppoe	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。
nameif	インターフェイス名を設定します。
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します。
show ip address	インターフェイスの IP アドレスを表示します。

show ip audit count

監査ポリシーをインターフェイスに適用するときシグニチャの一致数を表示するには、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*]

構文の説明

global	(デフォルト)すべてのインターフェイスについての一致数を表示します。
interface *interface_name*	(任意)指定したインターフェイスについての一致数を表示します。

デフォルト

キーワードを指定しない場合、このコマンドは、すべてのインターフェイスについての一致数を表示します(**global**)。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

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** コマンドを使用します。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。

```
ciscoasa# 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 I DNS Host Info               0
6051 I DNS Zone Xfer               0
6052 I DNS Zone Xfer High Port     0
6053 I 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 ypupdated 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
clear ip audit count	監査ポリシーのシグニチャ一致カウントをクリアします。
ip audit interface	監査ポリシーをインターフェイスに割り当てます。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
show running-config ip audit attack	**ip audit attack** コマンドのコンフィギュレーションを表示します。

show ip local pool

IPv4 アドレス プール情報を表示するには、特権 EXEC モードで **show ip local pool** コマンドを使用します。

show ip local pool interface *pool_name*

構文の説明

pool_name	アドレス プールの名前。プールのリストを確認するには、? を入力します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用し、**ip local pool** コマンドで作成した IPv4 アドレス プールの内容を表示します。これらのプールは、リモート アクセス VPN およびクラスタリングで使用されます。IPv6 アドレス プールを表示するには、**ipv6 local pool** コマンドを使用します。

例

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

```
ciscoasa# show ip local pool test-ipv4-pool
Begin           End             Mask            Free     Held     In use
10.100.10.10    10.100.10.254   255.255.255.0     245        0        0

Available Addresses:
10.100.10.10
10.100.10.11
10.100.10.12
10.100.10.13
10.100.10.14
10.100.10.15
10.100.10.16
...(remaining output redacted)...
```

関連コマンド

コマンド	説明
ip local pool	IPv4 アドレス プールを設定します。

show ip verify statistics

ユニキャスト RPF 機能が原因でドロップし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。ユニキャスト 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*]

構文の説明

interface *interface_name*	（任意）指定したインターフェイスの統計情報を表示します。

デフォルト

このコマンドは、すべてのインターフェイスの統計情報を表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

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

```
ciscoasa# 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
clear configure ip verify reverse-path	**ip verify reverse-path** コンフィギュレーションをクリアします。
clear ip verify statistics	ユニキャスト RPF の統計情報をクリアします。
ip verify reverse-path	IP スプーフィングを防ぐユニキャスト リバース パス転送機能をイネーブルにします。
show running-config ip verify reverse-path	**ip verify reverse-path** コンフィギュレーションを表示します。

show ips

AIP SSMで設定されている使用可能な IPS 仮想センサーをすべて表示するには、特権 EXEC モードで **show ips** コマンドを使用します。

show ips [**detail**]

構文の説明

detail	(任意)センサーの ID 番号と名前を表示します。

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

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

マルチ コンテキスト モードでは、このコマンドは、システム実行スペースで入力するとすべての仮想センサーを表示しますが、コンテキスト実行スペース内ではコンテキストに割り当てられた仮想センサーのみ表示します。仮想センサーをコンテキストに割り当てることについては、**allocate-ips** コマンドを参照してください。

仮想センサーは IPS バージョン 6.0 以降で使用できます。

例

次に、**show ips** コマンドの出力例を示します。

```
ciscoasa# show ips
センサー名
------------
ips1
ips2
```

次に、**show ips detail** コマンドの出力例を示します。

```
ciscoasa# show ips detail
Sensor name              Sensor ID
------------             ---------
ips1                     1
ips2                     2
```

関連コマンド

コマンド	説明
allocate-ips	セキュリティ コンテキストに仮想センサーを割り当てます。
ips	トラフィックを AIP SSMに迂回させます。

show ipsec df-bit

指定されたインターフェイスの IPsec パケットの IPsec do-not-fragment（DF ビット）ポリシーを表示するには、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 df-bit**コマンドを使用します。また、同じ意味を持つ **show crypto ipsec df-bit** コマンドも使用できます。

show ipsec df-bit *interface*

構文の説明

interface	インターフェイス名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

d f ビットの設定によって、カプセル化されたヘッダーの do-not-fragment（DF）ビットのシステムによる処理方法が決まります。IP ヘッダー内の DF ビットにより、デバイスがパケットをフラグメント化できるかどうかが決定されます。この設定に基づき、システムは暗号の適用時に外側の IPsec ヘッダーに対するクリアテキスト パケットの DF ビットの設定をクリアするか、設定するか、コピーするかのいずれかを実行します。

例

次に、inside というインターフェイスの IPsec DF ビット ポリシーを表示する例を示します。

```
ciscoasa(config)# show ipsec df-bit inside
df-bit inside copy
ciscoasa(config)#
```

関連コマンド

コマンド	説明
crypto ipsec df-bit	IPsec パケットの IPsec DF ビット ポリシーを設定します。
crypto ipsec fragmentation	IPsec パケットのフラグメンテーション ポリシーを設定します。
show crypto ipsec fragmentation	IPsec パケットのフラグメンテーション ポリシーを表示します。

show crypto ipsec fragmentation

IPsec パケットのフラグメンテーション ポリシーを表示するには、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 fragmentation** コマンドを使用します。また、同じ意味を持つ **show crypto ipsec fragmentation** コマンドも使用できます。

show ipsec fragmentation *interface*

構文の説明

interface	インターフェイス名を指定します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

VPN に対するパケットを暗号化する際、システムはパケット長をアウトバウンド インターフェイスの MTU と比較します。パケットの暗号化が MTU を超える場合は、パケットをフラグメント化する必要があります。このコマンドは、パケットを暗号化した後（after-encryption）、または暗号化する前（before-encryption）にシステムがパケットをフラグメント化するかどうかを表示します。暗号化前のパケットのフラグメント化は、事前フラグメント化とも呼ばれ、暗号化パフォーマンス全体を向上させるため、システムのデフォルト動作になっています。

例

次に、グローバル コンフィギュレーション モードで、inside という名前のインターフェイスの IPsec フラグメンテーション ポリシーを表示する例を示します。

```
ciscoasa(config)# show ipsec fragmentation inside
fragmentation inside before-encryption
ciscoasa(config)#
```

関連コマンド

コマンド	説明
crypto ipsec fragmentation	IPsec パケットのフラグメンテーション ポリシーを設定します。
crypto ipsec df-bit	IPsec パケットの DF ビット ポリシーを設定します。
show ipsec df-bit	指定したインターフェイスの DF ビット ポリシーを表示します。

show ipsec policy

OSPFv3 に設定されている IPsec セキュア ソケット API（SS API）セキュリティ ポリシーを表示するには、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 policy** コマンドを使用します。また、このコマンドの別の形式である **show crypto ipsec policy** を使用することもできます。

show ipsec policy

構文の説明

このコマンドには、キーワードや変数はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

例

次に、OSPFv3 認証と暗号方式ポリシーを表示する例を示します。

```
ciscoasa# show ipsec policy

Crypto IPsec client security policy data

Policy name:      OSPFv3-1-256
Policy refcount:  1
Policy flags:     0x00000000
SA handles:       sess 268382208 (0xfff3000) / in 55017 (0xd6e9) / out 90369 (0x16101)
Inbound  ESP SPI:        256 (0x100)
Outbound ESP SPI:        256 (0x100)
Inbound  ESP Auth Key:   12345678901234567890123456789012345678901
Outbound ESP Auth Key:   12345678901234567890123456789012345678901
Inbound  ESP Cipher Key: 123456789012345678901234567890123456789012
Outbound ESP Cipher Key: 123456789012345678901234567890123456789012
Transform set:    esp-aes esp-sha-hmac
```

関連コマンド

コマンド	説明
ipv6 ospf encryption	OSPFv3 の認証と暗号方式ポリシーを設定します。
show crypto sockets	セキュアなソケット情報を表示します。
show ipv6 ospf interface	OSPFv3 インターフェイスに関する情報を表示します。

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。また、このコマンドの代替形式の **show crypto ipsec sa** も使用できます。

show ipsec sa [**assigned-address** *hostname or IP address* | **entry** | **identity** | **inactive** | **map** *map-name* | **peer** *peer-addr*] [**detail**]

構文の説明

assigned-address	(オプション)指定されたホスト名または IP アドレスの IPsec SA を表示します。
detail	(任意)表示されているものに対する詳細なエラー情報を表示します。
entry	(オプション)IPsec SA をピア アドレスの順に表示します。
identity	(オプション)IPsec SA を ID の順に表示します。ESP は含まれません。これは簡略化された形式です。
inactive	(オプション)トラフィックを渡すことができない IPsec SA を表示します。
map *map-name*	(オプション)指定されたクリプト マップの IPsec SA を表示します。
peer *peer-addr*	(オプション)指定されたピア 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

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	OSPFv3 およびマルチ コンテキスト モードのサポートが追加されました。
9.1(4)	割り当てられた IPv6 アドレスを反映し、IKEv2 デュアルトラフィックの実行時に、GRE トランスポート モードのセキュリティ アソシエーションを示すように、出力が更新されました。

例

次に、グローバル コンフィギュレーション モードで、IPsec SA を表示する例を示します。ここには、割り当てられた IPv6 アドレス、およびトランスポート モードと GRE カプセル化の表示が含まれます。

```
ciscoasa(config)# sho ipsec sa
interface: outside
    Crypto map tag: def, seq num: 1, local addr: 75.2.1.23

      local ident (addr/mask/prot/port): (75.2.1.23/255.255.255.255/47/0)
      remote ident (addr/mask/prot/port): (75.2.1.60/255.255.255.255/47/0)
      current_peer: 75.2.1.60, username: rashmi
      dynamic allocated peer ip: 65.2.1.100
      dynamic allocated peer ip(ipv6): 2001:1000::10

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 18, #pkts decrypt: 18, #pkts verify: 18
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 4

     local crypto endpt.: 75.2.1.23/4500, remote crypto endpt.: 75.2.1.60/64251
      path mtu 1342, ipsec overhead 62(44), override mtu 1280, media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: D9C00FC2
      current inbound spi : 4FCB6624

    inbound esp sas:
      spi: 0x4FCB6624 (1338730020)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
         slot: 0, conn_id: 8192, crypto-map: def
         sa timing: remaining key lifetime (sec): 28387
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x0003FFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0xD9C00FC2 (3653242818)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
         slot: 0, conn_id: 8192, crypto-map: def
         sa timing: remaining key lifetime (sec): 28387
         IV size: 8 bytes
        replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

次に、グローバル コンフィギュレーション モードで、IPsec SA を表示する例を示します。ここには使用中の設定が含まれ、トンネルが OSPFv3 として示されています。

```
ciscoasa(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 ={L2L, Transport, Manual key (OSPFv3),}
         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 ={L2L, Transport, Manual key (OSPFv3), }
         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)
ciscoasa(config)#
```

(注) IPSec SA ポリシーに、フラグメンテーションは IPsec 処理の前に発生すると明記されている場合、フラグメンテーション統計情報は、フラグメンテーション前の統計情報です。SA ポリシーに、フラグメンテーションは IPsec 処理の後に発生すると明記されている場合、フラグメンテーション後の統計情報が表示されます。

次に、グローバル コンフィギュレーション モードで、def という名前のクリプト マップの IPsec SA を表示する例を示します。

```
ciscoasa(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
ciscoasa(config)#
```

次に、グローバル コンフィギュレーション モードで、キーワード **entry** に対する IPsec SA を表示する例を示します。

```
ciscoasa(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
ciscoasa(config)#
```

次に、グローバル コンフィギュレーション モードで、キーワード **entry detail** を使用して IPsec SA を表示する例を示します。

```
ciscoasa(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
ciscoasa(config)#
```

次に、キーワード **identity** を使用した IPsec SA の例を示します。

```
ciscoasa(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
```

次に、キーワード **identity** および **detail** を使用した IPsec SA の例を示します。

```
ciscoasa(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
```

次の例では、IPv6 で割り当てられたアドレスに基づいて IPSec SA を表示しています。

```
ciscoasa(config)# sho ipsec sa assigned-address 2001:1000::10
assigned address: 2001:1000::10
    Crypto map tag: def, seq num: 1, local addr: 75.2.1.23

      local ident (addr/mask/prot/port): (75.2.1.23/255.255.255.255/47/0)
```

```
      remote ident (addr/mask/prot/port): (75.2.1.60/255.255.255.255/47/0)
      current_peer: 75.2.1.60, username: rashmi
      dynamic allocated peer ip: 65.2.1.100
      dynamic allocated peer ip(ipv6): 2001:1000::10

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 326, #pkts decrypt: 326, #pkts verify: 326
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0      #TFC
rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 35

      local crypto endpt.: 75.2.1.23/4500, remote crypto endpt.: 75.2.1.60/64251
      path mtu 1342, ipsec overhead 62(44), override mtu 1280, media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: D9C00FC2
      current inbound spi : 4FCB6624

    inbound esp sas:
      spi: 0x4FCB6624 (1338730020)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
         slot: 0, conn_id: 8192, crypto-map: def
         sa timing: remaining key lifetime (sec): 28108
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0xFFFFFFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0xD9C00FC2 (3653242818)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
         slot: 0, conn_id: 8192, crypto-map: def
         sa timing: remaining key lifetime (sec): 28108
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
isakmp enable	IPsec ピアが ASAと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

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

構文の説明

このコマンドには、引数または変数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

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

例

次に、グローバル コンフィギュレーション モードで、次の接続タイプ別に IPsec SA の要約を表示する例を示します。

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

```
ciscoasa(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
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear ipsec sa	IPsec SA を完全に削除するか、特定のパラメータに基づいて削除します。
show ipsec sa	IPsec SA のリストを表示します。
show ipsec stats	IPsec 統計情報のリストを表示します。

show ipsec stats

IPSec 統計情報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 stats** コマンドを使用します。

show ipsec stats

構文の説明

このコマンドには、キーワードや変数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	ESPv3 統計情報が IPSec サブシステムとともに示され、マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

次に、出力エントリが示す内容について説明した表を示します。

出力	説明
IPsec Global Statistics	このセクションは、ASAがサポートする IPsec トンネルの総数に関係します。
Active tunnels	現在接続されている IPsec トンネルの数。
Previous tunnels	接続されたことがある IPsec トンネルの数(アクティブなトンネルを含む)。
Inbound	このセクションは、IPsec トンネルを介して受信した着信暗号トラフィックに関係します。
Bytes	受信した暗号トラフィックのバイト数。
Decompressed bytes	圧縮解除が実行された後に受信された暗号トラフィックのバイト数(該当する場合)。圧縮がイネーブルでない場合、このカウンタは常に上記のカウンタと等しくなるはずです。

出力（続き）	説明（続き）
Packets	受信された IPsec 暗号化パケットの数。
Dropped packets	受信されたがエラーのためドロップされた IPsec 暗号化パケットの数。
Replay failures	受信された IPsec 暗号化パケットについて検出されたアンチリプレイの失敗数。
Authentications	受信された IPsec 暗号化パケットについて実行された認証の成功数。
Authentication failures	受信された IPsec 暗号化パケットについて検出された認証の失敗数。
Decryptions	受信された IPsec 暗号化パケットについて実行された復号化の成功数。
Decryption failures	受信された IPsec 暗号化パケットについて検出された復号の失敗数。
Decapsulated fragments needing reassembly	再構築が必要な IP フラグメントを含む復号 IPSec パケットの数。
Outbound	このセクションは、IPsec トラフィックを介して送信される発信クリアテキスト トラフィックに関係します。
Bytes	IPsec トンネルを介して暗号化および送信されるクリアテキスト トラフィックのバイト数。
Uncompressed bytes	IPsec トンネルを介して暗号化および送信される圧縮解除されたクリアテキスト トラフィックのバイト数。圧縮がイネーブルでない場合、このカウンタは常に上記のカウンタと等しくなるはずです。
Packets	IPsec トンネルを介して暗号化および送信されるクリアテキスト パケットの数。
Dropped packets	IPsec トンネルを介して暗号化および送信されるが、エラーが原因でドロップされたクリアテキスト パケットの数。
Authentications	IPsec トンネルを介して送信されるパケットについて実行された認証の成功数。
Authentication failures	IPsec トンネルを介して送信されるパケットについて検出された認証の失敗数。
Encryptions	IPsec トンネルを介して送信されるパケットについて実行された暗号化の成功数。
Encryption failures	IPsec トンネルを介して送信されるパケットについて検出された暗号化の失敗数。
Fragmentation successes	発信 IPsec パケットの変換の一部として実行されたフラグメンテーション操作の成功数。
Pre-fragmentation successes	発信 IPsec パケット変換の一部として実行された、成功した事前フラグメンテーション操作の数。事前フラグメンテーションは、クリアテキスト パケットが暗号化され、1 つ以上の IPsec パケットとしてカプセル化される前に行われます。

出力（続き）	説明（続き）
Post-fragmentation successes	発信 IPsec パケット変換の一部として実行された、成功した事前フラグメンテーション操作の数。事後フラグメンテーションは、クリアテキスト パケットが暗号化され、IPsec パケットとしてカプセル化されることによって複数の IP フラグメントが作成される前に行われます。これらのフラグメントは、復号化前に再構築する必要があります。
Fragmentation failures	発信 IPsec パケットの変換中に発生したフラグメンテーションの失敗数。
Pre-fragmentation failures	発信 IPsec パケットの変換中に発生したプリフラグメンテーションの失敗数。事前フラグメンテーションは、クリアテキスト パケットが暗号化され、1 つ以上の IPsec パケットとしてカプセル化される前に行われます。
Post-fragmentation failure	発信 IPsec パケットの変換中に発生したポストフラグメンテーションの失敗数。事後フラグメンテーションは、クリアテキスト パケットが暗号化され、IPsec パケットとしてカプセル化されることによって複数の IP フラグメントが作成される前に行われます。これらのフラグメントは、復号化前に再構築する必要があります。
Fragments created	IPsec の変換の一部として作成されたフラグメントの数。
PMTUs sent	IPsec システムによって送信されたパス MTU メッセージの数。IPsec は、暗号化後に、IPsec トンネルを介して送信するには大きすぎるパケットを送信している内部ホストに対して PMTU メッセージを送信します。PMTU メッセージは、ホストの MTU を低くして、IPsec トンネルを介して送信するパケットのサイズを小さくすることをホストに求めるメッセージです。
PMTUs recvd	IPsec システムによって受信されたパス MTU メッセージの数。IPsec は、トンネルを介して送信するパケットが大きすぎてネットワーク要素を通過できない場合、ダウンストリームのネットワーク要素からパス MTU メッセージを受信します。パス MTU メッセージを受信すると、IPsec は通常、トンネル MTU を低くします。
Protocol failures	受信した不正な形式の IPsec パケットの数。
Missing SA failures	指定された IPsec セキュリティ アソシエーションが存在しない、要求された IPsec の動作の数。
System capacity failures	IPsec システムの容量が十分でないためデータ レートをサポートできないことが原因で完了できない IPsec の動作の数。

例

次の例をグローバル コンフィギュレーション モードで入力すると、IPSec 統計情報が表示されます。

```
ciscoasa(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
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear ipsec sa	指定されたパラメータに基づいて、IPsec SA またはカウンタをクリアします。
crypto ipsec transform-set	トランスフォーム セットを定義します。
show ipsec sa	指定されたパラメータに基づいて IPsec SA を表示します。
show ipsec sa summary	IPsec SA の要約を表示します。