CHAPTER 3

integrity コマンド～ ipsec-udp-port コマンド

整合性

AnyConnect IPsec 接続に使用する IKEv2 セキュリティ アソシエーション（SA）の ESP 整合性アルゴリズムを指定するには、IKEv2 ポリシー コンフィギュレーション モードで **integrity** コマンドを使用します。コマンドを削除してデフォルト設定を使用するには、このコマンドの **no** 形式を使用します。

integrity {**md5** | **sha** | **sha256** | **sha384** | **sha512** | **null**}

no integrity {**md5** | **sha** | **sha256** | **sha384** | **sha512** | **null**}

構文の説明

md5	ESP の整合性保護のために MD5 アルゴリズムを指定します。
null	AES-GCM を暗号化アルゴリズムとして指定されている場合に管理者が IKEv2 整合性アルゴリズムとして null を選択できるようにします。
sha	（デフォルト）は、ESP の整合性保護のために米国連邦情報処理標準（FIPS）で定義されたセキュア ハッシュ アルゴリズム（SHA）SHA 1 を指定します。
sha256	256 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
sha384	384 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
sha512	512 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。

デフォルト

デフォルトは **sha**（SHA 1 アルゴリズム）です。

使用上のガイドライン

IKEv2 SA は、IKEv2 ピアがフェーズ 2 で安全に通信できるようにするためにフェーズ 1 で使用されるキーです。**crypto ikev2 policy** コマンドを入力した後、**integrity** コマンドを使用して ESP プロトコルの整合性アルゴリズムを設定します。

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。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
8.4(2)	SHA 2 をサポートするために、**sha256**、**sha384**、および **sha512** の各キーワードが追加されました。
9.0(1)	IKEv2 整合性アルゴリズムとして null オプションが追加されました。

例

次に、IKEv2 ポリシー コンフィギュレーション モードを開始し、整合性アルゴリズムを MD5 に設定する例を示します。

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# integrity md5
```

関連コマンド

コマンド	説明
encryption	AnyConnect IPsec 接続に対して IKEv2 SA の暗号化アルゴリズムを指定します。
group	AnyConnect IPsec 接続に対して IKEv2 SA の Diffie-Hellman グループを指定します。
ライフタイム	AnyConnect IPsec 接続に対して IKEv2 SA の SA ライフタイムを指定します。
prf	AnyConnect IPsec 接続に対して IKEv2 SA の疑似乱数関数を指定します。

intercept-dhcp

DHCP 代行受信をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで **intercept-dhcp enable** コマンドを使用します。実行コンフィギュレーションから **intercept-dhcp** 属性を削除し、ユーザがデフォルトまたはその他のグループ ポリシーから DHCP 代行受信コンフィギュレーションを継承できるようにするには、このコマンドの **no** 形式を使用します。

intercept-dhcp *netmask* {**enable | disable**}

no intercept-dhcp

構文の説明

disable	DHCP 代行受信をディセーブルにします。
enable	DHCP 代行受信をイネーブルにします。
netmask	トンネル IP アドレスのサブネット マスクを提供します。

デフォルト

DHCP 代行受信はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(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

DHCP 代行受信をディセーブルにするには、**intercept-dhcp disable** コマンドを使用します。

スプリット トンネル オプションが 255 バイトを超えていると、Microsoft XP で異常が発生し、ドメイン名が破損します。この問題を回避するには、ASA で送信ルートの数を 27 ～ 40 に制限します。ルートの数はルートのクラスによって異なります。

DHCP 代行受信によって Microsoft XP クライアントは、ASA でスプリット トンネリングを使用できるようになります。ASA は、Microsoft Windows XP クライアント DHCP Inform メッセージに直接応答して、クライアントにトンネル IP アドレス用のサブネット マスク、ドメイン名、およびクラスレス スタティック ルートを提供します。Windows クライアントが XP 以前である場合は、DHCP 代行受信により、ドメイン名およびサブネット マスクが提供されます。これは、DHCP サーバを使用するのが効果的でない環境で役立ちます。

例

次に、FirstGroup というグループ ポリシーに DHCP 代行受信を設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# intercept-dhcp enable
```

interface (global)

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 モードを開始するには、グローバル コンフィギュレーション モードで **interface** コマンドを使用します。サブインターフェイスを削除するには、このコマンドの **no** 形式を使用します。物理インターフェイスまたはマッピングされているインターフェイスは削除できません。

物理インターフェイスの場合（ASASM を除くすべてのモデルが対象）：

interface *physical_interface*

サブインターフェイスの場合（ASA 5505 と ASASM、および ASA 5506-X ～ ASA 5555-X の管理インターフェイスには使用不可）：

interface {*physical_interface* | **redundant** *number* | **port-channel** *number*}**.***subinterface*

no interface {*physical_interface* | **redundant** *number* | **port-channel** *number*}**.***subinterface*

マルチ コンテキスト モードの場合（マッピング名が割り当てられているとき）：

interface *mapped_name*

構文の説明

mapped_name	マルチ コンテキスト モードで、**allocate-interface** コマンドを使用してマッピング名が割り当てられている場合は、マッピング名を指定します。
physical_interface	*type*[*slot*/]*port* という形式で物理インターフェイスのタイプ、スロット、およびポート番号を指定します。タイプとスロット/ポート間のスペースは任意です。 物理インターフェイスのタイプには、次のものがあります。 • **ethernet** • **gigabitethernet** • **tengigabitethernet** • **管理** タイプに続けてスロット/ポートを入力します。たとえば、**GigabitEthernet 0/1** というようになります。 管理インターフェイスは、管理トラフィック専用のインターフェイスです。ただし、モデルによっては、必要に応じて通過トラフィックにも使用できます（**management-only** コマンドを参照）。 インターフェイスのタイプ、スロット、およびポート番号を確認するには、モデルに付属のハードウェア マニュアルを参照してください。
サブインターフェイス	論理サブインターフェイスに指定されている 1 ～ 4294967293 の整数を指定します。サブインターフェイスの最大数は、ASA モデルによって異なります。サブインターフェイスは、ASA 5505 および ASASM や、ASA 5512-X ～ ASA 5555-X の管理インターフェイスには使用できません。プラットフォームあたりのサブインターフェイス（または VLAN）の最大数については構成ガイドを参照してください。VLAN サブインターフェイスが 1 つ以上あるインターフェイスは、自動的に 802.1Q トランクとして設定されます。

デフォルト

デフォルトでは、ASA はすべての物理インターフェイスを対象に **interface** コマンドを自動的に生成します。

マルチ コンテキスト モードでは、ASA は **allocate-interface** コマンドを使用して、コンテキストに割り当てられているすべてのインターフェイスを対象に **interface** コマンドを自動的に生成します。

インターフェイスのデフォルトの状態は、そのタイプおよびコンテキスト モードによって異なります。

- マルチ コンテキスト モード、コンテキスト:システム実行スペース内でのインターフェイスの状態にかかわらず、すべての割り当て済みのインターフェイスがデフォルトでイネーブルになっています。ただし、トラフィックがインターフェイスを通過するためには、そのインターフェイスもシステム実行スペース内でイネーブルになっている必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、それを共有しているすべてのコンテキストでダウンします。
- シングル モードまたはマルチ コンテキスト モード、システム:インターフェイスのデフォルトの状態は次のとおりです。
  - 物理インターフェイス:ディセーブル。
  - サブインターフェイス:イネーブル。ただし、トラフィックがサブインターフェイスを通過するためには、物理インターフェイスもイネーブルになっている必要があります。

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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、サブインターフェイスの新しい命名規則に対応し、インターフェイス コンフィギュレーション モードでは引数が独立したコマンドとなるように変更されました。

使用上のガイドライン

インターフェイス コンフィギュレーション モードでは、インターフェイスのタイプおよびセキュリティ コンテキスト モードに応じて、ハードウェアの設定(物理インターフェイスの場合)、名前の割り当て、VLAN の割り当て、IP アドレスの割り当てをはじめ、数多くの設定を行うことができます。

イネーブルになっているインターフェイスでトラフィックを通過させるには、インターフェイス コンフィギュレーション モード コマンドである **nameif** を設定し、ルーテッド モードの場合には **ip address** も設定します。サブインターフェイスの場合は、**vlan** コマンドも設定します。

インターフェイス設定を変更し、既存接続のタイムアウトを待たずに新しいセキュリティ情報を使用する場合は、**clear local-host** コマンドを使用して接続をクリアできます。

ASA 5512-X ～ ASA 5555-X の Management 0/0 インターフェイスには、次の特性があります。

- 通過トラフィックはサポートされません。
- サブインターフェイスはサポートされません
- プライオリティ キューはサポートされません
- マルチキャスト MAC はサポートされません
- IPS SSP ソフトウェア モジュールによって Management 0/0 インターフェイスは共有されます。ASA と IPS モジュールのそれぞれに別の MAC アドレスと IP アドレスがサポートされます。IPS オペレーティング システムで IPS の IP アドレスのコンフィギュレーションを実行する必要があります。ただし、物理特性（インターフェイスのイネーブル化など）は、ASA 上で設定されます。

例

次に、シングル モードで物理インターフェイスのパラメータを設定する例を示します。

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# speed 1000
ciscoasa(config-if)# duplex full
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```

次に、シングル モードでサブインターフェイスのパラメータを設定する例を示します。

```
ciscoasa(config)# interface gigabitethernet0/1.1
ciscoasa(config-subif)# vlan 101
ciscoasa(config-subif)# nameif dmz1
ciscoasa(config-subif)# security-level 50
ciscoasa(config-subif)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-subif)# no shutdown
```

次に、システム コンフィギュレーション用にマルチ コンテキスト モードでインターフェイス パラメータを設定し、GigabitEthernet 0/1.1 サブインターフェイスをコンテキスト A に割り当てる例を示します。

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# speed 1000
ciscoasa(config-if)# duplex full
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface gigabitethernet0/1.1
ciscoasa(config-subif)# vlan 101
ciscoasa(config-subif)# no shutdown
ciscoasa(config-subif)# context contextA
ciscoasa(config-ctx)# ...
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.1
```

次に、コンテキスト コンフィギュレーション用にマルチ コンテキスト モードでパラメータを設定する例を示します。

```
ciscoasa/contextA(config)# interface gigabitethernet0/1.1
ciscoasa/contextA(config-if)# nameif inside
ciscoasa/contextA(config-if)# security-level 100
ciscoasa/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
ciscoasa/contextA(config-if)# no shutdown
```

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。
member-interface	インターフェイスを冗長インターフェイスに割り当てます。
clear interface	**show interface** コマンドのカウンタをクリアします。
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。
vlan	サブインターフェイスに VLAN を割り当てます。

interface（vpn ロード バランシング）

VPN ロード バランシングの仮想クラスタで VPN ロード バランシング用にデフォルト以外のパブリック インターフェイスまたはプライベート インターフェイスを指定するには、VPN ロード バランシング モードで **interface** コマンドを使用します。このインターフェイス指定を削除し、デフォルトのインターフェイスに戻すには、このコマンドの **no** 形式を使用します。

interface {**lbprivate** | **lbpublic**} *interface-name*

no interface {**lbprivate** | **lbpublic**}

構文の説明

interface-name	VPN ロード バランシング クラスタのパブリック インターフェイスまたはプライベート インターフェイスとして設定されるインターフェイスの名前。
lbprivate	このコマンドが VPN ロード バランシングのプライベート インターフェイスを設定することを指定します。
lbpublic	このコマンドが VPN ロード バランシングのパブリック インターフェイスを設定することを指定します。

デフォルト

interface コマンドを省略した場合、**lbprivate** インターフェイスはデフォルトで **inside** に設定され、**lbpublic** インターフェイスはデフォルトで **outside** に設定されます。

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
vpn ロード バランシング	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

先に **vpn load-balancing** コマンドを使用して、VPN ロード バランシング コンフィギュレーション モードを開始しておく必要があります。

また、あらかじめ **interface**、**ip address**、**nameif** の各コマンドを使用して、このコマンドで指定するインターフェイスを設定し、名前を割り当てておく必要があります。

例

次に、**vpn load-balancing** コマンド シーケンスの例を示します。この中の **interface** コマンドでは、クラスタのプライベート インターフェイスをデフォルト（inside）に戻す「test」インターフェイスとして、クラスタのパブリック インターフェイスを指定しています。

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# no interface lbprivate
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# participate
ciscoasa(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
vpn load-balancing	VPN ロード バランシング コンフィギュレーション モードを開始します。

interface bvi

ブリッジ グループにブリッジ仮想インターフェイス（BVI）を設定するには、グローバル コンフィギュレーション モードで **interface bvi** コマンドを使用します。BVI コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

interface bvi *bridge_group_number*

no interface bvi *bridge_group_number*

構文の説明

bridge_group_number	ブリッジ グループの番号を 1 ～ 100 の範囲で指定します。9.3(1) 以降では、範囲が 1 ～ 250 に拡大されています。

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	—	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.3(1)	250 BVI をサポートするために数値の範囲が 1 ～ 250 に増加しました。
9.6(2)	ブリッジ グループあたりのインターフェイスの最大数が 4 から 64 に拡張されました。

使用上のガイドライン

このコマンドを使用してインターフェイス コンフィギュレーション モードを開始すると、ブリッジ グループの管理用 IP アドレスを設定できます。セキュリティ コンテキストのオーバーヘッドを避けたい場合、またはセキュリティ コンテキストを最大限に使用したい場合、インターフェイスをブリッジ グループにグループ化し、各ネットワークに 1 つずつ複数のブリッジ グループを設定できます。ブリッジ グループのトラフィックは他のブリッジ グループから隔離され、トラフィックは ASA 内の他のブリッジ グループにはルーティングされません。また、トラフィックは外部ルータから ASA 内の他のブリッジ グループにルーティングされる前に、ASA から出る必要があります。ブリッジング機能はブリッジ グループごとに分かれていますが、その他の多くの機能はすべてのブリッジ グループ間で共有されます。たとえば、syslog サーバまたは AAA サーバの設定は、すべてのブリッジ グループで共有されます。セキュリティ ポリシーを完全に分離するには、各コンテキスト内に 1 つのブリッジ グループにして、セキュリティ コンテキストを使用します。コンテキストまたはシングル モードごとに、少なくとも 1 つのブリッジ グループが必要です。

ブリッジ グループにはそれぞれ管理 IP アドレスが必要です。ASA はブリッジ グループが発信元になるパケットの送信元アドレスとして、この IP アドレスを使用します。管理 IP アドレスは、接続されているネットワークと同じサブネット内にある必要があります。IPv4 トラフィックの場合、すべてのトラフィックを通過させるには、管理 IP アドレスが必要です。IPv6 トラフィックの場合は、少なくとも、トラフィックを通過させるリンクローカル アドレスを設定する必要があります。リモート管理などの管理操作を含めたフル機能を実現するために、グローバル管理アドレスを設定することを推奨します。他の管理方法としては、ブリッジ グループとは別に管理インターフェイスを設定する方法があります。

9.2 以前では、シングル モードまたはマルチ モードのコンテキストごとに最大 8 個のブリッジ グループを設定できます。9.3(1) 以降では、最大 250 個のブリッジ グループを設定できます。各ブリッジ グループには、最大 4 つのインターフェイスを含めることができます。9.6(2) 以降では、最大 64 のインターフェイスをブリッジ グループに追加できます。同一インターフェイスを複数のブリッジ グループに割り当てることはできません。少なくとも 1 つのブリッジ グループを使用し、データ インターフェイスがブリッジ グループに属している必要があることに注意してください。

(注) ASA 5505 に複数のブリッジ グループを設定できますが、ASA 5505 のトランスペアレント モードのデータ インターフェイスは 2 つという制限は、実質的にブリッジ グループを 1 つだけ使用できることを意味します。

(注) 個別の管理インターフェイスでは、設定できないブリッジ グループ（ID 301）は、設定に自動的に追加されます。このブリッジ グループはブリッジ グループの制限に含まれません。

(注) ASA では、セカンダリ ネットワーク上のトラフィックはサポートされていません。管理 IP アドレスと同じネットワーク上のトラフィックだけがサポートされています。

例

次の例では、3 つのインターフェイスそれぞれの 2 つのブリッジ グループと管理専用インターフェイスを示します。

```
interface gigabitethernet 0/0
    nameif inside
    security-level 100
    bridge-group 1
    no shutdown
interface gigabitethernet 0/1
    nameif outside
    security-level 0
    bridge-group 1
    no shutdown
interface gigabitethernet 0/2
    nameif dmz
    security-level 50
    bridge-group 1
    no shutdown
interface bvi 1
    ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2

interface gigabitethernet 1/0
    nameif inside
    security-level 100
    bridge-group 2
    no shutdown
```

```
interface gigabitethernet 1/1
    nameif outside
    security-level 0
    bridge-group 2
    no shutdown
interface gigabitethernet 1/2
    nameif dmz
    security-level 50
    bridge-group 2
    no shutdown
interface bvi 2
    ip address 10.3.5.8 255.255.255.0 standby 10.3.5.9

interface management 0/0
    nameif mgmt
    security-level 100
    ip address 10.2.1.1 255.255.255.0 standby 10.2.1.2
    no shutdown
```

関連コマンド

コマンド	説明
ace/bvi	ブリッジ仮想インターフェイスの設定を消去します。
bridge-group	トランスペアレント ファイアウォール インターフェイスをブリッジ グループにグループ化します。
interface	インターフェイスを設定します。
ip address	ブリッジ グループの管理 IP アドレスを設定します。
show bridge-group	メンバ インターフェイスや IP アドレスなど、ブリッジ グループの情報を表示します。
show running-config interface bvi	ブリッジ グループ インターフェイス コンフィギュレーションを表示します。

interface-policy

モニタリングでインターフェイスの障害を検出する際にフェールオーバーのポリシーを指定するには、フェールオーバー グループ コンフィギュレーション モードで **interface-policy** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

interface-policy *num*[**%**]

no interface-policy *num*[**%**]

構文の説明

num	パーセンテージとして使用するときには 1 ～ 100 の数値を指定し、そうでなければインターフェイスの最大数として 1 を指定します。
%	(任意)*num* の数字が、モニタ対象インターフェイスのパーセンテージであることを指定します。

デフォルト

ユニットに **failover interface-policy** コマンドが設定されている場合は、その値が **interface-policy** フェールオーバー グループ コマンドのデフォルトと見なされます。そうでない場合、*num* は 1 となります。

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
フェールオーバー グループ コンフィギュレーション	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
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

num 引数とオプションの **%** キーワードの間にはスペースを挿入しません。

障害が発生したインターフェイスの数が設定したポリシーを満たし、他の ASA が正しく機能している場合、ASA が自らを障害発生としてマークし、フェールオーバーが発生することがあります(アクティブな ASA で障害が発生した場合)。ポリシーでカウントされるのは、**monitor-interface** コマンドでモニタ対象として指定したインターフェイスのみです。

例

次の部分的な例では、フェールオーバー グループで可能な設定を示します。

```
ciscoasa(config)# failover group 1
ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# interface-policy 25%
ciscoasa(config-fover-group)# exit
ciscoasa(config)#
```

関連コマンド

コマンド	説明
failover group	Active/Active フェールオーバーのためのフェールオーバー グループを定義します。
failover interface-policy	インターフェイス モニタリング ポリシーを設定します。
monitor-interface	フェールオーバーのためにモニタ対象にするインターフェイスを指定します。

interface port-channel

EtherChannel 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 モードを開始するには、グローバル コンフィギュレーション モードで **interface port-channel** コマンドを使用します。EtherChannel インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

interface port-channel *number*

no interface port-channel *number*

構文の説明

number	EtherChannel チャネル グループ ID を指定します。範囲は 1 ～48 です。このインターフェイスは、チャネル グループにインターフェイスを追加したときに自動的に作成されたものです。まだインターフェイスを追加していない場合は、このコマンドを実行するとポートチャネル インターフェイスが作成されます。 **（注）** 少なくとも 1 つのメンバ インターフェイスをポートチャネル インターフェイスに追加してからでなければ、インターフェイスの論理パラメータ（名前など）は設定できません。

デフォルト

デフォルトでは、ポートチャネル インターフェイスはイネーブルになっています。ただし、トラフィックが EtherChannel を通過するためには、チャネル グループ物理インターフェイスもイネーブルになっている必要があります。

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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。

使用上のガイドライン

インターフェイス コンフィギュレーション モードでは、名前や IP アドレスの割り当てなど、さまざまな設定を行うことができます。

イネーブルになっているインターフェイスでトラフィックを通過させるには、インターフェイス コンフィギュレーション モード コマンドである **nameif** を設定し、ルーテッド モードの場合には **ip address** も設定します。

インターフェイス設定を変更し、既存接続のタイムアウトを待たずに新しいセキュリティ情報を使用する場合は、**clear local-host** コマンドを使用して接続をクリアできます。

(注) このコマンドは、ASA 5505 または ASASM ではサポートされません。4GE SSM（これには ASA 5550 のスロット 1 の統合 4GE SSM も含まれます）上のインターフェイスを EtherChannel の一部として使用することはできません。

インターフェイスの詳細については、CLI 設定ガイドを参照してください。

例

次の例では、3 つのインターフェイスを EtherChannel の一部として設定します。また、システム プライオリティをより高く設定するとともに、GigabitEthernet 0/2 のプライオリティを他のインターフェイスよりも高く設定します。これは、8 個を超えるインターフェイスが EtherChannel に割り当てられた場合に備えるためです。

```
ciscoasa(config)# lacp system-priority 1234
ciscoasa(config-if)# interface GigabitEthernet0/0
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# interface GigabitEthernet0/1
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# interface GigabitEthernet0/2
ciscoasa(config-if)# lacp port-priority 1234
ciscoasa(config-if)# channel-group 1 mode passive
ciscoasa(config-if)# interface Port-channel1
ciscoasa(config-if)# lacp max-bundle 4
ciscoasa(config-if)# port-channel min-bundle 2
ciscoasa(config-if)# port-channel load-balance dst-ip
```

関連コマンド

コマンド	説明
channel-group	EtherChannel にインターフェイスを追加します。
lacp max-bundle	チャネル グループで許可されるアクティブ インターフェイスの最大数を指定します。
lacp port-priority	チャネル グループの物理インターフェイスのプライオリティを設定します。
lacp system-priority	LACP システム プライオリティを設定します。
port-channel load-balance	ロード バランシング アルゴリズムを設定します。
port-channel min-bundle	ポートチャネル インターフェイスがアクティブになるために必要な、アクティブ インターフェイスの最小数を指定します。
show lacp	LACP 情報（トラフィック統計情報、システム ID、ネイバーの詳細など）が表示されます。
show port-channel	EtherChannel 情報が、詳細に 1 行のサマリー形式で表示されます。このコマンドは、ポートとポートチャネルの情報も表示します。
show port-channel load-balance	ポートチャネル負荷分散情報が、指定のパラメータ セットに対するハッシュ結果および選択されたメンバー インターフェイスとともに表示されます。

interface redundant

冗長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 モードを開始するには、グローバル コンフィギュレーション モードで **interface redundant** コマンドを使用します。冗長インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

interface redundant *number*

no interface redundant *number*

構文の説明

number	論理冗長インターフェイス ID を指定します。範囲は 1 ～8 です。**redundant** と ID 間のスペースは任意です。

デフォルト

デフォルトでは、冗長インターフェイスはイネーブルになっています。ただし、トラフィックが冗長インターフェイスを通過するためには、メンバ物理インターフェイスもイネーブルになっている必要があります。

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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
8.0(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

冗長インターフェイスは、アクティブ物理インターフェイスとスタンバイ物理インターフェイスのペアとなっています（**member-interface** コマンドを参照）。アクティブ インターフェイスで障害が発生すると、スタンバイ インターフェイスがアクティブになって、トラフィックを通過させ始めます。

すべての ASA コンフィギュレーションは、メンバ物理インターフェイスではなく論理冗長インターフェイスを参照します。

インターフェイス コンフィギュレーション モードでは、名前や IP アドレスの割り当てなど、さまざまな設定を行うことができます。

イネーブルになっているインターフェイスでトラフィックを通過させるには、インターフェイス コンフィギュレーション モード コマンドである **nameif** を設定し、ルーテッド モードの場合には **ip address** も設定します。

インターフェイス設定を変更し、既存接続のタイムアウトを待たずに新しいセキュリティ情報を使用する場合は、**clear local-host** コマンドを使用して接続をクリアできます。

(注) このコマンドは、ASA 5505 または ASASM ではサポートされません。

インターフェイスの詳細については、CLI 設定ガイドを参照してください。

例

次の例では、2 つの冗長インターフェイスを作成します。

```
ciscoasa(config)# interface redundant 1
ciscoasa(config-if)# member-interface gigabitethernet 0/0
ciscoasa(config-if)# member-interface gigabitethernet 0/1
ciscoasa(config-if)# interface redundant 2
ciscoasa(config-if)# member-interface gigabitethernet 0/2
ciscoasa(config-if)# member-interface gigabitethernet 0/3
```

関連コマンド

コマンド	説明
clear interface	**show interface** コマンドのカウンタをクリアします。
debug redundant-interface	冗長インターフェイスのイベントまたはエラーに関するデバッグ メッセージを表示します。
member-interface	物理インターフェイスを冗長インターフェイスに割り当てます。
redundant-interface	アクティブなメンバ インターフェイスを変更します。
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。

interface tunnel

新しい VTI トンネル インターフェイスを作成するには、グローバル コンフィギュレーション モードで **interface tunnel** コマンドを使用します。VTI トンネル インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

interface tunnel *number*

no interface tunnel *number*

構文の説明

number	トンネル インターフェイスに番号を割り当てます。0 ～ 100 の任意の値を指定できます。

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
グローバル設定	• 対応	• なし	• 対応	• なし	• -

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドとそのサブモードを導入しました。

例

次に、新しいトンネル インターフェイスを作成する例を示します。

```
ciscoasa(config)# interface tunnel 10
```

関連コマンド

コマンド	説明
tunnel source interface	VTI トンネルを作成するための送信元インターフェイスを指定します。
tunnel destination	VTI トンネルの宛先の IP アドレスを指定します。
トンネル モード	IPsec がトンネル保護に使用されることを指定します。
tunnel protection ipsec	トンネル保護に使用される IPsec プロファイルを指定します。

interface vlan

ASA 5505 および ASASM で、VLAN 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 モードを開始するには、グローバル コンフィギュレーション モードで **interface vlan** コマンドを使用します。VLAN インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

interface vlan *number*

no interface vlan *number*

構文の説明

number	VLAN ID を指定します。 ASA 5505 の場合、1 ～ 4090 の ID を使用します。VLAN インターフェイス ID は、デフォルトでは VLAN 1 でイネーブルになっています。 ASASM の場合は、2 ～ 1000 および 1025 ～ 4094 の ID を使用します。

デフォルト

デフォルトで、VLAN インターフェイスはイネーブルになっています。

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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
8.4(1)	ASASM のサポートが追加されました。

使用上のガイドライン

ASASM では、コンフィギュレーションに任意の VLAN ID を追加できますが、トラフィックを転送できるのはスイッチによって ASA に割り当てられた VLAN だけです。**show vlan** コマンドを使用して、ASA に割り当てられたすべての VLAN を表示します。スイッチによって ASA にまだ割り当てられていない VLAN にインターフェイスを追加した場合、そのインターフェイスはダウン ステートになります。ASA に VLAN を割り当てた時点で、インターフェイスはアップ ステートに変化します。インターフェイス ステートの詳細については、**show interface** コマンドを参照してください。

インターフェイス コンフィギュレーション モードでは、名前や IP アドレスの割り当てなど、さまざまな設定を行うことができます。

イネーブルになっているインターフェイスでトラフィックを通過させるには、インターフェイス コンフィギュレーション モード コマンドである **nameif** を設定し、ルーテッド モードの場合には **ip address** も設定します。ASA 5505 スイッチの物理インターフェイスについては、**switchport access vlan** コマンドを使用して VLAN インターフェイスに割り当てます。

インターフェイス設定を変更し、既存接続のタイムアウトを待たずに新しいセキュリティ情報を使用する場合は、**clear local-host** コマンドを使用して接続をクリアできます。

インターフェイスの詳細については、CLI 設定ガイドを参照してください。

例

次の例では、3 つの VLAN インターフェイスを設定します。3 つめの家庭用インターフェイスは、業務用インターフェイスにトラフィックを転送できません。

```
ciscoasa(config)# interface vlan 100
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address dhcp
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface vlan 200
ciscoasa(config-if)# nameif work
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface vlan 300
ciscoasa(config-if)# no forward interface vlan 200
ciscoasa(config-if)# nameif home
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.2.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/2
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/3
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/4
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# no shutdown
```

次に、**failover lan** コマンドを使用して別途設定されるフェールオーバー インターフェイスを含め、5 つの VLAN インターフェイスを設定する例を示します。

```
ciscoasa(config)# interface vlan 100
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```

```
ciscoasa(config-if)# interface vlan 200
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.2.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface vlan 300
ciscoasa(config-if)# nameif dmz
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.3.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface vlan 400
ciscoasa(config-if)# nameif backup-isp
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# failover lan faillink vlan500
ciscoasa(config)# failover interface ip faillink 10.4.1.1 255.255.255.0 standby 10.4.1.2
255.255.255.0

ciscoasa(config)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/2
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/3
ciscoasa(config-if)# switchport access vlan 400
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/4
ciscoasa(config-if)# switchport access vlan 500
ciscoasa(config-if)# no shutdown
```

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。
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。

interface vni

VXLAN ネットワーク ID（VNI）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 モードを開始するには、グローバル コンフィギュレーション モードで **interface vni** コマンドを使用します。VNI インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

interface vni *number*

no interface vni *number*

構文の説明

number	1 ～ 10000 の範囲で ID を設定します。この ID は内部インターフェイス識別子です。

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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.4(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

vtep-nve コマンドを使用して VNI インターフェイスと VTEP 送信元インターフェイスを関連付ける必要があります。また、VXLAN **セグメント ID** を設定する必要があります。

例

次に、GigabitEthernet 1/1 インターフェイスを VTEP 送信元インターフェイスとして設定し、VNI 1 インターフェイスをそれに関連付ける例を示します。

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config)# nve 1
ciscoasa(cfg-nve)# source-interface outside
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# segment-id 1000
```

```
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# mcast-group 236.0.0.100
```

関連コマンド

コマンド	説明
debug vxlan	VXLAN トラフィックをデバッグします。
default-mcast-group	VTEP 送信元インターフェイスに関連付けられているすべての VNI インターフェイスのデフォルトのマルチキャスト グループを指定します。
encapsulation vxlan	NVE インスタンスを VXLAN カプセル化に設定します。
inspect vxlan	標準 VXLAN ヘッダー形式に強制的に準拠させます。
mcast-group	VNI インターフェイスのマルチキャスト グループ アドレスを設定します。
nve	ネットワーク仮想化エンドポイント インスタンスを指定します。
nve-only	VXLAN 送信元インターフェイスが NVE 専用であることを指定します。
peer ip	ピア VTEP の IP アドレスを手動で指定します。
segment-id	VNI インターフェイスの VXLAN セグメント ID を指定します。
show arp vtep-mapping	リモート セグメント ドメインにある IP アドレスとリモート VTEP IP アドレス用の VNI インターフェイスにキャッシュされた MAC アドレスを表示します。
show interface vni	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。
show mac-address-table vtep-mapping	リモート VTEP IP アドレスが設定された VNI インターフェイス上のレイヤ 2 転送テーブル(MAC アドレス テーブル)を表示します。
show nve	NVE インターフェイスのパラメータ、ステータス、および統計情報とキャリア インターフェイス(送信元インターフェイス)のステータス、この NVE を VXLAN VTEP として使用する VNI、ならびにこの NVE インターフェイスに関連付けられているピア VTEP IP アドレスを表示します。
show vni vlan-mapping	VNI セグメント ID と、VLAN インターフェイスまたはトランスペアレント モードの物理インターフェイス間のマッピングを表示します。
source-interface	VTEP 送信元インターフェイスを指定します。
vtep-nve	VNI インターフェイスを VTEP 送信元インターフェイスに関連付けます。
vxlan port	VXLAN UDP ポートを設定します。デフォルトでは、VTEP 送信元インターフェイスは UDP ポート 4789 への VXLAN トラフィックを受け入れます。

interim-accounting-update

AAA サーバ グループ用の RADIUS 中間アカウンティング更新メッセージの生成をイネーブルにするには、AAA サーバ グループ コンフィギュレーション モードで **interim-accounting-update** コマンドを使用します。中間アカウンティング更新メッセージをディセーブルにするには、このコマンドの **no** 形式を使用します。

interim-accounting-update [**periodic** [*hours*]]

no interim-accounting-update [**periodic** [*hours*]]

構文の説明

periodic [*hours*]	（オプション）対象のサーバ グループにアカウンティング レコードを送信するように設定されたすべての VPN セッションのアカウンティング レコードの定期的な生成と伝送をイネーブルにします。オプションで、これらの更新の送信間隔（時間単位）を含めることができます。デフォルトは 24 時間で、指定できる範囲は 1 ～ 120 時間です。 このオプションは、ISE 認証変更用に設定されたサーバ グループに対して使用します。

デフォルト

デフォルトでは、中間アカウンティング更新はイネーブルになりません。

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
aaa サーバ グループ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	**periodic** キーワードが追加されました。

使用上のガイドライン

periodic キーワードなしでこのコマンドを使用すると、ASA は、VPN トンネル接続がクライアントレス VPN セッションに追加されたときにのみ中間アカウンティング更新メッセージを送信します。これが発生した場合、新たに割り当てられた IP アドレスを RADIUS に通知するためのアカウンティング アップデートが生成されます。

サーバ グループを使用してリモート アクセス VPN の ISE 認可変更を設定する場合は、**periodic** キーワードを追加します。定期期間には、AnyConnect 接続とクライアントレス セッションが含まれます。

ISE は、ASA などの NAS デバイスから受信するアカウンティング レコードに基づいてアクティブ セッションのディレクトリを保持します。ただし、セッションが依然としてアクティブなアカウンティング メッセージ(またはポスチャ トランザクション)であるという通知を 5 日間にわたって受信しない場合、ISE はセッション レコードをデータベースから削除します。長期間アクティブな VPN 接続が削除されないようにするには、すべてのアクティブ セッションに関して定期的な中間アカウンティング更新メッセージを ISE 送信するようにグループを設定します。

例

次の例は、ISE サーバ グループに、動的認可(CoA)のアップデートと時間ごとの定期的なアカウンティングを設定する方法を示しています。ISE によるパスワード認証を設定するトンネル グループ設定が含まれています。

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

次に、ISE でローカル証明書の検証と認可用のトンネル グループを設定する例を示します。この場合、サーバ グループは認証用に使用されないため、**authorize-only** コマンドをサーバ グループ コンフィギュレーションに組み込みます。

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# authorize-only
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication certificate
ciscoasa(config-tunnel-general)# authorization-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

関連コマンド

コマンド	説明
authorize-only	RADIUS サーバ グループ用の認可専用モードをイネーブルにします。
dynamic-authorization	RADIUS サーバ グループ用のダイナミック認可をイネーブルにします。

internal-password

クライアントレス SSL VPN ポータル ページで追加パスワード フィールドを表示するには、webvpn コンフィギュレーション モードで **internal-password** コマンドを使用します。この追加パスワードは、SSO が許可されているユーザをファイル サーバに対して認証するために ASA で使用されます。

内部パスワードの使用をディセーブルにするには、このコマンドの **no** 形式を使用します。

internal-password enable

no internal password

構文の説明

enable	内部パスワードの使用をイネーブルにします。

デフォルト

デフォルトではディセーブルになっています。

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
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
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

イネーブルにした場合、エンド ユーザはクライアントレス SSL VPN セッションにログインするときに 2 つめのパスワードを入力します。クライアントレス SSL VPN サーバは、HTTPS を使用して、ユーザ名やパスワードなどの SSO 認証要求を認証サーバに送信します。認証サーバが認証要求を承認すると、SSO 認証クッキーがクライアントレス SSL VPN サーバに返されます。このクッキーは、ユーザの代理として ASA で保持され、ユーザ認証でこのクッキーを使用して、SSO サーバで保護されているドメイン内部の Web サイトの安全を確保します。

内部パスワード機能は、内部パスワードを SSL VPN パスワードとは異なるものにする場合に便利です。特に、ASA への認証にワンタイム パスワードを使用し、内部サイトの認証に別のパスワードを使用できます。

例

次に、内部パスワードをイネーブルにする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# internal password enable
ciscoasa(config-webvpn)#
```

関連コマンド

コマンド	説明
webvpn	webvpn コンフィギュレーション モードを開始します。このモードではクライアントレス SSL VPN 接続の属性を設定できます。

interval maximum

DDNS 更新方式による更新試行の最大間隔を設定するには、DDNS 更新方式モードで **interval** コマンドを使用します。実行コンフィギュレーションから DDNS 更新方式の間隔を削除するには、このコマンドの **no** 形式を使用します。

interval maximum *days hours minutes seconds*

no interval maximum *days hours minutes seconds*

構文の説明

days	更新試行間の日数を 0 ～ 364 の範囲で指定します。
hours	更新試行間の時間数を 0 ～ 23 の範囲で指定します。
minutes	更新試行間の分数を 0 ～ 59 の範囲で指定します。
seconds	更新試行間の秒数を 0 ～ 59 の範囲で指定します。

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
DDNS 更新方式コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
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

日、時間、分、および秒を足すと、間隔の合計時間になります。

例

次に、3 分 15 秒ごとに更新を試行する方式を ddns-2 という名前で設定する例を示します。

```
ciscoasa(config)# ddns update method ddns-2
ciscoasa(DDNS-update-method)# interval maximum 0 0 3 15
```

関連コマンド

コマンド	説明
ddns	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
ddns update	DDNS アップデート方式を ASA インターフェイスまたは DDNS アップデート ホスト名に関連付けます。
ddns update method	DNS のリソース レコードをダイナミックにアップデートするための方式を作成します。
dhcp-client update dns	DHCP クライアントが DHCP サーバに渡すアップデート パラメータを設定します。
dhcpd update dns	DHCP サーバによる DDNS アップデートの実行をイネーブルにします。

invalid-ack

ACK が無効になっているパケットに対するアクションを設定するには、tcp-map コンフィギュレーション モードで **invalid-ack** コマンドを使用します。値をデフォルトに戻すには、このコマンドの **no** 形式を使用します。このコマンドは、**set connection advanced-options** コマンドを使用してイネーブルにされる TCP 正規化ポリシーの一部です。

invalid-ack {**allow** | **drop**}

no invalid-ack

構文の説明

allow	ACK が無効になっているパケットを許可します。
drop	ACK が無効になっているパケットをドロップします。

デフォルト

デフォルト アクションは、ACK が無効になっているパケットをドロップすることです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(4)/8.0(4)	このコマンドが追加されました。

使用上のガイドライン

TCP 正規化をイネーブルにするには、モジュラ ポリシー フレームワークを次のように使用します。

1. **tcp-map**：TCP 正規化アクションを指定します。
   a. **invalid-ack**：tcp-map コンフィギュレーション モードでは、**invalid-ack** コマンドをはじめ多数のコマンドを入力できます。
2. **class-map**：TCP 正規化を実行するトラフィックを指定します。
3. **policy-map**：各クラス マップに関連付けるアクションを指定します。
   a. **class**：アクションを実行するクラス マップを指定します。
   b. **set connection advanced-options**：作成した TCP マップを指定します。
4. **service-policy**：ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

次のような場合に無効な ACK が検出される可能性があります。

- TCP 接続が SYN-ACK-received ステータスでは、受信した TCP パケットの ACK 番号が次の TCP パケット送信のシーケンス番号と同じでない場合、その ACK は無効です。
- 受信した TCP パケットの ACK 番号が次の TCP パケット送信のシーケンス番号より大きい場合は常に、その ACK は無効です。

(注) 無効な ACK を含む TCP パケットは、WAAS 接続で自動的に許可されます。

例

次に、ACK が無効になっているパケットを許可するように ASA を設定する例を示します。

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# invalid-ack allow
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match any
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
ciscoasa(config)#
```

関連コマンド

コマンド	説明
class-map	サービス ポリシーに対してトラフィックを指定します。
policy-map	サービス ポリシーのトラフィックに適用するアクションを指定します。
set connection advanced-options	TCP 正規化をイネーブルにします。
service-policy	サービス ポリシーをインターフェイスに適用します。
show running-config tcp-map	TCP マップ コンフィギュレーションを表示します。
tcp-map	TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。

ip address

インターフェイスの IP アドレス（ルーテッド モード）や、ブリッジ仮想インターフェイス（BVI）（ルーテッド モードまたはトランスペアレント モード）を設定するには、インターフェイス コンフィギュレーション モードで **ip address** コマンドを使用します。IP アドレスを削除するには、このコマンドの **no** 形式を使用します。

ip address *ip_address* [*mask*] [**standby** *ip_address* | **cluster-pool** *poolname*]

no ip address [*ip_address*]

構文の説明

cluster-pool *poolname*	（オプション）ASA クラスタリングの場合に、**ip local pool** コマンドで定義されたアドレスのクラスタ プールを設定します。*ip_address* 引数で定義されたメイン クラスタの IP アドレスは、現在のマスター ユニットだけに属します。各クラスタ メンバには、このプールからローカル IP アドレスが割り当てられます。 各ユニットに割り当てられるアドレスを、事前に正確に特定することはできません。各ユニットで使用されているアドレスを表示するには、**show ip local pool** *poolname* コマンドを入力します。各クラスタ メンバには、クラスタに参加したときにメンバ ID が割り当てられます。この ID によって、プールから使用されるローカル IP が決定します。
ip_address	インターフェイスの IP アドレス。
mask	（任意）IP アドレスのサブネット マスク。マスクを設定しない場合、ASA では IP アドレス クラスのデフォルト マスクが使用されます。
standby *ip_address*	（オプション）フェールオーバーの場合に、スタンバイ ユニットの IP アドレスを設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	ルーテッド モードの場合、このコマンドは、グローバル コンフィギュレーション コマンドからインターフェイス コンフィギュレーション モードのコマンドに変更されました。
8.4(1)	トランスペアレント モード用にブリッジ グループが追加されました。BVI の IP アドレスを設定し、グローバルには設定しません。
9.0(1)	ASA クラスタリングをサポートするために、**cluster-pool** キーワードが追加されました。
9.7(1)	ルーテッド インターフェイスに関しては、ポイントツーポイント接続向けの 31 ビットのサブネット に IP アドレスを設定できます。

使用上のガイドライン

このコマンドはこの他、フェールオーバーのスタンバイ アドレスを設定します。

マルチ コンテキスト モードのガイドライン

シングル コンテキスト ルーテッド ファイアウォール モードでは、各インターフェイス アドレスはそれぞれ固有のサブネットに存在する必要があります。マルチ コンテキスト モードでは、このインターフェイスが共有インターフェイスにある場合、各 IP アドレスはそれぞれ固有であるものの、同じサブネットに存在する必要があります。インターフェイスが固有のものである場合、この IP アドレスを必要に応じて他のコンテキストで使用できます。

トランスペアレント ファイアウォールのガイドライン

トランスペアレント ファイアウォールは、IP ルーティングに参加しません。ASA に必要な唯一の IP コンフィギュレーションは、BVI のアドレスを設定することです。このアドレスが必要になるのは、ASA がシステム メッセージや AAA サーバとの通信など ASA で発信されるトラフィックの送信元アドレスとしてこのアドレスを使用するためです。このアドレスは、リモート管理アクセスにも使用できます。このアドレスは、上流のルータおよび下流のルータと同じサブネットに存在する必要があります。マルチ コンテキスト モードの場合、各コンテキスト内の管理 IP アドレスを設定します。管理インターフェイスを含むモデルの場合は、このインターフェイスの IP アドレスを管理用に設定することもできます。

フェールオーバーのガイドライン

スタンバイ IP アドレスは、メイン IP アドレスと同じサブネットに存在する必要があります。

ASA クラスタリングのガイドライン

個々のインターフェイスのクラスタ プールは、クラスタ インターフェイス モードを個別インターフェイスに設定（**cluster-interface mode individual** コマンド）してからでないと設定できません。唯一の例外は管理専用インターフェイスです。

- 管理専用インターフェイスはいつでも、個別インターフェイスとして設定できます（スパンド EtherChannel モードのときでも）。管理インターフェイスは、個別インターフェイスとすることができます（トランスペアレント ファイアウォール モードのときでも）。
- スパンド EtherChannel モードでは、管理インターフェイスを個別インターフェイスとして設定すると、管理インターフェイスに対してダイナミック ルーティングをイネーブルにできません。スタティック ルートを使用する必要があります。

/31 サブネットのガイドライン

ルーテッド インターフェイスに関しては、ポイントツーポイント接続向けの 31 ビットのサブネットに IP アドレスを設定できます。31 ビット サブネットには 2 つのアドレスのみが含まれます。通常、サブネットの最初と最後のアドレスはネットワーク用とブロードキャスト用に予約されており、2 アドレス サブネットは使用できません。ただし、ポイントツーポイント接続があり、ネットワーク アドレスやブロードキャスト アドレスが不要な場合は、IPv4 形式でアドレスを保持するのに 31 サブネット ビットが役立ちます。たとえば、2 つの ASA 間のフェールオーバー リンクに必要なアドレスは 2 つだけです。リンクの一方の側から送信されるパケットはすべてもう一方の側で受信され、ブロードキャスティングは必要ありません。また、SNMP や Syslog を実行する管理ステーションを直接接続することもできます。

- 31 ビット サブネットとクラスタリング：スパンド EtherChannel に 31 ビット サブネット マスクを使用できます。個々のインターフェイス（スパンド EtherChannel モードの管理 IP アドレスを含む）は 31 ビット サブネットをサポートしていません。また、クラスタ制御リンクにも 31 ビット サブネットを使用できません。
- 31 ビット サブネットとフェールオーバー：フェールオーバーに関しては、ASA インターフェイスの IP アドレスに 31 ビットのサブネットを使用した場合、アドレスが不足しているため、インターフェイス用のスタンバイ IP アドレスは設定できません。通常、アクティブなユニットがインターフェイスのテストを実行し、スタンバイのインターフェイスの健全性を保証できるよう、フェールオーバー インターフェイスはスタンバイ IP アドレスを必要とします。スタンバイ IP アドレスがないと、ASA はネットワークのテストを実行できず、リンクステートのみしか追跡できません。ポイントツーポイント接続であるフェールオーバーと任意のステートリンクでは、31 ビットのサブネットも使用できます。
- 31 ビット サブネットと管理：直接接続されている管理ステーションがあれば、ASA 上で SSH または HTTP にポイントツーポイント接続を、または管理ステーション上で SNMP または Syslog にポイントツーポイント接続をそれぞれ使用できます。
- 31 ビット サブネットをサポートしていない機能：次の機能は、31 ビット サブネットをサポートしていません。
  - ブリッジ グループ用 BVI インターフェイス：ブリッジ グループには BVI、2 つのブリッジ グループ メンバーに接続された 2 つのホスト用に、少なくとも 3 つのホスト アドレスが必要です。/29 サブネット以下を使用する必要があります。
  - マルチキャスト ルーティング

例

次に、2 つのインターフェイスの IP アドレスおよびスタンバイ アドレスを設定する例を示します。

```
ciscoasa(config)# interface gigabitethernet0/2
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface gigabitethernet0/3
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.2.1 255.255.255.0 standby 10.1.2.2
ciscoasa(config-if)# no shutdown
```

次に、ブリッジ グループ 1 の管理アドレスおよびスタンバイ アドレスを設定する例を示します。

```
ciscoasa(config)# interface bvi 1
ciscoasa(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
```

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。
show ip address	インターフェイスに割り当てられた IP アドレスを表示します。

ip address dhcp

DHCP を使用してインターフェイスの IP アドレスを取得するには、インターフェイス コンフィギュレーション モードで **ip address dhcp** コマンドを使用します。このインターフェイスの DHCP クライアントをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip address dhcp [**setroute**]

no ip address dhcp

構文の説明

setroute	（任意）ASA が DHCP サーバから提供されたデフォルト ルートを使用できるようにします。

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
インターフェイス コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、グローバル コンフィギュレーション コマンドからインターフェイス コンフィギュレーション モード コマンドに変更されました。このコマンドは、外部インターフェイスだけでなく、任意のインターフェイスもイネーブルにできます。

使用上のガイドライン

DHCP リースをリセットし、新規リースを要求するには、このコマンドを再入力します。

ip address dhcp コマンドを入力する前に、**no shutdown** コマンドを使用してインターフェイスをイネーブルにしなかった場合、DHCP 要求が送信されないことがあります。

（注） ASA は、タイムアウトが 32 秒未満のリースを拒否します。

例

次に、Gigabitethernet0/1 インターフェイスで DHCP をイネーブルにする例を示します。

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# ip address dhcp
```

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	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。
show ip address dhcp	DHCP サーバから取得された IP アドレスを示します。

ip address pppoe

PPPoE をイネーブルにするには、インターフェイス コンフィギュレーション モードで **ip address pppoe** コマンドを使用します。PPPoE をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip address [*ip_address* [*mask*]] **pppoe** [**setroute**]

no ip address [*ip_address* [*mask*]] **pppoe**

構文の説明

ip_address	IP アドレスを PPPoE サーバから受信するのではなく手動で設定します。
mask	IP アドレスのサブネット マスクを指定します。マスクを設定しない場合、ASA では IP アドレス クラスのデフォルト マスクが使用されます。
setroute	ASA が、PPPoE サーバから提供されるデフォルト ルートを使用できるようにします。PPPoE サーバがデフォルト ルートを送信しない場合、ASA はアクセス コンセントレータのアドレスをゲートウェイとするデフォルト ルートを作成します。

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
インターフェイス コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(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

PPPoE は、イーサネットと PPP という広く受け入れられている 2 つの標準を結合して、IP アドレスをクライアント システムに割り当てる認証方式を提供します。ISP は、既存のリモート アクセス インフラストラクチャを使用して高速ブロードバンド アクセスをサポートするためと、顧客の使い勝手向上のために、PPPoE を配置します。

PPPoE を使用して IP アドレスを設定する前に、**vpdn** コマンドでユーザ名、パスワード、および認証プロトコルを設定します。複数のインターフェイスでこのコマンドをイネーブルにした場合（たとえば、ISP へのバックアップ リンク用）は、**pppoe client vpdn group** コマンドを使用して、必要に応じて各インターフェイスをそれぞれ異なる VPDN グループに割り当てることができます。

最大伝送単位（MTU）サイズは、自動的に 1492 バイトに設定されます。これは、イーサネット フレーム内で PPPoE 伝送を許可する正しい値です。

PPPoE セッションをリセットして再起動するには、このコマンドを再入力します。

このコマンドは、**ip address** コマンドまたは **ip address dhcp** コマンドと同時には設定できません。

例

次に、GigabitEthernet 0/1 インターフェイスで PPPoE をイネーブルにする例を示します。

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address pppoe
ciscoasa(config-if)# no shutdown
```

次に、PPPoE インターフェイスの IP アドレスを手動で設定する例を示します。

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 pppoe
ciscoasa(config-if)# no shutdown
```

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	インターフェイスの IP アドレスを設定します。
pppoe client vpdn group	このインターフェイスを特定の VPDN グループに割り当てます。
show ip address pppoe	PPPoE サーバから取得された IP アドレスを表示します。
vpdn group	VPDN グループを作成し、PPPoE クライアントを設定します。

ip-address-privacy

IP アドレスのプライバシーをイネーブルにするには、パラメータ コンフィギュレーション モードで **ip-address-privacy** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip-address-privacy

no ip-address-privacy

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

このコマンドは、デフォルトでディセーブルになっています。

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
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、SIP インスペクション ポリシー マップで SIP を経由する IP アドレスのプライバシーをイネーブルにする例を示します。

```
ciscoasa(config)# policy-map type inspect sip sip_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# ip-address-privacy
```

関連コマンド

コマンド	説明
policy-map type inspect	インスペクション ポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

ip audit attack

攻撃シグニチャに一致するパケットに対してデフォルト アクションを設定するには、グローバル コンフィギュレーション モードで **ip audit attack** コマンドを使用します。デフォルト アクションを復元（して接続をリセット）するには、このコマンドの **no** 形式を使用します。

ip audit attack [**action** [**alarm**] [**drop**] [**reset**]]

no ip audit attack

構文の説明

アクション	（任意）一連のデフォルト アクションを定義することを指定します。このキーワードの後に何もアクションを指定しない場合、ASA はアクションを実行しません。**action** キーワードを入力しない場合、ASA ではキーワードが入力されたものと見なして、**action** キーワードをコンフィギュレーションに記述します。
アラーム	（デフォルト）パケットがシグニチャに一致したことを示すシステム メッセージを生成します。
drop	（任意）パケットをドロップします。
reset	（任意）パケットをドロップし、接続を閉じます。

デフォルト

デフォルト アクションは、送信し、アラームを生成することです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

アクションは複数指定することも、まったく指定しないこともできます。このコマンドで設定するアクションは、**ip audit name** コマンドを使用して監査ポリシーを設定すると上書きできます。**ip audit name** コマンドでアクションを指定しない場合は、このコマンドで設定するアクションが使用されます。

シグニチャのリストについては、**ip audit signature** コマンドを参照してください。

例

次に、攻撃シグニチャに一致するパケットに対してアラームを生成し、リセットするデフォルトアクションを設定する例を示します。内部インターフェイスの監査ポリシーはアラームだけを生成するようにこのデフォルトを上書きしますが、外部インターフェイスの監査ポリシーは **ip audit attack** コマンドで設定されたデフォルト設定を使用します。

```
ciscoasa(config)# ip audit attack action alarm reset
ciscoasa(config)# ip audit name insidepolicy attack action alarm
ciscoasa(config)# ip audit name outsidepolicy attack
ciscoasa(config)# ip audit interface inside insidepolicy
ciscoasa(config)# ip audit interface outside outsidepolicy
```

関連コマンド

コマンド	説明
ip audit info	情報シグニチャに一致するパケットのデフォルト アクションを設定します。
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。
ip audit signature	シグニチャをディセーブルにします。
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。

ip audit info

情報シグニチャに一致するパケットに対してデフォルト アクションを設定するには、グローバル コンフィギュレーション モードで **ip audit info** コマンドを使用します。デフォルト アクションを復元（してアラームを生成）するには、このコマンドの **no** 形式を使用します。アクションは複数指定することも、まったく指定しないこともできます。

ip audit info [**action** [**alarm**] [**drop**] [**reset**]]

no ip audit info

構文の説明

アクション	（任意）一連のデフォルト アクションを定義することを指定します。このキーワードの後に何もアクションを指定しない場合、ASA はアクションを実行しません。**action** キーワードを入力しない場合、ASA ではキーワードが入力されたものと見なして、**action** キーワードをコンフィギュレーションに記述します。
アラーム	（デフォルト）パケットがシグニチャに一致したことを示すシステム メッセージを生成します。
drop	（任意）パケットをドロップします。
reset	（任意）パケットをドロップし、接続を閉じます。

デフォルト

デフォルト アクションは、アラームを生成することです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドで設定するアクションは、**ip audit name** コマンドを使用して監査ポリシーを設定すると上書きできます。**ip audit name** コマンドでアクションを指定しない場合は、このコマンドで設定するアクションが使用されます。

シグニチャのリストについては、**ip audit signature** コマンドを参照してください。

例

次に、情報シグニチャに一致するパケットに対してアラームを生成し、リセットするデフォルトアクションを設定する例を示します。内部インターフェイスの監査ポリシーはアラームを生成し、ドロップするようにこのデフォルトを上書きしますが、外部インターフェイスの監査ポリシーは **ip audit info** コマンドで設定されたデフォルト設定を使用します。

```
ciscoasa(config)# ip audit info action alarm reset
ciscoasa(config)# ip audit name insidepolicy info action alarm drop
ciscoasa(config)# ip audit name outsidepolicy info
ciscoasa(config)# ip audit interface inside insidepolicy
ciscoasa(config)# ip audit interface outside outsidepolicy
```

関連コマンド

コマンド	説明
ip audit attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
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。
ip audit signature	シグニチャをディセーブルにします。
show running-config ip audit info	**ip audit info** コマンドのコンフィギュレーションを表示します。

ip audit interface

監査ポリシーをインターフェイスに割り当てるには、グローバル コンフィギュレーション モードで **ip audit interface** コマンドを使用します。インターフェイスからポリシーを削除するには、このコマンドの **no** 形式を使用します。

ip audit interface *interface_name policy_name*

no ip audit interface *interface_name policy_name*

構文の説明

interface_name	インターフェイス名を指定します。
policy_name	**ip audit name** コマンドで追加したポリシーの名前。各インターフェイスに info ポリシーおよび attack ポリシーを割り当てることができます。

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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、監査ポリシーを内部インターフェイスおよび外部インターフェイスに適用する例を示します。

```
ciscoasa(config)# ip audit name insidepolicy1 attack action alarm
ciscoasa(config)# ip audit name insidepolicy2 info action alarm
ciscoasa(config)# ip audit name outsidepolicy1 attack action reset
ciscoasa(config)# ip audit name outsidepolicy2 info action alarm
ciscoasa(config)# ip audit interface inside insidepolicy1
ciscoasa(config)# ip audit interface inside insidepolicy2
ciscoasa(config)# ip audit interface outside outsidepolicy1
ciscoasa(config)# ip audit interface outside outsidepolicy2
```

関連コマンド

コマンド	説明
ip audit attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit info	情報シグニチャに一致するパケットのデフォルト アクションを設定します。
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。
ip audit signature	シグニチャをディセーブルにします。
show running-config ip audit interface	**ip audit interface** コマンドのコンフィギュレーションを表示します。

ip audit name

パケットが定義済みの攻撃シグニチャまたは情報シグニチャに一致したときに実行するアクションを識別する名前付き監査ポリシーを作成するには、グローバル コンフィギュレーション モードで **ip audit name** コマンドを使用します。ポリシーを削除するには、このコマンドの **no** 形式を使用します。

ip audit name *name* {**info** | **attack**} [**action** [**alarm**] [**drop**] [**reset**]]

no ip audit name *name* {**info** | **attack**} [**action** [**alarm**] [**drop**] [**reset**]]

構文の説明

アクション	(任意)一連のアクションを定義することを指定します。このキーワードの後に何もアクションを指定しない場合、ASA はアクションを実行しません。**action** キーワードを入力しないと、ASA は **ip audit attack** コマンドおよび **ip audit info** コマンドによって設定されたデフォルト アクションを使用します。
アラーム	(任意)パケットがシグニチャに一致したことを示すシステム メッセージを生成します。
攻撃	攻撃シグニチャの監査ポリシーを作成します。パケットは、DoS 攻撃や不正な FTP コマンドなど、ネットワークでの攻撃の一部となる可能性があります。
drop	(任意)パケットをドロップします。
info	情報シグニチャの監査ポリシーを作成します。パケットは、現時点ではネットワークを攻撃していませんが、ポート スイープなど情報収集アクティビティの一部である可能性があります。
name	ポリシーの名前を設定します。
reset	(任意)パケットをドロップし、接続を閉じます。

デフォルト

ip audit attack コマンドおよび **ip audit info** コマンドを使用してデフォルト アクションを変更しなかった場合、攻撃シグニチャおよび情報シグニチャのデフォルト アクションはアラームを生成することです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

シグニチャは、既知の攻撃パターンに一致するアクティビティです。たとえば、DoS 攻撃に一致するシグニチャがあります。ポリシーを適用するには、**ip audit interface** コマンドを使用して、そのポリシーをインターフェイスに割り当てます。各インターフェイスに info ポリシーおよび attack ポリシーを割り当てることができます。

シグニチャのリストについては、**ip audit signature** コマンドを参照してください。

トラフィックがシグニチャに一致し、そのトラフィックに対してアクションを実行する場合は、**shun** コマンドを使用して、問題のホストからの新規接続を拒否し、既存の接続からのパケットの受信を禁止します。

例

次に、内部インターフェイスには攻撃シグニチャおよび情報シグニチャに関するアラームを生成する監査ポリシーを設定し、外部インターフェイスには攻撃に備えて接続をリセットする監査ポリシーを設定する例を示します。

```
ciscoasa(config)# ip audit name insidepolicy1 attack action alarm
ciscoasa(config)# ip audit name insidepolicy2 info action alarm
ciscoasa(config)# ip audit name outsidepolicy1 attack action reset
ciscoasa(config)# ip audit name outsidepolicy2 info action alarm
ciscoasa(config)# ip audit interface inside insidepolicy1
ciscoasa(config)# ip audit interface inside insidepolicy2
ciscoasa(config)# ip audit interface outside outsidepolicy1
ciscoasa(config)# ip audit interface outside outsidepolicy2
```

関連コマンド

コマンド	説明
ip audit attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit info	情報シグニチャに一致するパケットのデフォルト アクションを設定します。
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 signature	シグニチャをディセーブルにします。
shun	特定の送信元アドレスおよび宛先アドレスでパケットをブロックします。

ip audit signature

監査ポリシーに対してシグニチャをディセーブルにするには、グローバル コンフィギュレーション モードで **ip audit signature** コマンドを使用します。シグニチャを再びイネーブルにするには、このコマンドの **no** 形式を使用します。

ip audit signature *signature_number* **disable**

no ip audit signature *signature_number*

構文の説明

disable	シグニチャをディセーブルにします。
signature_number	ディセーブルにするシグニチャ番号を指定します。サポートされているシグニチャのリストについては、表 3-1 を参照してください。

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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

正規のトラフィックが頻繁にシグニチャに一致する場合には、シグニチャをディセーブルにしてみてください。リスクが伴うことを承知でシグニチャをディセーブルにすると、多数のアラームを回避できます。表 3-1 に、サポートされているシグニチャおよびメッセージ番号の一覧を示します。

表 3-1　シグニチャ ID とシステム メッセージ番号

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
1000	400000	IP options-Bad Option List	情報	IP データグラム ヘッダーの IP オプションのリストが不完全であるか、または不正な形式になっている IP データグラムを受信するとトリガーされます。IP オプションのリストには、さまざまなネットワーク管理タスクまたはデバッグ タスクを実行するオプションが 1 つ以上含まれています。
1001	400001	IP options-Record Packet Route	情報	データグラムの IP オプション リスト中にオプション 7（記録パケット ルート）を含む IP データグラムを受信するとトリガーされます。
1002	400002	IP options-Timestamp	情報	データグラムの IP オプション リスト中にオプション 4（タイムスタンプ）を含む IP データグラムを受信するとトリガーされます。
1003	400003	IP options-Security	情報	データグラムの IP オプション リスト中にオプション 2（セキュリティ オプション）を含む IP データグラムを受信するとトリガーされます。
1004	400004	IP options-Loose Source Route	情報	データグラムの IP オプション リスト中にオプション 3（緩慢な送信元ルート）を含む IP データグラムを受信するとトリガーされます。
1005	400005	IP options-SATNET ID	情報	データグラムの IP オプション リスト中にオプション 8（SATNET ストリーム ID）を含む IP データグラムを受信するとトリガーされます。
1006	400006	IP options-Strict Source Route	情報	データグラムの IP オプション リスト中にオプション 2（厳密な送信元ルーティング）を含む IP データグラムを受信するとトリガーされます。
1100	400007	IP Fragment Attack	攻撃	オフセット フィールドのオフセット値が 0 より大きく 5 未満になっている IP データグラムを受信するとトリガーされます。
1102	400008	IP Impossible Packet	攻撃	送信元と宛先が同じアドレスになっている IP パケットが到着するとトリガーされます。このシグニチャは、いわゆる Land Attack を捕捉します。

表 3-1　シグニチャ ID とシステム メッセージ番号（続き）

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
1103	400009	IP Overlapping Fragments（Teardrop）	攻撃	同じ IP データグラム内に含まれている 2 つのフラグメントのオフセット値が、そのデータグラム内の位置決めを共有していることを示す場合にトリガーされます。これは、フラグメント A がフラグメント B によって完全に上書きされること、またはフラグメント A がフラグメント B によって部分的に上書きされることを意味する場合があります。オペレーティング システムによっては、このように重複するフラグメントが正しく処理されず、重複フラグメントを受信すると例外をスローしたり、他の不適切な動作を行ったりします。Teardrop 攻撃では、これにより DoS 状態を引き起こします。
2000	400010	ICMP Echo Reply	情報	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 0（エコー応答）に設定された IP データグラムを受信するとトリガーされます。
2001	400011	ICMP Host Unreachable	情報	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 3（ホスト到達不能）に設定された IP データグラムを受信するとトリガーされます。
2002	400012	ICMP Source Quench	情報	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 4（ソース クエンチ）に設定された IP データグラムを受信するとトリガーされます。
2003	400013	ICMP Redirect	情報	P ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 5（リダイレクト）に設定された IP データグラムを受信するとトリガーされます。
2004	400014	ICMP Echo Request	情報	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 8（エコー要求）に設定された IP データグラムを受信するとトリガーされます。
2005	400015	ICMP Time Exceeded for a Datagram	情報	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 11（データグラムの超過時間）に設定された IP データグラムを受信するとトリガーされます。

表 3-1　シグニチャ ID とシステム メッセージ番号(続き)

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
2006	400016	ICMP Parameter Problem on Datagram	情報	IP ヘッダーのプロトコル フィールドが 1(ICMP)に設定され、ICMP ヘッダーのタイプ フィールドが 12(データグラムのパラメータ問題)に設定された IP データグラムを受信するとトリガーされます。
2007	400017	ICMP Timestamp Request	情報	IP ヘッダーのプロトコル フィールドが 1(ICMP)に設定され、ICMP ヘッダーのタイプ フィールドが 13(タイムスタンプ要求)に設定された IP データグラムを受信するとトリガーされます。
2008	400018	ICMP Timestamp Reply	情報	IP ヘッダーのプロトコル フィールドが 1(ICMP)に設定され、ICMP ヘッダーのタイプ フィールドが 14(タイムスタンプ応答)に設定された IP データグラムを受信するとトリガーされます。
2009	400019	ICMP Information Request	情報	IP ヘッダーのプロトコル フィールドが 1(ICMP)に設定され、ICMP ヘッダーのタイプ フィールドが 15(情報要求)に設定された IP データグラムを受信するとトリガーされます。
2010	400020	ICMP Information Reply	情報	IP ヘッダーのプロトコル フィールドが 1(ICMP)に設定され、ICMP ヘッダーのタイプ フィールドが 16(ICMP 情報応答)に設定された IP データグラムを受信するとトリガーされます。
2011	400021	ICMP Address Mask Request	情報	IP ヘッダーのプロトコル フィールドが 1(ICMP)に設定され、ICMP ヘッダーのタイプ フィールドが 17(アドレス マスク要求)に設定された IP データグラムを受信するとトリガーされます。
2012	400022	ICMP Address Mask Reply	情報	IP ヘッダーのプロトコル フィールドが 1(ICMP)に設定され、ICMP ヘッダーのタイプ フィールドが 18(アドレス マスク応答)に設定された IP データグラムを受信するとトリガーされます。
2150	400023	Fragmented ICMP Traffic	攻撃	IP ヘッダーのプロトコル フィールドが 1(ICMP)に設定され、他にも 1(ICMP)に設定されたフラグメント フラグが存在するか、またはオフセット フィールドにオフセット値が指定されている IP データグラムを受信するとトリガーされます。

表 3-1　シグニチャ ID とシステム メッセージ番号（続き）

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
2151	400024	Large ICMP Traffic	攻撃	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、IP 長が 1024 より大きくなっている IP データグラムを受信するとトリガーされます。
2154	400025	Ping of Death 攻撃	攻撃	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、最終フラグメント ビットが設定され、さらに（IP オフセット * 8）+（IP データ長）が 65535 を超えている場合、つまり IP オフセット（このフラグメントの元のパケットでの開始位置を表し、かつ 8 バイト単位であるもの）にパケットの残りを加えた値が、IP パケットの最大サイズを超えている IP データグラムを受信するとトリガーします。
3040	400026	TCP NULL flags	攻撃	SYN、FIN、ACK、または RST のいずれのフラグも設定されていない 1 つの TCP パケットが特定のホストに送信されるとトリガーされます。
3041	400027	TCP SYN+FIN flags	攻撃	SYN および FIN のフラグが設定されている 1 つの TCP パケットが特定のホストに送信されるとトリガーされます。
3042	400028	TCP FIN only flags	攻撃	1 つの孤立 TCP FIN パケットが特定のホストの特権ポート（ポート番号が 1024 未満）に送信されるとトリガーされます。
3153	400029	FTP Improper Address Specified	情報	要求側ホストと異なるアドレスを指定して port コマンドが発行された場合にトリガーされます。
3154	400030	FTP Improper Port Specified	情報	1024 未満または 65535 より大きい値のデータ ポートを指定して port コマンドが発行された場合にトリガーされます。
4050	400031	UDP Bomb attack	攻撃	指定されている UDP 長が、指定されている IP 長より短い場合にトリガーされます。この不正な形式のパケット タイプは、サービス拒絶攻撃と関連付けられています。
4051	400032	UDP Snork attack	攻撃	送信元ポートが 135、7、または 19 のいずれかで、宛先ポートが 135 になっている UDP パケットが検出されるとトリガーされます。
4052	400033	UDP Chargen DoS attack	攻撃	このシグニチャは、送信元ポート 7 および宛先ポート 19 において UDP パケットが検出されるとトリガーされます。
6050	400034	DNS HINFO Request	情報	DNS サーバから HINFO レコードへのアクセスが試みられるとトリガーされます。

表 3-1　シグニチャ ID とシステム メッセージ番号(続き)

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
6051	400035	DNS Zone Transfer	情報	送信元ポートが 53 の通常の DNS ゾーン転送が実行されるとトリガーされます。
6052	400036	DNS Zone Transfer from High Port	情報	送信元ポートが 53 以外のときに不正な DNS ゾーン転送が発生するとトリガーされます。
6053	400037	DNS Request for All Records	情報	すべてのレコードに対する DNS 要求があるとトリガーされます。
6100	400038	RPC Port Registration	情報	ターゲット ホストで新しい RPC サービスを登録する試みがあるとトリガーされます。
6101	400039	RPC Port Unregistration	情報	ターゲット ホストで既存の RPC サービスを登録解除する試みがあるとトリガーされます。
6102	400040	RPC Dump	情報	ターゲット ホストに対して RPC ダンプ要求が発行されるとトリガーされます。
6103	400041	Proxied RPC Request	攻撃	ターゲット ホストのポートマッパーにプロキシ RPC 要求が送信されるとトリガーされます。
6150	400042	ypserv (YP server daemon) Portmap Request	情報	YP サーバ デーモン(ypserv)ポートのポートマッパーに対して要求が行われるとトリガーされます。
6151	400043	ypbind (YP bind daemon) Portmap Request	情報	YP バインド デーモン(ypbind)ポートのポートマッパーに対して要求が行われるとトリガーされます。
6152	400044	yppasswdd (YP password daemon) Portmap Request	情報	YP パスワード デーモン(yppasswdd)ポートのポートマッパーに対して要求が行われるとトリガーされます。
6153	400045	ypupdated (YP update daemon) Portmap Request	情報	YP 更新デーモン(ypupdated)ポートのポートマッパーに対して要求が行われるとトリガーされます。
6154	400046	ypxfrd (YP transfer daemon) Portmap Request	情報	YP 転送デーモン(ypxfrd)ポートのポートマッパーに対して要求が行われるとトリガーされます。
6155	400047	mountd (mount daemon) Portmap Request	情報	マウント デーモン(mountd)ポートのポートマッパーに対して要求が行われるとトリガーされます。
6175	400048	rexd (remote execution daemon) Portmap Request	情報	リモート実行デーモン(rexd)ポートのポートマッパーに対して要求が行われるとトリガーされます。

表 3-1　シグニチャ ID とシステム メッセージ番号（続き）

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
6180	400049	rexd (remote execution daemon) Attempt	情報	rexd プログラムの呼び出しが行われるとトリガーされます。リモート実行デーモンは、プログラムをリモート実行する役割を担うサーバです。rexd プログラムの呼び出しは、システム リソースへの不正アクセスの試みを示唆している場合があります。
6190	400050	statd Buffer Overflow	攻撃	サイズの大きな statd 要求が送信されるとトリガーされます。これは、バッファをオーバーフローさせてシステムへアクセスしようとする試みの可能性があります。

例

次に、シグニチャ 6100 をディセーブルにする例を示します。

```
ciscoasa(config)# ip audit signature 6100 disable
```

関連コマンド

コマンド	説明
ip audit attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit info	情報シグニチャに一致するパケットのデフォルト アクションを設定します。
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 signature	**ip audit signature** コマンドのコンフィギュレーションを表示します。

ip-client

FXOS での管理トラフィックの開始と、Firepower 2100 ASA データ インターフェイスから外部への送信を許可するには、グローバル構成モードで **ip-client** コマンドを使用します。トラフィックの開始を無効にするには、このコマンドの **no** 形式を使用します。

ip-client *interface_name*

no ip-client *interface_name*

構文の説明

interface_name	FXOS が管理トラフィックを送信できるインターフェイス名を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.8(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

ASA データ インターフェイスで FXOS 管理トラフィック開始を有効にすることができます。これは、たとえば、SNMP トラップ、NTP と DNS のサーバ アクセスなどに必要です。受信管理トラフィックについては、**fxos permit** コマンドを参照してください。

FXOS の設定で、デフォルト ゲートウェイが 0.0.0.0 に設定されていることを確認します。これは ASA をゲートウェイとして設定します。FXOS の **set out-of-band** コマンドを参照してください。

例

次のコマンドにより、外部インターフェイスを介して FXOS トラフィックを開始できます。

```
ciscoasa(config)# ip-client outside
```

関連コマンド

コマンド	説明
connect fxos	ASA CLI から FXOS CLI に接続します。
fxos permit	ASA データ インターフェイスでの FXOS 管理アクセスを許可します。
fxos port	FXOS 管理アクセス ポートを設定します。

ip-comp

LZS IP 圧縮をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで **ip-comp enable** コマンドを使用します。IP 圧縮をディセーブルにするには、**ip-comp disable** コマンドを使用します。実行コンフィギュレーションから **ip-comp** 属性を削除するには、このコマンドの **no** 形式を使用します。

ip-comp {**enable** | **disable**}

no ip-comp

構文の説明

disable	IP 圧縮をディセーブルにします。
enable	IP 圧縮をイネーブルにします。

デフォルト

IP 圧縮はディセーブルになっています。

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
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(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

このコマンドの **no** 形式を使用すると、別のグループ ポリシーから値を継承できます。データ圧縮をイネーブルにすると、モデムで接続するリモート ダイヤルイン ユーザのデータ伝送レートが向上する場合があります。

注意 データ圧縮を使用すると、各ユーザ セッションのメモリ要件と CPU 使用率が高くなり、その結果 ASA 全体のスループットが低下します。そのため、データ圧縮はモデムで接続しているリモート ユーザに対してだけイネーブルにすることを推奨します。モデム ユーザに固有のグループ ポリシーを設計し、それらのユーザに対してだけ圧縮をイネーブルにします。

エンドポイントで IP 圧縮トラフィックが生成される場合、パケットの不正な圧縮解除を防ぐために、IP 圧縮をディセーブルにする必要があります。特定の LAN-to-LAN トンネルで IP 圧縮がイネーブルになっている場合、トンネルの一方からもう一方に IP 圧縮データを渡そうとするときに、ホスト A はホスト B と通信できません。

（注） **ip-comp** コマンドがイネーブルで、「暗号化前」の処理として IPsec フラグメンテーションが設定されている場合、IPsec 圧縮（ip-comp_option と pre-encryption）は使用できません。暗号化チップに送信される IP ヘッダーが圧縮によってあいまいになり、暗号化チップによる着信パケットの処理時にエラーが生成されるためです。この場合は、MTU レベルをチェックして少量（600 バイトなど）であることを確認してください。

例

次に、「FirstGroup」というグループ ポリシーの IP 圧縮をイネーブルにする例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# ip-comp enable
```

ip local pool

IP アドレス プールを設定するには、グローバル コンフィギュレーション モードで **ip local pool** コマンドを使用します。アドレス プールを削除するには、このコマンドの **no** 形式を使用します。

ip local pool *poolname first-address—last-address* [**mask** *mask*]

no ip local pool *poolname*

構文の説明

first-address	IP アドレスの範囲における開始アドレスを指定します。
last-address	IP アドレスの範囲における最終アドレスを指定します。
mask *mask*	（任意）アドレス プールのサブネット マスクを指定します。
poolname	IP アドレス プールの名前を指定します。

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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	ASA クラスタリングをサポートするために、**ip address** コマンドでクラスタ プールとして IP ローカル プールを指定できるようになりました。

使用上のガイドライン

VPN クライアントに割り当てられた IP アドレスが標準以外のネットワークに属しているときには、マスク値を指定する必要があります。デフォルト マスクを使用した場合には、データが誤ってルーティングされることがあります。典型的な例が、IP ローカル プールに 10.10.10.0/255.255.255.0 アドレスが含まれている場合で、これはデフォルトではクラス A ネットワークです。この結果、VPN クライアントが異なるインターフェイス経由で 10 ネットワーク内の別のサブネットにアクセスする必要がある場合には、ある種のルーティング問題が発生することがあります。たとえば、アドレス 10.10.100.1/255.255.255.0 のプリンタがインターフェイス 2 を介して使用できるようになっているものの、10.10.10.0 ネットワークが VPN トンネルを経由するためインターフェイス 1 で使用できるようになっている場合、VPN クライアントはプリンタ宛てのデータのルーティング先を正確に把握できなくなります。10.10.10.0 と 10.10.100.0 のサブネットは両方とも、10.0.0.0 クラス A ネットワークに分類されるため、プリンタ データが VPN トンネル経由で送信される可能性があります。

例

次に、firstpool という名前で IP アドレス プールを設定する例を示します。開始アドレスは 10.20.30.40 で、最終アドレスは 10.20.30.50 です。ネットワーク マスクは 255.255.255.0 です。

```
ciscoasa(config)# ip local pool firstpool 10.20.30.40-10.20.30.50 mask 255.255.255.0
```

関連コマンド

コマンド	説明
clear configure ip local pool	すべての IP ローカル プールを削除します。
show running-config ip local pool	IP プール コンフィギュレーションを表示します。特定の IP アドレス プールを指定するには、その名前をコマンドに含めます。

ip-phone-bypass

IP Phone Bypass をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで **ip-phone-bypass enable** コマンドを使用します。実行コンフィギュレーションから IP Phone Bypass 属性を削除するには、このコマンドの **no** 形式を使用します。

ip-phone-bypass {**enable** | **disable**}

no ip-phone-bypass

構文の説明

disable	IP Phone Bypass をディセーブルにします。
enable	IP Phone Bypass をイネーブルにします。

デフォルト

IP Phone Bypass はディセーブルになっています。

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
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(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

IP Phone Bypass をディセーブルにするには、**ip-phone-bypass disable** コマンドを使用します。このコマンド オプションの **no** 形式を使用すると、別のグループ ポリシーから IP Phone Bypass の値を継承できます。

IP Phone Bypass を使用すると、ハードウェア クライアントの背後にある IP フォンが、ユーザ認証プロセスなしで接続できます。イネーブルの場合、セキュア ユニット認証は有効のままになります。

IP Phone Bypass は、ユーザ認証をイネーブルにした場合にだけ設定する必要があります。

また、**mac-exempt** オプションを設定してクライアントの認証を免除する必要があります。詳細については、**vpnclient mac-exempt** コマンドを参照してください。

例

次の例は、FirstGroup というグループ ポリシーに対して IP Phone Bypass をイネーブルにする方法を示しています。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# ip-phone-bypass enable
```

関連コマンド

コマンド	説明
user-authentication	ハードウェア クライアントの背後にいるユーザに対して、接続前に ASA に識別情報を示すように要求します。

ips

インスペクションのために ASA から AIP SSM にトラフィックを迂回させるには、クラス コンフィギュレーション モードで **ips** コマンドを使用します。このコマンドを削除するには、このコマンドの **no** 形式を使用します。

ips {**inline** | **promiscuous**} {**fail-close** | **fail-open**} [**sensor** {*sensor_name* | *mapped_name*}]

no ips {**inline** | **promiscuous**} {**fail-close** | **fail-open**} [**sensor** {*sensor_name* | *mapped_name*}]

構文の説明

fail-close	AIP SSM で障害が発生した場合には、トラフィックをブロックします。
fail-open	AIP SSM で障害が発生しても、トラフィックを許可します。
inline	パケットを AIP SSM に向けて送ります。パケットは、IPS が動作した結果、ドロップされる場合があります。
promiscuous	AIP SSM 向けにパケットを複製します。AIP SSM が元のパケットをドロップすることはできません。
sensor {*sensor_name* | *mapped_name*}	このトラフィックの仮想センサー名を設定します。AIP SSM（バージョン 6.0 以降）で仮想センサーを使用する場合は、この引数を使用してセンサー名を指定できます。使用可能なセンサー名を表示するには、**ips ... sensor ?** コマンドを使用します。使用可能なセンサーの一覧が表示されます。また、**show ips** コマンドを使用することもできます。 ASA でマルチ コンテキスト モードを使用する場合は、コンテキストに割り当てたセンサーのみを指定できます（**allocate-ips** コマンドを参照）。コンテキストで設定する場合は、*mapped_name* 引数を使用します。 センサー名を指定しないと、トラフィックはデフォルトのセンサーを使用します。マルチ コンテキスト モードでは、コンテキストのデフォルトのセンサーを指定できます。シングル モードの場合、またはマルチ モードでデフォルトのセンサーを指定しない場合、トラフィックは AIP SSM に設定されているデフォルトのセンサーを使用します。 AIP SSM にまだ存在しない名前を入力した場合は、エラーが発生し、コマンドが拒否されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.0(2)	仮想センサーのサポートが追加されました。

使用上のガイドライン

ASA 5500 シリーズは、AIP SSM をサポートします。これは、プロアクティブでフル機能の侵入防御サービスを提供する高度な IPS ソフトウェアを実行して、ワームやネットワーク ウイルスなど悪意のあるトラフィックを停止し、ネットワークに影響が及ばないようにします。ASA で **ips** コマンドを設定する前または後に、AIP SSM でセキュリティ ポリシーを設定します。ASA から AIP SSM へのセッションを確立するか（**session** コマンド）、または管理インターフェイスで SSH または Telnet を使用して直接 AIP SSM に接続できます。または、ASDM を使用する方法もあります。AIP SSM の設定の詳細については、*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface* を参照してください。

ips コマンドを設定するには、先に **class-map** コマンド、**policy-map** コマンド、および **class** コマンドを設定する必要があります。

AIP SSM は、ASA とは別のアプリケーションを実行します。ただし、そのアプリケーションは ASA のトラフィック フローに統合されます。AIP SSM には、管理インターフェイス以外に外部インターフェイス自体は含まれていません。ASA でトラフィック クラスに対して **ips** コマンドを適用すると、トラフィックは次のように ASA および AIP SSM を経由します。

1. トラフィックは ASA に入ります。
2. ファイアウォール ポリシーが適用されます。
3. トラフィックがバックプレーン経由で AIP SSM に送信されます（**inline** キーワードを使用します。トラフィックのコピーを AIP SSM に送信するだけの場合の詳細については、**promiscuous** キーワードを参照してください）。
4. AIP SSM が、セキュリティ ポリシーをトラフィックに適用し、適切なアクションを実行します。
5. 有効なトラフィックがバックプレーン経由で ASA に返送されます。AIP SSM が、セキュリティ ポリシーに従ってトラフィックをブロックすることがあり、そのトラフィックは渡されません。
6. VPN ポリシーが適用されます（設定されている場合）。
7. トラフィックが ASA から出ます。

例

次に、無差別モードですべての IP トラフィックを AIP SSM に迂回させ、何らかの理由で AIP SSM カードで障害が発生した場合にはすべての IP トラフィックをブロックする例を示します。

```
ciscoasa(config)# access-list IPS permit ip any any
ciscoasa(config)# class-map my-ips-class
ciscoasa(config-cmap)# match access-list IPS
ciscoasa(config-cmap)# policy-map my-ips-policy
ciscoasa(config-pmap)# class my-ips-class
ciscoasa(config-pmap-c)# ips promiscuous fail-close
ciscoasa(config-pmap-c)# service-policy my-ips-policy global
```

次に、インライン モードで 10.1.1.0 ネットワークおよび 10.2.1.0 ネットワーク宛てのすべての IP トラフィックを AIP SSM に迂回させ、何らかの理由で AIP SSM カードで障害が発生してもすべてのトラフィックを許可する例を示します。my-ips-class トラフィックにはセンサー 1 が使用され、my-ips-class2 トラフィックにはセンサー 2 が使用されます。

```
ciscoasa(config)# access-list my-ips-acl permit ip any 10.1.1.0 255.255.255.0
ciscoasa(config)# access-list my-ips-acl2 permit ip any 10.2.1.0 255.255.255.0
ciscoasa(config)# class-map my-ips-class
ciscoasa(config-cmap)# match access-list my-ips-acl
ciscoasa(config)# class-map my-ips-class2
ciscoasa(config-cmap)# match access-list my-ips-acl2
ciscoasa(config-cmap)# policy-map my-ips-policy
ciscoasa(config-pmap)# class my-ips-class
ciscoasa(config-pmap-c)# ips inline fail-open sensor sensor1
ciscoasa(config-pmap)# class my-ips-class2
ciscoasa(config-pmap-c)# ips inline fail-open sensor sensor2
ciscoasa(config-pmap-c)# service-policy my-ips-policy interface outside
```

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。
class	トラフィック分類に使用するクラス マップを指定します。
class-map	ポリシー マップ用にトラフィックを識別します。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

ipsec-udp

IPsec over UDP をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで **ipsec-udp enable** コマンドを使用します。現在のグループ ポリシーから IPsec over UDP 属性を削除するには、このコマンドの **no** 形式を使用します。

ipsec-udp {**enable** | **disable**}

no ipsec-udp

構文の説明

disable	IPsec over UDP をディセーブルにします。
enable	IPsec over UDP をイネーブルにします。

デフォルト

IPsec over UDP はディセーブルになっています。

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
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(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

このコマンドの **no** 形式を使用すると、別のグループ ポリシーから IPsec over UDP の値を継承できます。

IPsec over UDP（IPsec through NAT と呼ばれることもあります）を使用すると、Cisco VPN Client またはハードウェア クライアントは、NAT を実行している ASA に UDP 経由で接続できます。

IPsec over UDP をディセーブルにするには、**ipsec-udp disable** コマンドを使用します。

IPsec over UDP を使用するには、**ipsec-udp-port** コマンドも設定する必要があります。

また、IPsec over UDP を使用するように Cisco VPN Client を設定しておく必要があります（Cisco VPN Client は、デフォルトで IPsec over UDP を使用するように設定されています）。VPN 3002 では、IPsec over UDP を使用するためのコンフィギュレーションが必要ありません。

IPsec over UDP は独自仕様で、リモート アクセス接続にだけ適用され、モード コンフィギュレーションが必要です。つまり、ASA は SA のネゴシエーション中にクライアントとコンフィギュレーション パラメータを交換します。

IPSec over UDP を使用すると、システム パフォーマンスが若干低下します。

ipsec-udp-port コマンドは、VPN クライアントとして動作する ASA 5505 ではサポートされません。クライアント モードの ASA 5505 では、UDP ポート 500 または 4500 で IPsec セッションを開始できます。

例

次に、FirstGroup というグループ ポリシーの IPsec over UDP を設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# ipsec-udp enable
```

関連コマンド

コマンド	説明
ipsec-udp-port	ASA が UDP トラフィックを受信するポートを指定します。

ipsec-udp-port

IPsec over UDP の UDP ポート番号を設定するには、グループ ポリシー コンフィギュレーション モードで **ipsec-udp-port** コマンドを使用します。UDP ポートをディセーブルにするには、このコマンドの **no** 形式を使用します。

ipsec-udp-port *port*

no ipsec-udp-port

構文の説明

port	4001 ～ 49151 の範囲内の整数を使用して、UDP ポート番号を識別します。

デフォルト

デフォルトのポートは 10000 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(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

このコマンドの **no** 形式を使用すると、別のグループ ポリシーから IPsec over UDP のポートの値を継承できます。

IPSec ネゴシエーションでは、ASA は設定されたポートでリッスンし、他のフィルタ ルールで UDP トラフィックがドロップされていても、そのポート宛ての UDP トラフィックを転送します。

この機能をイネーブルにすると、複数のグループ ポリシーを設定し、各グループ ポリシーでそれぞれ別のポート番号を使用できます。

例

次に、FirstGroup というグループ ポリシーの IPsec UDP ポートをポート 4025 に設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# ipsec-udp-port 4025
```

関連コマンド

コマンド	説明
ipsec-udp	Cisco VPN Client またはハードウェア クライアントが、NAT を実行している ASA に UDP 経由で接続できるようにします。