CHAPTER 17

subject-name コマンド～ sysopt traffic detailed-statistics コマンド

subject-name（暗号 CA 証明書マップ）

IPsec ピア証明書のサブジェクト DN にルール エントリが適用されることを指定するには、クリプト CA 証明書マップ コンフィギュレーション モードで **subject-name** コマンドを使用します。サブジェクト名を削除するには、このコマンドの **no** 形式を使用します。

subject-name [**attr** *tag* **eq | ne |co | nc** *string*]

no subject-name [**attr** *tag* **eq | ne |co | nc** *string*]

構文の説明

attr *tag*	証明書 DN の指定された属性値のみがルール エントリ ストリングと比較されることを指定します。タグ値は次のとおりです。 DNQ = DN 修飾子 GENQ = 世代識別子 I = イニシャル GN = 姓名の名 N = 名前 SN = 姓名の姓 IP = IP アドレス SER = シリアル番号 UNAME = 非構造化名 EA = 電子メール アドレス T = タイトル O = 組織名 L = 地名 SP = 州/都道府県 C = 国 OU = 組織ユニット CN = 一般名
co	ルール エントリ ストリングが DN ストリングまたは指定された属性のサブストリングである必要があることを指定します。
eq	DN ストリングまたは指定された属性がルール ストリング全体と一致する必要があることを指定します。

nc	ルール エントリ ストリングが DN ストリングまたは指定された属性のサブストリングでないことが必要であることを指定します。
ne	DN ストリングまたは指定された属性がルール ストリング全体と一致しないことが必要であることを指定します。
string	照合される値を指定します。

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
クリプト CA 証明書マップ コンフィギュレーション	• Yes	• Yes	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、証明書マップ 1 に対して CA 証明書マップ コンフィギュレーション モードを開始して、証明書サブジェクト名の組織属性が Central と等しくなる必要があることを指定するルール エントリを作成する例を示します。

```
ciscoasa(config)# crypto ca certificate map 1
ciscoasa(ca-certificate-map)# subject-name attr o eq central
ciscoasa(ca-certificate-map)# exit
```

関連コマンド

コマンド	説明
crypto ca certificate map	CA 証明書マップ コンフィギュレーション モードを開始します。
issuer-name	ルール エントリ文字列との比較対象となる、CA 証明書に含まれている DN を指定します。
tunnel-group-map	**crypto ca certificate map** コマンドを使用して作成された証明書マップ エントリをトンネル グループに関連付けます。

subject-name（暗号 CA トラストポイント）

指定したサブジェクト DN を登録時に証明書に含めるには、クリプト CA トラストポイント コンフィギュレーション モードで **subject-name** コマンドを使用します。これは、証明書を使用する人またはシステムです。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

subject-name *X.500_name*

no subject-name

構文の説明

X.500_name	X.500 認定者名を定義します。属性と値のペアを区切るには、カンマを使用します。カンマやスペースを含む値は、引用符で囲みます。たとえば、**cn=crl,ou=certs,o="cisco systems, inc.",c=US** です。最大長は 500 文字です。

デフォルト

デフォルト設定では、サブジェクト名は含まれません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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
クリプト CA トラストポイント 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
7.0(1)	このコマンドが追加されました。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、URL https//:frog.example.com での自動登録を設定し、サブジェクト DN OU certs をトラストポイント central の登録要求に含める例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# enrollment url http://frog.example.com/
ciscoasa(ca-trustpoint)# subject-name ou=certs
ciscoasa(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
default enrollment	登録パラメータをデフォルト値に戻します。
enrollment url	CA に対する登録用の URL を指定します。

subject-name-default

ローカル CA サーバが発行するすべてのユーザ証明書でユーザ名に追加される一般的なサブジェクト名認定者名(DN)を指定するには、CA サーバ コンフィギュレーション モードで **subject-name-default** コマンドを使用します。サブジェクト名 DN をデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

subject-name-default *dn*

no subject-name-default

構文の説明

dn	ローカル CA サーバが発行するすべてのユーザ証明書でユーザ名に含める一般的なサブジェクト名 DN を指定します。サポートされている DN 属性は、cn(一般名)、ou(組織ユニット)、ol(組織の地名)、st(州)、ea(電子メール アドレス)、c(会社)、t(タイトル)、および sn(姓名の姓)です。属性と値のペアを区切るには、カンマを使用します。カンマを含む値は、引用符で囲んでください。*dn* に使用できる文字数は最大 500 文字です。

デフォルト

このコマンドは、デフォルトのコンフィギュレーションの一部ではありません。このコマンドでは、証明書のデフォルトの DN を指定します。ユーザ入力に DN がある場合、このコマンドは ASA によって無視されます。

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
CA サーバ コンフィギュレーション	• Yes	—	• Yes	—	—

コマンド履歴

リリース	変更内容
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

subject-name-default コマンドでは、発行される証明書のサブジェクト名を構成するユーザ名で使用される、共通の一般的な DN を指定します。この目的には、*dn* 値は cn=username で十分です。このコマンドによって、ユーザごとに個別にサブジェクト名 DN を定義する必要がなくなります。**crypto ca server user-db add** dn *dn* コマンドを使用してユーザが追加される場合、DN フィールドは任意です。

ASA では、このコマンドは、ユーザ入力で DN が指定されない場合に、証明書を発行するときにのみ使用されます。

例

次に、DN を指定する例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# subject-name-default cn=cisco,cn=example_corp,ou=eng,st=ma,
c="cisco systems, inc.”
ciscoasa(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
issuer-name	認証局証明書のサブジェクト名 DN を指定します。
keysize	ユーザ証明書登録で生成される公開キーと秘密キーのサイズを指定します。
ライフタイム	CA 証明書、発行済みの証明書、または CRL のライフタイムを指定します。

サブネット

ネットワーク オブジェクトのネットワークを設定するには、オブジェクト コンフィギュレーション モードで **subnet** コマンドを使用します。コンフィギュレーションからオブジェクトを削除するには、このコマンドの **no** 形式を使用します。

subnet {*IPv4_address IPv4_mask* | *IPv6_address*/*IPv6_prefix*}

no subnet {*IPv4_address IPv4_mask* | *IPv6_address*/*IPv6_prefix*}

構文の説明

IPv4_address IPv4_mask	IPv4 ネットワーク アドレスとサブネット マスクを、スペースで区切って指定します。
IPv6_address/*IPv6_prefix*	IPv6 ネットワーク アドレスとプレフィックス長を、/ 記号で区切って指定します。スペースは使用しません。

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
オブジェクト ネットワーク コンフィギュレーション	• Yes	• Yes	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
8.3(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

既存のネットワーク オブジェクトを異なる IP アドレスを使用して設定すると、新しいコンフィギュレーションが既存のコンフィギュレーションに置き換わります。

例

次に、サブネット ネットワーク オブジェクトを作成する例を示します。

```
ciscoasa (config)# object network OBJECT_SUBNET
ciscoasa (config-network-object)# subnet 10.1.1.0 255.255.255.0
```

関連コマンド

コマンド	説明
clear configure object	作成されたすべてのオブジェクトをクリアします。
説明	ネットワーク オブジェクトに説明を追加します。
fqdn	完全修飾ドメイン名のネットワーク オブジェクトを指定します。
ホスト	ホスト ネットワーク オブジェクトを指定します。
nat	ネットワーク オブジェクトの NAT をイネーブルにします。
object network	ネットワーク オブジェクトを作成します。
object-group network	ネットワーク オブジェクト グループを作成します。
range	ネットワーク オブジェクトのアドレス範囲を指定します。
show running-config object network	ネットワーク オブジェクト コンフィギュレーションを表示します。

summary-address（インターフェイス）

特定のインターフェイスの EIGRP のサマリーを設定するには、インターフェイス コンフィギュレーション モードで **summary-address** コマンドを使用します。サマリー 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。

summary-address *as-number addr mask* [*admin-distance*]

no summary-address *as-number addr mask*

構文の説明

as-number	自律システム番号。これは、EIGRP ルーティング プロセスの自律システム番号と同じである必要があります。
addr	サマリー IP アドレス。
mask	IP アドレスに適用されるサブネット マスク。
admin-distance	（任意）集約ルートのアドミニストレーティブ ディスタンス。有効な値は、0 ～ 255 です。指定されていない場合、デフォルト値は 5 です。

デフォルト

デフォルトの設定は次のとおりです。

- EIGRP は、単一のホスト ルートの場合でも、ルートをネットワーク レベルに自動的に集約します。
- EIGRP 集約ルートのアドミニストレーティブ ディスタンスは 5 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
インターフェイス 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
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードはサポートされます。

使用上のガイドライン

デフォルトでは、EIGRP はサブネット ルートをネットワーク レベルに集約します。自動ルート集約をディセーブルにするには、**no auto-summary** コマンドを使用します。**summary-address** コマンドを使用すると、サブネット ルート集約をインターフェイス単位で手動で定義できます。

例

次の例では、**tag** を 3 に設定してルート集約を設定しています。

```
ciscoasa(config-if)# summary-address 1.1.0.0 255.255.0.0
ciscoasa(config-if)#
```

次の例に、**no** 形式の **summary-address** コマンドをオプションとともに使用して、オプションをデフォルト値に戻す方法を示します。この例では、先の例で 3 に設定された **tag** 値が、**summary-address** コマンドから削除されます。

```
ciscoasa(config-if)# no summary-address 1.1.0.0 255.255.0.0
ciscoasa(config-if)#
```

次の例では、コンフィギュレーションから **summary-address** コマンドを削除しています。

```
ciscoasa(config-if)# no summary-address 1.1.0.0 255.255.0.0
ciscoasa(config-if)#
```

関連コマンド

コマンド	説明
auto-summary	EIGRP ルーティング プロセスのサマリー アドレスを自動的に作成します。

summary-prefix（IPv6 ルータ OSPF）

IPv6 サマリー プレフィックスを設定するには、IPv6 ルータ OSPF コンフィギュレーション モードで **summary-prefix** コマンドを使用します。デフォルトに戻す場合は、このコマンドの **no** 形式を入力します。

summary-prefix *prefix* [**not-advertise**] [**tag** *tag_value*]

no summary-prefix *prefix* [**not-advertise**] [**tag** *tag_value*]

構文の説明

not-advertise	（オプション）指定されたプレフィックスとマスクのペアに一致するルートを抑制します。このキーワードは OSPFv3 だけに適用されます。
prefix	宛先の IPv6 プレフィックスを指定します。
tag *tag_value*	（オプション）ルート マップを使用して再配布を制御する match 値として使用できるタグ値を指定します。このキーワードは OSPFv3 だけに適用されます。

デフォルト

デフォルトの設定は次のとおりです。

- *tag_value* は 0 です。
- 指定されたプレフィックスとマスクのペアに一致するルートは抑制されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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
IPv6 ルータ 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
9.0(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て、IPv6 サマリー プレフィックスを設定します。

例

次の例では、サマリー プレフィックス FECO::/24 が、アドレス FECO::/1 ～ FECO::/24 を含んでいます。アドレス FECO::/24 のみが外部 LSA でアドバタイズされます。

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-router)# router-id 172.16.3.3
ciscoasa(config-router)# summary-prefix FECO::/24
ciscoasa(config-router)# redistribute static
```

関連コマンド

コマンド	説明
ipv6 router ospf	OSPFv3 のルータ コンフィギュレーション モードを開始します。
redistribute	ある OSPFv3 ルーティング ドメインから別の OSPFv3 ルーティング ドメインへ IPv6 ルートを再配布します。

summary-address（ルータ ISIS）

IS-IS の集約アドレスを作成するには、ルータ ISIS コンフィギュレーション モードで **summary-address** 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。

summary-address *address mask* [**level-1 | level-1-2 | level-2**] [**tag** *tag-number*] [**metric** *metric-value*]

no summary-address *address mask* [**level-1 | level-1-2 | level-2**] [**tag** *tag-number*] [**metric** *metric-value*]

構文の説明

level-1	（オプション）設定済みアドレスとマスク値を使用して、レベル 1 に再配布されたルートのみが集約されます。
level-1-2	（オプション）ルートをレベル 1 およびレベル 2 IS-IS に再配布するとき、およびレベル 2 IS-IS がレベル 1 をエリアで到達可能なものとしてアドバタイズしたときにサマリー ルートが適用されます。
level-2	（オプション）設定済みアドレスとマスク値を使用して、レベル 1 ルーティングが学習したルートはレベル 2 バックボーンに集約されます。レベル 2 の IS-IS に再配布されたルートもサマライズされます。
address	アドレスの範囲を表すために指定するサマリー アドレス。
mask	サマリー ルートに使用される IP サブネット マスク。
tag *tag-number*	（オプション）サマリー ルートにタグを付けるために使用される整数を指定します。
metric *metric-value*	（オプション）サマリー ルートに適用されるメトリック値を指定します。

コマンド デフォルト

すべてのルートは個別にアドバタイズされます。

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
ルータ isis 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
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

複数のアドレス グループを特定のレベルに集約できます。他のルーティング プロトコルから学習したルートも集約できます。サマリーのアドバタイズに使用されるメトリックは、具体的なルートすべての中で最小のメトリックです。このコマンドは、ルーティング テーブルの容量縮小に有効です。

リンクステート パケット（LSP）とリンクステート データベース（LSDB）のサイズも小さくします。また、要約アドバタイズメントは多くの特定ルートによって異なるので、ネットワークの安定にも役立ちます。たいていの場合、1 つのルート フラップが原因で要約アドバタイズメントはフラップしません。

サマリー アドレスを使用する場合の欠点は、他のルートには、個々の宛先すべてに最適なルーティング テーブルを計算するための情報が少なくなることです。

例

次に、IS-IS に Routing Information Protocol（RIP）ルートを再配布する例を示します。RIP ネットワークでは、10.1.1、10.1.2、10.1.3、10.1.4 のような IP ルートがあります次に、10.1.0.0 のみを IS-IS レベル 1 リンクステート プロトコル データ ユニット（PDU）にアドバタイズする例を示します。サマリー アドレスに 100 のタグが付けられ、110 のメトリック値が指定されます。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# net 01.0000.0000.0001.00
ciscoasa(config-router)# redistribute rip level-1 metric 40
ciscoasa(config-router)# summary-address 10.1.0.0 255.255.0.0 tag 100 metric 110
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
認証キー	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。

コマンド	説明
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される(受信ではなく)IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト(TLV)を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。

コマンド	説明
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。

summary-address（ルータ OSPF）

OSPF の集約アドレスを作成するには、ルータ OSPF コンフィギュレーション モードで **summary-address** コマンドを使用します。サマリー アドレスまたは特定のサマリー アドレス オプ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。

summary-address *addr mask* [**not-advertise**] [**tag** *tag_value*]

no summary-address *addr mask* [**not-advertise**] [**tag** *tag_value*]

構文の説明

addr	アドレス範囲に対して指定されるサマリー アドレスの値。
mask	集約ルートに対して使用される IP サブネット マスク。
not-advertise	（任意）指定されたプレフィックス/マスク ペアと一致するルートを抑制します。
tag *tag_value*	（任意）各外部ルートに付けられた 32 ビットの 10 進値。この値は OSPF 自体には使用されません。ASBR 間での情報通信に使用されることはあります。何も指定しない場合、BGP および EGP からのルートにはリモート自律システムの番号が使用され、その他のプロトコルには 0 が使用されます。有効値の範囲は、0 ～ 4294967295 です。

デフォルト

デフォルトの設定は次のとおりです。

- *tag_value* は 0 です。
- 指定されたプレフィックス/マスク ペアと一致するルートは抑制されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

使用上のガイドライン

他のルーティング プロトコルから学習したルートをサマライズできます。このコマンドを OSPF に対して使用すると、OSPF 自律システム境界ルータ（ASBR）により、このアドレスの対象となる再配布されるすべてのルートの集約として、1 つの外部ルートがアドバタイズされます。このコマンドでは、OSPF に再配布されている、他のルーティング プロトコルからのルートのみが集約されます。OSPF エリア間のルート集約には **area range** コマンドを使用します。

summary-address コマンドをコンフィギュレーションから削除するには、このコマンドの no 形式を、任意のキーワードまたは引数を指定しないで使用します。コンフィギュレーションの summary コマンドからオプションを削除するには、このコマンドの **no** 形式を使用して、削除するオプションを指定します。詳細については、「例」を参照してください。

例

次の例では、**tag** を 3 に設定してルート集約を設定しています。

```
ciscoasa(config-router)# summary-address 1.1.0.0 255.255.0.0 tag 3
ciscoasa(config-router)#
```

次の例に、**no** 形式の **summary-address** コマンドをオプションとともに使用して、オプションをデフォルト値に戻す方法を示します。この例では、先の例で 3 に設定された **tag** 値が、**summary-address** コマンドから削除されます。

```
ciscoasa(config-router)# no summary-address 1.1.0.0 255.255.0.0 tag 3
ciscoasa(config-router)#
```

次の例では、コンフィギュレーションから **summary-address** コマンドを削除しています。

```
ciscoasa(config-router)# no summary-address 1.1.0.0 255.255.0.0
ciscoasa(config-router)#
```

関連コマンド

コマンド	説明
area range	エリア境界でルートを統合および集約します。
router ospf	ルータ コンフィギュレーション モードを開始します。
show ospf summary-address	各 OSPF ルーティング プロセスのサマリー アドレス設定を表示します。

sunrpc-server

SunRPC サービス テーブルのエントリを作成するには、グローバル コンフィギュレーション モードで **sunrpc-server** コマンドを使用します。SunRPC サービス テーブルのエントリをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

sunrpc-server *ifc_name ip_addr mask* **service** *service_type* **protocol** [**tcp** | **udp**] **port** *port* **[-** *port* **] timeout** *hh:mm:ss*

no sunrpc-server *ifc_name ip_addr mask* **service** *service_type* **protocol** [**tcp** | **udp**] **port** *port* [*- port]* **timeout** *hh:mm:ss*

no sunrpc-server active service *service_type* **server** *ip_addr*

構文の説明

ifc_name	サーバ インターフェイス名。
ip_addr	SunRPC サーバの IP アドレス。
mask	ネットワーク マスク。
port *port* [- *port*]	SunRPC プロトコルのポート範囲を指定します。
port- *port*	（任意）SunRPC プロトコルのポート範囲を指定します。
protocol tcp	SunRPC トランスポート プロトコルを指定します。
protocol udp	SunRPC トランスポート プロトコルを指定します。
service	サービスを指定します。
service_type	**sunrpcinfo** コマンドで指定した SunRPC サービス プログラム番号を設定します。
timeout *hh:mm:ss*	SunRPC サービス トラフィックへのアクセスが終了するまでのタイムアウト アイドル時間を指定します。

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	• 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

SunRPC サービス テーブルは、timeout で指定された時間、確立された SunRPC セッションに基づいて、SunRPC トラフィックが ASA を通過するのを許可するために使用します。

例

次に、SunRPC サービス テーブルを作成する例を示します。

```
ciscoasa(config)# sunrpc-server outside 10.0.0.1 255.0.0.0 service 100003 protocol TCP
port 111 timeout 0:11:00
ciscoasa(config)# sunrpc-server outside 10.0.0.1 255.0.0.0 service 100005 protocol TCP
port 111 timeout 0:11:00
```

関連コマンド

コマンド	説明
clear configure sunrpc-server	ASA からの Sun リモート プロセッサ コール サービスをクリアします。
show running-config sunrpc-server	SunRPC コンフィギュレーションに関する情報を表示します。

support-user-cert-validation

現在のトラストポイントが、リモート ユーザ証明書を発行した CA に対して認証されている場合に、このトラストポイントに基づいてリモート証明書を検証するには、クリプト CA トラストポイント コンフィギュレーション モードで **support-user-cert-validation** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

support-user-cert-validation

no support-user-cert-validation

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

デフォルト設定では、ユーザ証明書の検証がサポートされています。

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
クリプト CA トラストポイント コンフィギュレーション	• Yes	• Yes	• Yes	• Yes	• Yes

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ASA では、同じ CA に対して 2 つのトラストポイントを保持できます。この場合は、同じ CA から 2 つの異なるアイデンティティ証明書が発行されます。トラストポイントが、この機能をイネーブルにしている別のトラストポイントにすでに関連付けられている CA に対して認証される場合、このオプションは自動的にディセーブルになります。これにより、パス検証パラメータの選択であいまいさが生じないようになります。ユーザが、この機能をイネーブルにした別のトラストポイントにすでに関連付けられている CA に認証されたトラストポイントでこの機能を有効化しようとした場合、アクションは許可されません。2 つのトラストポイント上でこの設定をイネーブルにして、同じ CA の認証を受けることはできません。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、トラストポイント central でユーザ検証を受け入れることができるようにする例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# support-user-cert-validation
ciscoasa(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
default enrollment	登録パラメータをデフォルト値に戻します。

sw-module module password-reset

ソフトウェア モジュールのパスワードをデフォルト値にリセットするには、特権 EXEC モードで **sw-module module password-reset** コマンドを使用します。

sw-module module *id* **password-reset**

構文の説明

id	**cxsc** または **ips** のいずれかのモジュール ID 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。

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
特権 EXEC	• Yes	• Yes	• Yes	—	• Yes

コマンド履歴

リリース	変更内容
8.6(1)	このコマンドが追加されました。
9.1(1)	**cxsc** キーワードを使用する ASA CX ソフトウェア モジュールのサポートが追加されました。

使用上のガイドライン

パスワードをリセットした後は、モジュール アプリケーションを使用してパスワードを独自の値に変更する必要があります。モジュールのパスワードをリセットすると、モジュールがリブートします。モジュールのリブート中はサービスを使用できません。リブートには数分を要する場合があります。**show module** コマンドを実行すると、モジュールの状態をモニタできます。

コマンドは、必ずプロンプトで確認を要求します。コマンドが成功した場合は、それ以上何も出力されません。コマンドが失敗した場合は、障害が発生した理由を示すエラー メッセージが表示されます。

このコマンドは、モジュールがアップ状態である場合にのみ有効です。

デフォルトのパスワードはモジュールによって異なります。

- ASA IPS：ユーザ cisco のデフォルトのパスワードは、**cisco** です。
- ASA CX：ユーザ admin のデフォルトのパスワードは、**Admin123** です。

例

次に、IPS モジュール上のパスワードをリセットする例を示します。

```
ciscoasa# sw-module module ips password-reset
Reset the password on module ips? [confirm] y
```

関連コマンド

コマンド	説明
sw-module module recover	ディスクから回復イメージをロードして、モジュールを回復します。
sw-module module reload	モジュール ソフトウェアをリロードします。
sw-module module reset	モジュールをシャットダウンし、リロードします。
sw-module module shutdown	コンフィギュレーション データを失わずに電源を切る準備をして、モジュール ソフトウェアをシャットダウンします。
show module	モジュール情報を表示します。

sw-module module recover

ソフトウェア モジュールのリカバリ用ソフトウェア イメージをディスクからロードする場合、またはイメージの場所を設定する場合は、特権 EXEC モードで **sw-module module recover** コマンドを使用します。たとえば、モジュールが現在のイメージをロードできない場合などに、このコマンドを使用してモジュールを回復することが必要になることがあります。

sw-module module *id* **recover** {**boot** | **stop** | **configure image** *path*}

構文の説明

id	次のいずれかのモジュール ID を指定します。 • **sfr**：ASA FirePOWER モジュール。 • **ips**：IPS モジュール • **cxsc**：ASA CX モジュール
boot	このモジュールの回復を開始し、**configure** 設定に従って回復イメージをダウンロードします。ダウンロード後、モジュールは新しいイメージからリブートします。
configure image *path*	ローカル ディスク上の新しいイメージの場所を設定します（例：disk0:image2）。
stop	リカバリ アクションを停止し、モジュールのイメージ ファイルを削除します。このコマンドは、**sw-module module** *id* **recover boot** コマンドを使用して回復を開始してから 30 秒以内に入力する必要があります。この期間が経過した後で **stop** コマンドを入力すると、モジュールが無応答になるなど、予期しない結果になることがあります。 すでにモジュールが無応答になっている場合、リブートしたり新しいイメージを適用したりするには、停止する必要が生じることがあります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.6(1)	このコマンドが追加されました。
9.1(1)	**cxsc** キーワードを使用する ASA CX ソフトウェア モジュールのサポートが追加されました。
9.2(1)	**sfr** キーワードを使用する ASA FirePOWER モジュールのサポートが追加されました。

使用上のガイドライン

このコマンドを使用して、ソフトウェア モジュールをインストールします。このモジュールは、デバイスで設定されていない新しいモジュールである場合と、障害が発生したために再インストールが必要となった既存のモジュールである場合があります。

イメージをインストールする場合は、次のコマンド シーケンスを使用します。

- **sw-module module** *id* **configure image** *path*（ソフトウェア モジュール イメージの disk0 上の場所を指定）。
- **sw-module module** *id* **boot**（該当イメージをブート）。

イメージのブートは、モジュールがアップ、ダウン、無応答、または回復のいずれかの状態である場合にのみ可能です。ステート情報については、**show module** コマンドを参照してください。モジュールがアップ状態でない場合、ASA は強制的にモジュールをシャットダウンします。強制シャットダウンでは、すべてのコンフィギュレーションを含む、古いモジュール ディスク イメージが破壊されます。このため、ディザスタ リカバリ メカニズムとしてのみ使用してください。

show module *id* **recover** コマンドを使用してリカバリ コンフィギュレーションを表示できます。

（注） IPS モジュールの場合、モジュール ソフトウェア内部では、イメージをインストールするために **upgrade** コマンドを使用しないでください。モジュールのインストールおよび初期設定を完了する方法については、各ソフトウェア モジュールの CLI 設定ガイドを参照してください。

例

次に、disk0:image2 からイメージをダウンロードするようにモジュールを設定する例を示します。

```
ciscoasa# sw-module module ips recover configure image disk0:image2
```

次に、モジュールを回復する例を示します。

```
ciscoasa# sw-module module ips recover boot
The module in slot ips will be recovered.  This may
erase all configuration and all data on that device and
attempt to download a new image for it.
Recover module in slot ips? [confirm]
```

関連コマンド

コマンド	説明
debug module-boot	モジュールのブート プロセスに関するデバッグ メッセージを表示します。
sw-module module reset	モジュールをシャットダウンし、リセットを実行します。
sw-module module reload	モジュール ソフトウェアをリロードします。

コマンド	説明
sw-module module shutdown	コンフィギュレーション データを失わずに電源を切る準備をして、モジュール ソフトウェアをシャットダウンします。
show module	モジュール情報を表示します。

sw-module module reload

ソフトウェア モジュールのモジュール ソフトウェアをリロードするには、特権 EXEC モードで **sw-module module reload** コマンドを使用します。

sw-module module *id* **reload**

構文の説明

id	次のいずれかのモジュール ID を指定します。 • **sfr**：ASA FirePOWER モジュール。 • **ips**：IPS モジュール • **cxsc**：ASA CX モジュール

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.6(1)	このコマンドが追加されました。
9.1(1)	**cxsc** キーワードを使用する ASA CX ソフトウェア モジュールのサポートが追加されました。
9.2(1)	**sfr** キーワードを使用する ASA FirePOWER モジュール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、モジュールをリロードする前にリセットを実行する **sw-module module reset** コマンドとは異なります。

このコマンドは、モジュールのステータスがアップ状態にある場合だけ有効です。ステート情報については、**show module** コマンドを参照してください。

例

次に、IPS モジュールをリロードする例を示します。

```
ciscoasa# sw-module module ips reload
Reload module in slot ips? [confirm] y
Reload issued for module in slot ips
%XXX-5-505002: Module in slot ips is reloading.  Please wait...
%XXX-5-505006: Module in slot ips is Up.
```

関連コマンド

コマンド	説明
debug module-boot	モジュールのブート プロセスに関するデバッグ メッセージを表示します。
sw-module module recover	ディスクから回復イメージをロードして、モジュールを回復します。
sw-module module reset	モジュールをシャットダウンし、リセットを実行します。
sw-module module shutdown	コンフィギュレーション データを失わずに電源を切る準備をして、モジュール ソフトウェアをシャットダウンします。
show module	モジュール情報を表示します。

sw-module module reset

モジュールをリセットしてからモジュール ソフトウェアをリロードするには、特権 EXEC モードで **sw-module module reset** コマンドを使用します。

sw-module module *id* **reset**

構文の説明

id	次のいずれかのモジュール ID を指定します。 • **sfr**：ASA FirePOWER モジュール。 • **ips**：IPS モジュール • **cxsc**：ASA CX モジュール

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.6(1)	このコマンドが追加されました。
9.1(1)	**cxsc** キーワードを使用する ASA CX ソフトウェア モジュールのサポートが追加されました。
9.2(1)	**sfr** キーワードを使用する ASA FirePOWER モジュールのサポートが追加されました。

使用上のガイドライン

モジュールがアップ状態の場合、**sw-module module reset** コマンドによって、リセットの前にソフトウェアをシャットダウンするように要求されます。

sw-module module recover コマンドを使用してモジュールを回復できます。モジュールが回復状態になっているときに **sw-module module reset** コマンドを入力しても、モジュールは回復プロセスを中断しません。**sw-module module reset** コマンドによって、モジュールのリセットが実行され、リセット後にモジュールの回復が続行します。モジュールがハングした場合は、回復中にモジュールをリセットできます。ハードウェア リセットによって、問題が解決することもあります。

このコマンドは、ソフトウェアのリロードのみを行いリセットは行わない **sw-module module reload** コマンドとは異なります。

このコマンドは、モジュールのステータスがアップ、ダウン、無応答、または回復のいずれかの場合にのみ有効です。ステート情報については、**show module** コマンドを参照してください。

例

次に、アップ状態の IPS モジュールをリセットする例を示します。

```
ciscoasa# sw-module module ips reset
The module in slot ips should be shut down before
resetting it or loss of configuration may occur.
Reset module in slot ips? [confirm] y
Reset issued for module in slot ips
%XXX-5-505001: Module in slot ips is shutting down.  Please wait...
%XXX-5-505004: Module in slot ips shutdown is complete.
%XXX-5-505003: Module in slot ips is resetting.  Please wait...
%XXX-5-505006: Module in slot ips is Up.
```

関連コマンド

コマンド	説明
debug module-boot	モジュールのブート プロセスに関するデバッグ メッセージを表示します。
sw-module module recover	ディスクから回復イメージをロードして、モジュールを回復します。
sw-module module reload	モジュール ソフトウェアをリロードします。
sw-module module shutdown	コンフィギュレーション データを失わずに電源を切る準備をして、モジュール ソフトウェアをシャットダウンします。
show module	モジュール情報を表示します。

sw-module module shutdown

モジュール ソフトウェアをシャットダウンするには、特権 EXEC モードで **sw-module module shutdown** コマンドを使用します。

sw-module module *id* **shutdown**

構文の説明

id	次のいずれかのモジュール ID を指定します。 • **sfr**：ASA FirePOWER モジュール。 • **ips**：IPS モジュール • **cxsc**：ASA CX モジュール

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.6(1)	このコマンドが追加されました。
9.1(1)	**cxsc** キーワードを使用する ASA CX ソフトウェア モジュールのサポートが追加されました。
9.2(1)	**sfr** キーワードを使用する ASA FirePOWER モジュールのサポートが追加されました。

使用上のガイドライン

モジュール ソフトウェアをシャットダウンするのは、コンフィギュレーション データを失うことなく安全にモジュールの電源をオフにできるように準備するためです。

このコマンドは、モジュール ステータスがアップまたは無応答である場合にのみ有効です。ステート情報については、**show module** コマンドを参照してください。

例

次に、IPS モジュールをシャットダウンする例を示します。

```
ciscoasa# sw-module module ips shutdown
Shutdown module in slot ips? [confirm] y
Shutdown issued for module in slot ips
ciscoasa#
%XXX-5-505001: Module in slot ips is shutting down.  Please wait...
%XXX-5-505004: Module in slot ips shutdown is complete.
```

関連コマンド

コマンド	説明
debug module-boot	モジュールのブート プロセスに関するデバッグ メッセージを表示します。
sw-module module recover	ディスクから回復イメージをロードして、モジュールを回復します。
sw-module module reload	モジュール ソフトウェアをリロードします。
sw-module module reset	モジュールをシャットダウンし、リセットを実行します。
show module	モジュール情報を表示します。

sw-module module uninstall

ソフトウェア モジュール イメージおよび関連するコンフィギュレーションをアンインストールするには、特権 EXEC モードで **sw-module module uninstall** コマンドを使用します。

sw-module module *id* **uninstall**

構文の説明

id	次のいずれかのモジュール ID を指定します。 • **sfr**：ASA FirePOWER モジュール。 • **ips**：IPS モジュール • **cxsc**：ASA CX モジュール

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.6(1)	このコマンドが追加されました。
9.1(1)	**cxsc** キーワードを使用する ASA CX ソフトウェア モジュールのサポートが追加されました。
9.2(1)	**sfr** キーワードを使用する ASA FirePOWER モジュール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、ソフトウェア モジュール イメージおよび関連するコンフィギュレーションを永続的にアンインストールします。

例

次に、IPS モジュール イメージおよびコンフィギュレーションをアンインストールする例を示します。

```
ciscoasa# sw-module module ips uninstall
Module ips will be uninstalled.This will completely remove the
disk image associated with the sw-module including any configuration
that existed within it.

Uninstall module <id>? [confirm]
```

関連コマンド

コマンド	説明
debug module-boot	モジュールのブート プロセスに関するデバッグ メッセージを表示します。
sw-module module recover	ディスクから回復イメージをロードして、モジュールを回復します。
sw-module module reload	モジュール ソフトウェアをリロードします。
sw-module module reset	モジュールをシャットダウンし、リセットを実行します。
show module	モジュール情報を表示します。

switchport access vlan

ASA 5505 適応型セキュリティ アプライアンスなど、組み込みスイッチを搭載したモデルの場合、インターフェイス コンフィギュレーション モードで **switchport access vlan** コマンドを使用して、スイッチ ポートを VLAN に割り当てます。

switchport access vlan *number*

no switchport access vlan *number*

構文の説明

vlan *number*	このスイッチ ポートを割り当てる VLAN ID を指定します。VLAN ID の範囲は 1 ～ 4090 です。

デフォルト

デフォルトでは、すべてのスイッチ ポートが VLAN 1 に割り当てられています。

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
インターフェイス 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
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

トランスペアレント ファイアウォール モードでは、ASA 5505 適応型セキュリティ アプライアンスの Base ライセンスで 2 つのアクティブ VLAN、Security Plus ライセンスで 3 つのアクティブ VLAN を設定でき、そのうちの 1 つはフェールオーバー用である必要があります。

ルーテッド モードでは、ASA 5505 適応型セキュリティ アプライアンスの Base ライセンスで最大 3 つのアクティブ VLAN、Security Plus ライセンスで最大 20 のアクティブ VLAN を設定できます。

アクティブな VLAN とは、**nameif** コマンドが設定された VLAN のことです。

switchport access vlan コマンドを使用して、1 つ以上の物理インターフェイスを各 VLAN に割り当てることができます。デフォルトでは、インターフェイスの VLAN モードはアクセス ポートになります（インターフェイスに関連付けられた 1 つの VLAN）。インターフェイスで複数の VLAN を渡すトランク ポートを作成する場合は、**switchport mode access trunk** コマンドを使用してモードをトランク モードに変更してから、**switchport trunk allowed vlan** コマンドを使用します。

例

次に、5 つの物理インターフェイスを 3 つの VLAN インターフェイスに割り当てる例を示します。

```
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

...
```

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 running-config interface	実行コンフィギュレーションのインターフェイス コンフィギュレーションを表示します。
switchport mode	VLAN モードをアクセスまたはトランクに設定します。
switchport protected	セキュリティを高めるため、スイッチ ポートが同一 VLAN 上の別のスイッチ ポートと通信しないようにします。
switchport trunk allowed vlan	VLAN をトランク ポートに割り当てます。

switchport mode

ASA 5505 適応型セキュリティ アプライアンスなど、組み込みスイッチを搭載したモデルの場合、インターフェイス コンフィギュレーション モードで **switchport mode** コマンドを使用して、VLAN モードをアクセス(デフォルト)またはトランクに設定します。

switchport mode {**access** | **trunk**}

no switchport mode {**access** | **trunk**}

構文の説明

アクセス	スイッチ ポートをアクセス モードに設定します。このモードでは、スイッチ ポートで 1 つの VLAN のみのトラフィックを渡すことができます。パケットは、802.1Q VLAN タグなしでスイッチ ポートから出ます。パケットがタグ付きでスイッチ ポートに入ると、パケットはドロップされます。
トランク	スイッチ ポートをトランク モードに設定します。そのため、複数の VLAN のトラフィックを渡すことができます。パケットは、802.1Q VLAN タグ付きでスイッチ ポートから出ます。パケットがタグなしでスイッチ ポートに入ると、パケットはドロップされます。

デフォルト

デフォルトでは、モードはアクセスです。

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
インターフェイス 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
7.2(1)	このコマンドが追加されました。
7.2(2)	1 つのトランクに制限されず、複数のトランク ポートを設定できるようになりました。

使用上のガイドライン

デフォルトでは、スイッチ ポートの VLAN モードはアクセス ポートになります（スイッチ ポートに関連付けられた 1 つの VLAN）。アクセス モードでは、**switchport access vlan** コマンドを使用してスイッチ ポートを VLAN に割り当てます。スイッチ ポートで複数の VLAN を渡すトランク ポートを作成する場合は、モードをトランク モードに設定してから、**switchport trunk allowed vlan** コマンドを使用して複数の VLAN をトランクに割り当てます。モードをトランク モードに設定し、**switchport trunk allowed vlan** コマンドを設定していない状態では、スイッチ ポートは「回線プロトコル ダウン」状態になり、トラフィック転送に参加できません。トランク モードが使用できるのは Security Plus ライセンスだけです。

モードをアクセス モードに設定しない限り、**switchport vlan access** コマンドは有効になりません。モードをトランク モードに設定しない限り、**switchport trunk allowed vlan** コマンドは有効になりません。

例

次に、VLAN 100 に割り当てられたアクセス モードのスイッチ ポートおよび VLAN 200 および 300 に割り当てられたトランク モードのスイッチ ポートを設定する例を示します。

```
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 mode trunk
ciscoasa(config-if)# switchport trunk allowed vlan 200,300
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。
show running-config interface	実行コンフィギュレーションのインターフェイス コンフィギュレーションを表示します。
switchport access vlan	スイッチ ポートを VLAN に割り当てます。
switchport protected	セキュリティを高めるため、スイッチ ポートが同一 VLAN 上の別のスイッチ ポートと通信しないようにします。
switchport trunk allowed vlan	VLAN をトランク ポートに割り当てます。

switchport monitor

ASA 5505 適応型セキュリティ アプライアンスなど、組み込みスイッチを搭載したモデルの場合、インターフェイス コンフィギュレーション モードで **switchport monitor** コマンドを使用して、SPAN（スイッチ ポート モニタリングとも呼ばれる）をイネーブルにします。このコマンドを入力する対象のポート（宛先ポートと呼ばれる）では、指定した送信元ポートで送受信されるすべてのパケットのコピーを受信します。SPAN 機能を使用すると、トラフィックをモニタできるように、スニファを宛先ポートに接続できます。このコマンドを複数回入力して、複数の送信元ポートを指定できます。SPAN をイネーブルにすることができるのは、1 つの宛先ポートのみです。送信元ポートのモニタリング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。

switchport monitor *source_port* [**tx | rx | both**]

no switchport monitor *source_port* [**tx | rx | both**]

構文の説明

both	（任意）送信トラフィックと受信トラフィックの両方をモニタすることを指定します。**both** がデフォルトです。
rx	（任意）受信トラフィックのみをモニタすることを指定します。
source_port	モニタするポートを指定します。任意のイーサネット ポートおよび VLAN インターフェイス間でトラフィックを渡す Internal-Data0/1 バックプレーン ポートを指定できます。Internal-Data0/1 ポートはギガビット イーサネット ポートであるため、ファスト イーサネット宛先ポートをトラフィックによって過負荷にする場合があります。Internal-Data0/1 ポートは注意してモニタしてください。
tx	（任意）送信トラフィックのみをモニタすることを指定します。

デフォルト

モニタするトラフィックのデフォルトのタイプは **both** 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
インターフェイス 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
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

SPAN をイネーブルにしない場合、スニファをスイッチ ポートの 1 つに接続すると、そのポートで送受信されるトラフィックのみがキャプチャされます。複数のポートで送受信されるトラフィックをキャプチャするには、SPAN をイネーブルにし、モニタするポートを指定する必要があります。

ネットワーク ループになる可能性があるため、SPAN 宛先ポートを別のスイッチに接続するときは注意してください。

例

次に、イーサネット 0/0 ポートとイーサネット 0/2 ポートをモニタする宛先ポートとして、イーサネット 0/1 ポートを設定する例を示します。

```
ciscoasa(config)# interface ethernet 0/1
ciscoasa(config-if)# switchport monitor ethernet 0/0
ciscoasa(config-if)# switchport monitor ethernet 0/2
```

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。
show running-config interface	実行コンフィギュレーションのインターフェイス コンフィギュレーションを表示します。
switchport access vlan	スイッチ ポートを VLAN に割り当てます。
switchport protected	セキュリティを高めるため、スイッチ ポートが同一 VLAN 上の別のスイッチ ポートと通信しないようにします。

switchport protected

ASA 5505 適応型セキュリティ アプライアンスなど、組み込みスイッチを搭載したモデルの場合、インターフェイス コンフィギュレーション モードで **switchport protected** コマンドを使用して、スイッチ ポートが同じ VLAN 上の他の保護されたスイッチ ポートと通信しないようにします。この機能により、あるスイッチ ポートが侵害された場合に、VLAN 上の他のスイッチ ポートに対して強固なセキュリティを提供します。

switchport protected

no switchport protected

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトでは、インターフェイスは保護されていません。

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	• Yes	• Yes	• Yes	—	—

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

スイッチ ポート上のデバイスが主に他の VLAN からアクセスされる場合、VLAN 内アクセスを許可する必要がない場合、および感染やその他のセキュリティ侵害に備えてデバイスを相互に分離する場合に、スイッチ ポートが相互に通信しないようにします。たとえば、3 つの Web サーバをホストする DMZ がある場合、各スイッチ ポートに **switchport protected** コマンドを適用すると、Web サーバを相互に分離できます。内部ネットワークと外部ネットワークはいずれも 3 つの Web サーバすべてと通信でき、その逆も可能ですが、Web サーバは相互に通信できません。

保護されていないポートとの通信は、このコマンドによって制限されません。

例

次に、7 つのスイッチ ポートを設定する例を示します。イーサネット 0/4、0/5、および 0/6 は DMZ ネットワークに割り当てられ、相互から保護されます。

```
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 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)# switchport protected
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/5
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# switchport protected
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/6
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# switchport protected
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。
show running-config interface	実行コンフィギュレーションのインターフェイス コンフィギュレーションを表示します。
switchport access vlan	スイッチ ポートを VLAN に割り当てます。
switchport mode	VLAN モードをアクセスまたはトランクに設定します。
switchport trunk allowed vlan	VLAN をトランク ポートに割り当てます。

switchport trunk

ASA 5505 適応型セキュリティ アプライアンスなど、組み込みスイッチを搭載したモデルの場合、インターフェイス コンフィギュレーション モードで **switchport trunk** コマンドを使用して、VLAN をトランク ポートに割り当てます。VLAN をトランクから削除するには、このコマンドの **no** 形式を使用します。

switchport trunk {allowed vlans *vlan_range* **| native vlan** v*lan*}

no switchport trunk {allowed vlans *vlan_range* **| native vlan** v*lan*}

構文の説明

allowed vlans *vlan_range*	トランク ポートに割り当てることができる 1 つ以上の VLAN を指定します。VLAN ID の範囲は 1 ～ 4090 です。 *vlan_range* は、次のいずれかの方法で指定できます。 • 単一の番号（n） • 範囲（n-x） 番号および範囲は、カンマで区切ります。たとえば、次のように指定します。 5,7-10,13,45-100 カンマの代わりにスペースを入力できますが、コマンドはカンマ付きでコンフィギュレーションに保存されます。 このコマンドにネイティブ VLAN を含めることができますが、必須ではありません。ネイティブ VLAN は、このコマンドに含まれているかどうかに関係なく渡されます。
native vlan *vlan*	ネイティブ VLAN をトランクに割り当てます。ネイティブ VLAN 上のパケットは、トランク経由で送信されるときに変更されません。 たとえば、ポートに VLAN 2、3、および 4 が割り当てられており、VLAN 2 がネイティブ VLAN である場合、ポートを出る VLAN 2 上のパケットは 802.1Q ヘッダーによって変更されません。このポートに入るフレームで 802.1Q ヘッダーがないものは、VLAN 2 に渡されます。 各ポートのネイティブ VLAN は 1 つのみですが、すべてのポートに同じネイティブ VLAN または異なるネイティブ VLAN を使用できます。

デフォルト

デフォルトでは、VLAN はトランクに割り当てられていません。

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		
				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
インターフェイス 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
7.2(1)	このコマンドが追加されました。
7.2(2)	このコマンドは、スイッチ ポートごとに 4 つ以上の VLAN を許可するように変更されました。また、1 つのみに制限されず、複数のトランク ポートを設定できるようになりました。このコマンドで、VLAN ID を区切るためにスペースではなくカンマも使用されます。
7.2(4)/8.0(4)	**native vlan** キーワードを使用するネイティブ VLAN サポートが追加されました。

使用上のガイドライン

スイッチ ポートで複数の VLAN を渡すトランク ポートを作成する場合は、**switchport mode trunk** コマンドを使用してモードをトランク モードに設定してから、**switchport trunk** コマンドを使用して VLAN をトランクに割り当てます。このスイッチ ポートに少なくとも 1 つの VLAN を割り当てるまで、このスイッチ ポートでトラフィックを渡すことはできません。モードをトランク モードに設定し、**switchport trunk allowed vlan** コマンドを設定していない状態では、スイッチ ポートは「回線プロトコル ダウン」状態になり、トラフィック転送に参加できません。トランク モードが使用できるのは Security Plus ライセンスだけです。**switchport mode trunk** コマンドを使用してモードをトランク モードに設定しない限り、**switchport trunk** コマンドは有効になりません。

(注) このコマンドにはバージョン 7.2(1) との下位互換性はありません。VLAN を区切るカンマは 7.2(1) では認識されません。ダウングレードする場合は、VLAN をスペースで区切り、3 つの VLAN という制限を超えないようにしてください。

例

次に、7 つの VLAN インターフェイスを設定する例を示します。**failover lan** コマンドを使用して設定するフェールオーバー インターフェイスが含まれています。VLAN 200、201、および 202 は、イーサネット 0/1 でトランキングされています。

```
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 201
ciscoasa(config-if)# nameif dept1
ciscoasa(config-if)# security-level 90
ciscoasa(config-if)# ip address 10.2.2.1 255.255.255.0
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface vlan 202
ciscoasa(config-if)# nameif dept2
ciscoasa(config-if)# security-level 90
ciscoasa(config-if)# ip address 10.2.3.1 255.255.255.0
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 mode trunk
ciscoasa(config-if)# switchport trunk allowed vlan 200-202
ciscoasa(config-if)# switchport trunk native vlan 5
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
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 running-config interface	実行コンフィギュレーションのインターフェイス コンフィギュレーションを表示します。
switchport access vlan	スイッチ ポートを VLAN に割り当てます。
switchport mode	VLAN モードをアクセスまたはトランクに設定します。
switchport protected	セキュリティを高めるため、スイッチ ポートが同一 VLAN 上の別のスイッチ ポートと通信しないようにします。

synack-data

データが含まれる TCP SYNACK パケットのアクションを設定するには、tcp マップ コンフィギュレーション モードで **synack-data** 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。

synack-data {**allow** | **drop**}

no synack-data

構文の説明

allow	データが含まれる TCP SYNACK パケットを許可します。
drop	データが含まれる TCP SYNACK パケットをドロップします。

デフォルト

デフォルト アクションでは、データが含まれる TCP SYNACK パケットをドロップします。

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
TCP マップ コンフィギュレーション	• Yes	• Yes	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
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. **synack-data**：tcp マップ コンフィギュレーション モードでは、**synack-data** などの数多く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。

例

次に、データが含まれる TCP SYNACK 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)# synack-data 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 ポリシー内で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。

synchronization

BGP と内部ゲートウェイ プロトコル(IGP)システム間の同期をイネーブルにするには、アドレス ファミリ コンフィギュレーション モードで **synchronization** コマンドを使用します。Cisco IOS ソフトウェアが IGP を待機せずにネットワーク ルートをアドバタイズ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。

同期

no synchronization

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
アドレスファミリ 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
9.2(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

通常、ルートがローカルであるか IGP に存在する場合を除き、BGP スピーカーは外部ネイバーにルートをアドバタイズしません。デフォルトでは BGP と IGP 間の同期はオフになっており、Cisco IOS ソフトウェアが IGP を待機せずにネットワーク ルートをアドバタイズできるようになっています。この機能により、自律システム内のルータおよびアクセス サーバは、BGP が他の自律システムでルートを使用可能にする前にルートを確保できるようになります。

自律システム内のルータが BGP を実行していない場合は、**synchronization** コマンドを使用します。

例

次に、アドレス ファミリ コンフィギュレーション モードで同期をイネーブルにする例を示します。ルータは、ルートを外部にアドバタイズする前に、IGP 内のネットワーク ルートを検証します。

```
ciscoasa(config)# router bgp 65120
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# synchronization
```

syn-data

データが含まれる SYN パケットを許可またはドロップするには、tcp マップ コンフィギュレーション モードで **syn-data** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

syn-data {**allow** | **drop**}

no syn-data {**allow** | **drop**}

構文の説明

allow	データが含まれる SYN パケットを許可します。
drop	データが含まれる SYN パケットをドロップします。

デフォルト

デフォルトでは、SYN データが含まれるパケットは許可されます。

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
TCP マップ コンフィギュレーション	• Yes	• Yes	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
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

tcp-map コマンドはモジュラ ポリシー フレームワーク インフラストラクチャと一緒に使用されます。**class-map** コマンドを使用してトラフィックのクラスを定義し、**tcp-map** コマンドで TCP インスペクションをカスタマイズします。**policy-map** コマンドを使用して、新しい TCP マップを適用します。**service-policy** コマンドで、TCP インスペクションをアクティブにします。

tcp-map コマンドを使用して、TCP マップ コンフィギュレーション モードを開始します。tcp マップ コンフィギュレーション モードで **syn-data** コマンドを使用して、SYN パケット内にデータが含まれるパケットをドロップします。

TCP の仕様によると、TCP 実装は SYN パケット内に含まれているデータを受け入れる必要があります。これは微妙であいまいな点であるため、一部の実装ではこのことが正しく処理されない場合があります。不適切なエンドシステム実装などの挿入攻撃に対する脆弱性を回避するために、SYN パケット内にデータが含まれるパケットをドロップすることを選択できます。

例

次に、データが含まれる SYN パケットをすべての TCP フローでドロップする例を示します。

```
ciscoasa(config)# access-list TCP extended permit tcp any any
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# syn-data drop
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match access-list TCP
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	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。
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。
set connection	接続値を設定します。
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。

sysopt connection permit-vpn

VPN トンネルを介して ASA に入り復号化されるトラフィックに対して、グローバル コンフィギュレーション モードで **sysopt connection permit-vpn** コマンドを使用して、トラフィックがインターフェイス アクセス リストをバイパスできるようにします。グループ ポリシーおよびユーザ単位の認可アクセス リストは、引き続きトラフィックに適用されます。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。

sysopt connection permit-vpn

no sysopt connection permit-vpn

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

この機能は、デフォルトでイネーブルにされています。

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	• 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、デフォルトでイネーブルになりました。また、インターフェイス アクセス リストのみがバイパスされます。グループ ポリシーまたはユーザ単位のアクセス リストは有効なままです。
7.1(1)	このコマンドは、**sysopt connection permit-ipsec** から変更されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

デフォルトでは、ASA によって、VPN トラフィックが ASA のインターフェイスで終端することが許可されています。IKE または ESP（またはその他のタイプの VPN パケット）をインターフェイス アクセス リストで許可する必要はありません。デフォルトでは、復号化された VPN パケットのローカル IP アドレスのインターフェイス アクセス リストも必要ありません。VPN トンネルは VPN セキュリティ メカニズムを使用して正常に終端されたため、この機能によって、コンフィギュレーションが簡略化され、ASA のパフォーマンスはセキュリティ リスクを負うことなく最大化されます（グループ ポリシーおよびユーザ単位の認可アクセス リストは、引き続きトラフィックに適用されます）。

no sysopt connection permit-vpn コマンドを入力して、インターフェイス アクセス リストをローカル IP アドレスに適用できます。アクセス リストを作成してインターフェイスに適用するには、**access-list** コマンドおよび **access-group** コマンドを参照してください。アクセス リストは、ローカル IP アドレスに適用され、VPN パケットが復号化される前に使用された元のクライアント IP アドレスには適用されません。

例

次に、復号化された VPN トラフィックがインターフェイス アクセス リストに従うようにする例を示します。

```
ciscoasa(config)# no sysopt connection permit-vpn
```

関連コマンド

コマンド	説明
clear configure sysopt	**sysopt** コマンド コンフィギュレーションをクリアします。
show running-config sysopt	**sysopt** コマンド コンフィギュレーションを表示します。
sysopt connection tcpmss	TCP セグメントの最大サイズを上書きします。または、確実に最大サイズが指定したサイズよりも小さくならないようにします。
sysopt connection timewait	最後の標準 TCP クローズダウン シーケンスの後、各 TCP 接続が短縮 TIME_WAIT 状態を保持するようにします。

sysopt connection preserve-vpn-flows

トンネルのドロップおよび回復後のタイムアウト期間内に、ステートフル(TCP)トンネル IPSec LAN-to-LAN トラフィックを保持して再開するには、**sysopt connection preserve-vpn-flows** コマンドを使用します。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。

sysopt connection preserve-vpn-flows

no sysopt connection preserve-vpn-flows

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

この機能はデフォルトで無効に設定されています。

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	• Yes	• Yes	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

永続的 IPSec トンネル フロー機能がイネーブルの場合、タイムアウト ウィンドウ内にトンネルが再作成される限り、セキュリティ アプライアンスで元のフロー内の状態情報にアクセスできるため、データは正常に流れ続けます。

このコマンドでは、ネットワーク拡張モードを含め、IPSec LAN-to-LAN トンネルのみがサポートされます。AnyConnect/SSL VPN または IPSec リモートアクセス トンネルはサポートされません。

例

次に、トンネルがドロップされ、タイムアウト期間内に再確立された後、トンネルの状態情報が保持されてトンネル IPSec LAN-to-LAN VPN トラフィックが再開されることを指定する例を示します。

```
ciscoasa(config)# no sysopt connection preserve-vpn-flows
```

この機能がイネーブルかどうかを確認するには、sysopt に対して show run all コマンドを入力します。

```
ciscoasa(config)# show run all sysopt
```

結果の例は次のとおりです。説明のために、これ以降のすべての例では、preserve-vpn-flows の項目は太字になっています。

```
no sysopt connection timewait
sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
sysopt connection permit-vpn
no sysopt connection reclassify-vpn
no sysopt connection preserve-vpn-flows
hostname(config)#
```

sysopt connection reclassify-vpn

既存の VPN フローを再分類するには、グローバル コンフィギュレーション モードで **sysopt connection reclassify-vpn** コマンドを使用します。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。

sysopt connection reclassify-vpn

no sysopt connection reclassify-vpn

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

この機能は、デフォルトでイネーブルにされています。

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	• Yes	—	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

VPN トンネルがアップになると、このコマンドによって既存の VPN フローは再分類され、暗号化が必要なフローは分解されて再作成されます。

このコマンドは、LAN-to-LAN およびダイナミック VPN についてのみ適用されます。このコマンドは EZVPN または VPN クライアント接続には影響しません。

例

次に、VPN 再分類をイネーブルにする例を示します。

```
ciscoasa(config)# sysopt connection reclassify-vpn
```

関連コマンド

コマンド	説明
clear configure sysopt	**sysopt** コマンド コンフィギュレーションをクリアします。
show running-config sysopt	**sysopt** コマンド コンフィギュレーションを表示します。
sysopt connection permit-vpn	インターフェイスのアクセス リストを確認することなく、IPsec トンネルを経由してきたパケットを許可します。
sysopt connection tcpmss	TCP セグメントの最大サイズを上書きします。または、確実に最大サイズが指定したサイズよりも小さくならないようにします。
sysopt connection timewait	最後の標準 TCP クローズダウン シーケンスの後、各 TCP 接続が短縮 TIME_WAIT 状態を保持するようにします。

sysopt connection tcpmss

通過トラフィックの最大 TCP セグメント サイズが設定した値を超えないようにし、指定したサイズ未満にならないようにするには、グローバル コンフィギュレーション モードで **sysopt connection tcpmss** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

sysopt connection tcpmss [**minimum**] *bytes*

no sysopt connection tcpmss [**minimum**] [*bytes*]

構文の説明

bytes	最大 TCP セグメント サイズをバイト単位で設定します(48 ～任意の最大値)。デフォルト値は 1380 バイトです。この機能をディセーブルにするには、*bytes* を 0 に設定します。 **minimum** キーワードの場合、*bytes* は許可される最も小さい最大値を表します。
minimum	最大セグメント サイズを上書きし、*bytes* 未満にならないようにします(48 ～ 65535 バイト)。この機能は、デフォルトでディセーブルです(0 に設定)。

デフォルト

デフォルトでは、ASA の最大 TCP MSS は 1380 バイトです。このデフォルトは、ヘッダーが最大 120 バイトの IPv4 IPsec VPN 接続に対応しています。この値は、MTU の デフォルトの 1500 バイト内にも収まっています。

minimum 機能は、デフォルトでディセーブルです(0 に設定)。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
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

最大セグメント サイズ(TCP MSS)とは、あらゆる TCP および IP ヘッダーが追加される前の TCP ペイロードのサイズです。UDP パケットは影響を受けません。接続を確立するときのスリーウェイ ハンドシェイク中に、クライアントとサーバは TCP MSS 値を交換します。

通過トラフィックの TCP MSS を ASA に設定できます。デフォルトでは、最大 TCP MSS は 1380 バイトに設定されます。この設定は、ASA が IPsec VPN カプセル化のパケット サイズを追加する必要がある場合に役立ちます。ただし、非 IPsec エンドポイントでは、ASA の最大 TCP MSS を無効にする必要があります。

最大 TCP MSS を設定している場合、接続のいずれかのエンドポイントが ASA に設定された値を超える TCP MSS を要求すると、ASA は要求パケット内の TCP MSS を ASA の最大サイズで上書きします。ホストまたはサーバが TCP MSS を要求しない場合、ASA は RFC 793 のデフォルト値 536 バイト(IPv4)または 1220 バイト(IPv6)を想定しますが、パケットは変更しません。たとえば、MTU を デフォルトの 1500 バイトのままにします。ホストは、1500 バイトの MSS から TCP および IP のヘッダー長を減算して、MSS を 1460 バイトに設定するように要求します。ASA の最大 TCP MSS が 1380(デフォルト)の場合は、ASA は TCP 要求パケットの MSS 値を 1380 に変更します。その後、サーバは、1380 バイトのペイロードを含むパケットを送信します。ASA は、最大 120 バイトのヘッダーをパケットに追加しても、1500 バイトの MTU サイズに適応することができます。

TCP の最小 MSS も設定できます。ホストまたはサーバが非常に小さい TCP MSS を要求した場合、ASA は値を調整します。デフォルトでは、最小 TCP MSS は有効ではありません。

SSL VPN 接続用を含め、to-the-box トラフィックの場合、この設定は適用されません。ASA は MTU を使用して、TCP MSS を導き出します。MTU - 40(IPv4)または MTU - 60(IPv6)となります。

デフォルトでは TCP MSS は、ASA が IPv4 IPsec VPN エンドポイントとして機能し、MTU が 1500 バイトであることを前提としています。ASA が IPv4 IPsec VPN エンドポイントとして機能している場合は、最大 120 バイトの TCP および IP ヘッダーに対応する必要があります。

MTU 値を変更して、IPv6 を使用するか、または IPsec VPN エンドポイントとして ASA を使用しない場合は、TCP MSS 設定を変更する必要があります。次のガイドラインを参照してください。

- 通常のトラフィック:TCP MSS の制限を無効にし、接続のエンドポイント間で確立された値を受け入れます。通常、接続エンドポイントは MTU から TCP MSS を取得するため、非 IPsec パケットは通常この TCP MSS を満たしています。
- IPv4 IPsec エンドポイント トラフィック:最大 TCP MSS を MTU - 120 に設定します。たとえば、ジャンボ フレームを使用しており、MTU を 9000 に設定すると、新しい MTU を使用するために、TCP MSS を 8880 に設定する必要があります。
- IPv6 IPsec エンドポイント トラフィック:最大 TCP MSS を MTU - 140 に設定します。

例

下記の例では、ジャンボ フレームをイネーブルにし、すべてのインターフェイスの MTU を増加し、非 VPN トラフィックの TCP MSS をディセーブルにします(TCP MSS を 0 に設定、すなわち無制限とすることによって行います)。

```
ciscoasa(config)# jumbo frame-reservation
ciscoasa(config)# mtu inside 9198
ciscoasa(config)# mtu outside 9198
ciscoasa(config)# sysopt connection tcpmss 0
```

下記の例では、ジャンボ フレームをイネーブルにし、すべてのインターフェイスの MTU を増加し、VPN トラフィックの TCP MSS を 9078 に変更します(MTU から 120 を差し引きます)。

```
ciscoasa(config)# jumbo frame-reservation
ciscoasa(config)# mtu inside 9198
ciscoasa(config)# mtu outside 9198
ciscoasa(config)# sysopt connection tcpmss 9078
```

関連コマンド

コマンド	説明
clear configure sysopt	**sysopt** コマンド コンフィギュレーションをクリアします。
show running-config sysopt	**sysopt** コマンド コンフィギュレーションを表示します。
sysopt connection permit-ipsec	ACL でインターフェイスをチェックせずに IPsec トンネルからのすべてのパケットを許可します。
sysopt connection timewait	最後の標準 TCP クローズダウン シーケンスの後、各 TCP 接続が短縮 TIME_WAIT 状態を保持するようにします。

sysopt connection timewait

各 TCP 接続において、最後の通常の TCP クローズ ダウン シーケンスの後に、少なくとも 15 秒の短い TIME_WAIT 状態が強制的に維持されるようにするには、グローバル コンフィギュレーション モードで **sysopt connection timewait** コマンドを使用します。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。エンド ホスト アプリケーションのデフォルト TCP 終了シーケンスが同時クローズである場合に、この機能を使用することを推奨します。

sysopt connection timewait

no sysopt connection timewait

(注) FIN_WAIT2 状態で受信した RST パケット（通常の TCP クローズダウン シーケンスではなく）は、15 秒の遅延もトリガーします。ASA では、接続の最後のパケット（FIN/ACK または RST）を受信した後、接続を 15 秒間保持します。

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

この機能はデフォルトで無効に設定されています。

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	• 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

ASA のデフォルトの動作では、シャットダウン シーケンスが追跡され、2 つの FIN と最後の FIN セグメントの ACK の後で接続が解放されます。この即時解放ヒューリスティックにより、ASA では、標準クローズ シーケンスと呼ばれる最も一般的なクロージング シーケンスに基づいて、高い接続レートを維持できます。ただし、一方の端が閉じ、もう一方の端が確認応答してから独自のクロージング シーケンスを開始する標準クローズ シーケンスとは異なり、同時クローズでは、トランザクションの両端がクロージング シーケンスを開始します（RFC 793 を参照）。したがって、同時クローズでは、即時解放によって接続の一方の側で CLOSING 状態が保持されます。多くのソケットを CLOSING 状態にすると、エンド ホストのパフォーマンスが低下する可能性があります。たとえば、一部の WinSock メインフレーム クライアントはこの動作を示し、メインフレーム サーバのパフォーマンスを低下させることが知られています。**sysopt connection timewait** コマンドを使用すると、同時クローズ ダウン シーケンスが完了するためのウィンドウが作成されます。

例

次に、timewait 機能をイネーブルにする例を示します。

```
ciscoasa(config)# sysopt connection timewait
```

関連コマンド

コマンド	説明
clear configure sysopt	**sysopt** コマンド コンフィギュレーションをクリアします。
show running-config sysopt	**sysopt** コマンド コンフィギュレーションを表示します。
sysopt connection permit-ipsec	ACL でインターフェイスをチェックせずに IPsec トンネルからのすべてのパケットを許可します。
sysopt connection tcpmss	TCP セグメントの最大サイズを上書きします。または、確実に最大サイズが指定したサイズよりも小さくならないようにします。

sysopt noproxyarp

インターフェイスで NAT グローバル アドレスまたは VPN クライアント アドレスに対するプロキシ ARP 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 **sysopt noproxyarp** コマンドを使用します。プロキシ ARP を再度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。

sysopt noproxyarp *interface_name*

no sysopt noproxyarp *interface_name*

構文の説明

interface_name	プロキシ ARP をディセーブルにするインターフェイス名。

デフォルト

プロキシ ARP は、デフォルトでイネーブルに設定されています。

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	• Yes	• Yes	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
8.0(3)	このコマンドは、VPN クライアント アドレスが内部ネットワークと重複するときに、VPN プロキシ ARP に影響を及ぼすように拡張されました。

使用上のガイドライン

既存のネットワークと重なる VPN クライアント アドレス プールがある場合、ASA は、デフォルトにより、すべてのインターフェイス上でプロキシ ARP を送信します。同じレイヤ 2 ドメイン上にもう 1 つインターフェイスがあると、そのインターフェイスは ARP 要求を検出し、自分の MAC アドレスで応答します。その結果、内部ホストへの VPN クライアントのリターン トラフィックは、その誤ったインターフェイスに送信され、破棄されます。この場合、プロキシ ARP が不要なインターフェイスに対して **sysopt noproxyarp** コマンドを入力する必要があります。

まれに、NAT グローバル アドレスに対してプロキシ ARP をディセーブルにする場合があります。

ホストによって IP トラフィックが同じイーサネット ネットワーク上の別のデバイスに送信される場合、ホストではそのデバイスの MAC アドレスを知る必要があります。ARP は、IP アドレスを MAC アドレスに解決するレイヤ 2 プロトコルです。ホストは IP アドレスの所有者を尋ねる ARP 要求を送信します。その IP アドレスを所有するデバイスは、自分が所有者であることを自分の MAC アドレスで返答します。

プロキシ ARP は、デバイスが IP アドレスを所有していなくても、その固有の MAC アドレスで ARP 要求に応答する場合に使用します。NAT を設定し、ASA のインターフェイスと同じネットワーク上にあるグローバル アドレスを指定すると、ASA によってプロキシ ARP が使用されます。トラフィックがホストにアクセスできる唯一の方法は、ASA でプロキシ ARP が使用されている場合、ASA の MAC アドレスが宛先グローバル アドレスに割り当てられていると主張することです。

例

次に、内部インターフェイスでプロキシ ARP をディセーブルにする例を示します。

```
ciscoasa(config)# sysopt noproxyarp inside
```

関連コマンド

コマンド	説明
alias	外部アドレスを変換し、変換に合わせて DNS レコードを変更します。
clear configure sysopt	**sysopt** コマンド コンフィギュレーションをクリアします。
show running-config sysopt	**sysopt** コマンド コンフィギュレーションを表示します。
sysopt nodnsalias	**alias** コマンドを使用するときに、DNS A レコード アドレスの変更をディセーブルにします。

sysopt radius ignore-secret

RADIUS アカウンティング応答内の認証キーを無視するには、グローバル コンフィギュレーション モードで **sysopt radius ignore-secret** コマンドを使用します。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。一部の RADIUS サーバとの互換性のために、このキーを無視する必要がある場合があります。

sysopt radius ignore-secret

no sysopt radius ignore-secret

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

この機能はデフォルトで無効に設定されています。

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。

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	• 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

一部の RADIUS サーバでは、アカウンティング確認応答内のオーセンティケータ ハッシュにこのキーが含まれていません。この使用上の注意により、ASA でアカウンティング要求を継続的に再送信する場合があります。**sysopt radius ignore-secret** コマンドを使用して、これらの確認応答内のキーを無視し、再送信の問題を回避します（ここで示すキーは、**aaa-server host** コマンドで設定するものと同じです）。

例

次に、アカウンティング応答内の認証キーを無視する例を示します。

```
ciscoasa(config)# sysopt radius ignore-secret
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバを指定します。
clear configure sysopt	**sysopt** コマンド コンフィギュレーションをクリアします。
show running-config sysopt	**sysopt** コマンド コンフィギュレーションを表示します。

sysopt traffic detailed-statistics

変更されたトラフィック システム オプションについて秒単位でプロトコルごとの詳細な統計情報を計算するには、グローバル コンフィギュレーション モードで **sysopt traffic detailed-statistics** コマンドを使用します。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。

sysopt traffic detailed-statistics

no sysopt traffic detailed-statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

この機能はデフォルトで無効に設定されています。

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	• 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

sysopt traffic detailed-statistics コマンドを使用して、変更されたトラフィック システム オプションについて秒単位でプロトコルごとに詳細な統計情報を計算できます。

例

次に、変更されたトラフィック システム オプションの詳細な統計情報を表示する例を示します。

```
ciscoasa(config)# sysopt traffic detailed-statistics
```

関連コマンド

コマンド	説明
clear configure sysopt	**sysopt** コマンド コンフィギュレーションをクリアします。
show running-config sysopt	**sysopt** コマンド コンフィギュレーションを表示します。