ar - az

area

OSPFv2 エリアまたは OSPFv3 エリアを作成するには、ルータ コンフィギュレーション モードで **area** コマンドを使用します。エリアを削除するには、このコマンドの **no** 形式を使用します。

area *area_id*
no area *area_id*

構文の説明

area_id	作成するエリアの ID。10 進数または IP アドレスのいずれかを使用して ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	—	—
IPv6 ルータ 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。
9.0(1)	OSPFv3 のサポートが追加されました。

使用上のガイドライン

作成したエリアには、パラメータが設定されていません。関連する **area** コマンドを使用してエリアパラメータを設定します。

例

次に、エリア ID が 1 の OSPF エリアを作成する例を示します。

```
ciscoasa(config-router)# area 1
ciscoasa(config-router)#
```

関連コマンド

コマンド	説明
area nssa	（任意）エリアを Not-So-Stubby Area として定義します。
area stub	エリアをスタブ エリアとして定義します。
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 running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

area authentication

OSPFv2エリアの認証をイネーブルにするには、ルータ コンフィギュレーション モードで**area authentication** コマンドを使用します。エリア認証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。

area *area_id* **authentication** [**message-digest**]
no area *area_id* **authentication** [**message-digest**]

構文の説明

area_id	認証をイネーブルにするエリアの ID。10 進数または IP アドレスのいずれかを使用して ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。
message-digest	（オプション）*area_id* で指定したエリアに対する Message Digest 5（MD5）認証をイネーブルにします。

コマンド デフォルト

エリア認証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。

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
ルータ 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。
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

指定した OSPFv2 エリアが存在しない場合は、このコマンドを入力すると作成されます。**message-digest** キーワードを指定せずに **area authentication** コマンドを入力した場合は、簡易パスワード認証がイネーブルになります。**message-digest** キーワードを指定すると、MD5 認証がイネーブルになります。

例

次に、エリア 1 に対して MD5 認証をイネーブルにする例を示します。

```
ciscoasa(config-router)# area 1 authentication message-digest
ciscoasa(config-router)#
```

関連コマンド

コマンド	説明
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 running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

area default-cost

スタブまたはNSSAに送信されるデフォルト集約ルートのコストを指定するには、ルータ コンフィギュレーション モードまたはIPv6ルータ コンフィギュレーション モードで **area default-cost** コマンドを使用します。デフォルトのコスト値に戻すには、このコマンドの **no** 形式を使用します。

area *area_id* **default-cost** *cost*
no area *area_id* **default-cost** *cost*

構文の説明

area_id	デフォルト コストを変更するスタブまたはNSSAのID。10進数またはIPアドレスのいずれかを使用してIDを指定できます。有効な10進値の範囲は、0 ～ 4294967295です。
cost	スタブまたはNSSAに使用されるデフォルト集約ルートのコストを指定します。有効な値の範囲は、0 ～ 65535です。

コマンド デフォルト

cost のデフォルト値は1です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—
IPv6ルータ 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。
9.0(1)	マルチ コンテキスト モードおよびOSPFv3がサポートされています。

使用上のガイドライン

指定したエリアが **area** コマンドを使用して過去に定義されていない場合は、指定したパラメータでこのコマンドがエリアを作成します。

例

次に、スタブまたはNSSAに送信される集約ルートのデフォルトコストを指定する例を示します。

```
ciscoasa(config-router)# area 1 default-cost 5
ciscoasa(config-router)#
```

関連コマンド

コマンド	説明
area nssa	（任意）エリアを Not-So-Stubby Area として定義します。
area stub	エリアをスタブ エリアとして定義します。
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 running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

area filter-list prefix

ABR の OSPFv2 エリア間のタイプ 3 LSA でアドバタイズされたプレフィックスをフィルタリングするには、ルータ コンフィギュレーション モードで **area filter-list prefix** コマンドを使用します。フィルタを変更またはキャンセルするには、このコマンドの **no** 形式を使用します。

area *area_id* **filter-list prefix** *list_name* { **in** | **out** }
no area *area_id* **filter-list prefix** *list_name* { **in** | **out** }

構文の説明

area_id	フィルタリングを設定するエリアを識別します。10進数またはIPアドレスのいずれかを使用して ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。
in	指定したエリアに着信するアドバタイズされたプレフィックスに、設定済みプレフィックス リストを適用します。
list_name	プレフィックス リストの名前を指定します。
out	指定したエリアから発信されるアドバタイズされたプレフィックスに、設定済みプレフィックス リストを適用します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

指定したエリアが **area** コマンドを使用して過去に定義されていない場合は、指定したパラメータでこのコマンドがエリアを作成します。

フィルタリングできるのはタイプ 3 LSA だけです。プライベート ネットワークに ASBR が設定されている場合、ASBR はプライベート ネットワークを記述するタイプ 5 LSA を送信します。この LSA は、パブリック エリアを含む AS 全体にフラッディングされます。

例

次に、他のすべてのエリアからエリア 1 に送信されるプレフィックスをフィルタリングする例を示します。

```
ciscoasa(config-router)# area 1 filter-list prefix-list AREA_1 in
ciscoasa(config-router)#
```

関連コマンド

コマンド	説明
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 running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

area nssa

エリアを NSSA として設定するには、ルータ コンフィギュレーション モードまたは IPv6 ルータ コンフィギュレーション モードで **area nssa** コマンドを使用します。NSSA 指定をエリアから削除するには、このコマンドの **no** 形式を使用します。

area *area_id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric-type** { **1** | **2** }] [**metric** *value*]] [**no-summary**]
no area *area_id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric-type** { **1** | **2** }] [**metric** *value*]] [**no-summary**]

構文の説明

area_id	NSSA として指定するエリアを識別します。10 進数または IP アドレスのいずれかを使用して ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。
default-information-originate	NSSA エリアでのタイプ 7 デフォルトの生成に使用します。このキーワードは、NSSA ABR または NSSA ASBR でのみ有効です。
metric *metric_value*	（任意）OSPF デフォルト メトリック値を指定します。有効値の範囲は 0 ～ 16777214 です。
metric-type {**1** | **2**}	（任意）デフォルト ルートの OSPF メトリック タイプ。有効な値は次のとおりです。 • **1**：タイプ 1 • **2**：タイプ 2。 デフォルト値は 2 です。
no-redistribution	（任意）ルータが NSSA ABR の場合、**redistribute** コマンドを使用して、ルートを NSSA エリアでなく通常のエリアにのみ取り込む場合に使用します。
no-summary	（任意）エリアを Not-So-Stubby Area（NSSA）とし、集約ルートが挿入されないようにします。

コマンド デフォルト

デフォルトの設定は次のとおりです。

- NSSA エリアは未定義です。
- **metric-type** は 2 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—
IPv6 ルータ 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。
9.0(1)	マルチ コンテキスト モードおよびOSPFv3 がサポートされています。

使用上のガイドライン

指定したエリアが**area**コマンドを使用して過去に定義されていない場合は、指定したパラメータでこのコマンドがエリアを作成します。

エリアに1つのオプションを設定し、後で別のオプションを指定した場合、両方のオプションが設定されます。たとえば、次の2のコマンドを別々に入力した場合、コンフィギュレーションには、両方のオプションを指定した 1 つのコマンドが設定されます。

```
ciscoasa(config-rtr)# area 1 nssa no-redistribution
ciscoasa(config-rtr)# area area_id nssa default-information-originate
```

例

次に、2つのオプションを別々に設定すると、1つのコマンドがコンフィギュレーションに設定される例を示します。

```
ciscoasa(config-rtr)# area 1 nssa no-redistribution
ciscoasa(config-rtr)# area 1 nssa default-information-originate
ciscoasa(config-rtr)# exit
ciscoasa(config-rtr)# show running-config router ospf 1
router ospf 1
 area 1 nssa no-redistribution default-information-originate
```

関連コマンド

コマンド	説明
area stub	エリアをスタブ エリアとして定義します。
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。

コマンド	説明
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

area-password

IS-IS エリア認証パスワードを設定するには、ルータ ISIS コンフィギュレーション モードで、**area-password** コマンドを使用します。パスワード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。

area-password *password* ［ **authenticate snp** { **validate** | **send-only** } ］
no area password ［ *password* ］

構文の説明

password	割り当てるパスワード。
authenticate snp	（任意）これを指定すると、システムはシーケンス番号 PDUS（SNP）にパスワードを挿入するようになります。
validate	これを指定すると、システムはパスワードを SNP に挿入し、受け取ったパスワードを SNP で確認するようになります。
send-only	これを指定すると、システムは SNP へのパスワードの挿入だけは行うようになりますが、SNP での受け取ったパスワードの確認は行われません。このキーワードは、ソフトウェアのアップグレード中、移行をスムーズに行うために使用します。

コマンド デフォルト

エリア パスワードは定義されていません。また、エリア パスワードの認証はディセ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。

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
ルータ isis 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
9.6(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

あるエリアに存在するすべてのルータで **area-password** コマンドを使用することにより、不正ルータによる、リンクステートデータベースへの誤ったルーティング情報の挿入を阻止できます。

このパスワードはプレーンテキストとしてやり取りされるため、この機能が提供するセキュリティは限定されています。

このパスワードは、レベル 1（ステーション ルータ レベル）の PDU リンクステート パケット（LSP）、Complete Sequence Number PDU（CSNP）、および Partial Sequence Number PDU（PSNP）に挿入されます。

authenticate snp キーワードを **validate** キーワードまたは **send-only** キーワードのいずれかと共に指定しない場合、IS-IS プロトコルはパスワードを SNP に挿入しません。

例

次に、エリア認証パスワードを割り当て、このパスワードを SNP に挿入し、システムが受け取った SNP で確認するように指定する例を示します。

```
ciscoasa(config-router)# router isis
ciscoasa(config-router)# area-password track authenticate snp validate
```

関連コマンド

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

コマンド	説明
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。

コマンド	説明
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更（アップまたはダウン）する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト（TLV）を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。

コマンド	説明
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

area range（IPv6 ルータ OSPF）

エリア境界で OSPFv3 ルートを統合および集約するには、IPv6 ルータ OSPF コンフィギュレーション モードで **area range** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

area *area_id ipv6-prefix-/prefix-length* [**advertise** | **not advertise**] [**cost** *cost*]
no area *area_id ipv6-prefix-/prefix-length* [**advertise** | **not advertise**] [**cost** *cost*]

構文の説明

advertise	（オプション）Type 3 サマリー LSA をアドバタイズおよび生成するように、範囲ステータスを設定します。
area_id	ルートを要約するエリアの ID を指定します。10 進数または IPv6 プレフィックスのいずれかを使用して ID を指定できます。
cost *cost*	（オプション）このサマリー ルートのメトリックまたはコストを指定します。宛先への最短パスを決定するための OSPF SPF 計算で使用します。有効値の範囲は 0 ～ 16777215 です。
ipv6-prefix	IPv6 プレフィックスを指定します。
not-advertise	（オプション）範囲ステータスを DoNotAdvertise に設定します。Type 3 サマリー LSA は抑制され、コンポーネント ネットワークは他のネットワークから隠された状態のままです。
prefix-length	IPv6 プレフィックス長を指定します。

コマンド デフォルト

範囲ステータスはデフォルトで advertise 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。

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
IPv6 ルータ OSPF 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
9.0(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

指定したエリアが **area** コマンドを使用して過去に定義されていない場合は、指定したパラメータでこのコマンドがエリアを作成します。

area range コマンドは、ABR でのみ使用されます。このコマンドによって、エリアのルートが統合または集約されます。その結果、1 つの集約ルートが ABR によって他のエリアにアドバタイズされます。ルーティング情報は、エリア境界でまとめられます。エリアの外部では、IPv6 プレフィックスおよびプレフィックス長ごとに 1 つのルートがアドバタイズされます。この動作はルート集約と呼ばれます。1 つのエリアに複数の **area range** コマンドを設定できます。このように、OSPFv3 は多くの異なる IPv6 プレフィックスおよびプレフィックス長セットのルートを集約できます。

例

次に、IPv6 プレフィックスが 2000:0:0:4::2 でプレフィックス長が 2001::/64 の他のエリアに ABR によってアドバタイズされる 1 つの集約ルートを指定する例を示します。

```
ciscoasa(config-router)# area 1 range
2000:0:0:4::2/2001::/64

ciscoasa(config-router)#
```

関連コマンド

コマンド	説明
ipv6 router ospf	OSPFv3 の IPv6 ルータ コンフィギュレーション モードを開始します。
show running-config ipv6 router	グローバル ルータ コンフィギュレーションの IPv6 コマンドを表示します。

area range（ルータ OSPF）

エリア境界でルートを統合および集約するには、OSPF ルータ コンフィギュレーション モードで **area range** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

area *area_id* **range** *address mask* **advertise** | **not-advertise**]
no area *area_id* **range** *address mask* **advertise** | **not-advertise**]

構文の説明

address	サブネット範囲の IP アドレス。
advertise	（任意）Type 3 サマリー LSA をアドバタイズおよび生成するように、アドレス範囲ステータスを設定します。
area_id	範囲を設定するエリアを識別します。10 進数または IP アドレスのいずれかを使用して ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。
mask	IP アドレスのサブネット マスク。
not-advertise	（任意）アドレス範囲ステータスを DoNotAdvertise に設定します。Type 3 サマリー LSA は抑制され、コンポーネント ネットワークは他のネットワークから隠された状態のままです。

コマンド デフォルト

アドレス範囲ステータスは advertise 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。

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
IPv6 ルータ OSPF 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。
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

指定したエリアが **area** コマンドを使用して過去に定義されていない場合は、指定したパラメータでこのコマンドがエリアを作成します。

area range コマンドは、エリアのルートを統合または集約するために ABR でのみ使用します。その結果、1 つの集約ルートが ABR によって他のエリアにアドバタイズされます。ルーティング情報は、エリア境界でまとめられます。エリアの外部では、アドレス範囲ごとに 1 つのルートがアドバタイズされます。この動作はルート集約と呼ばれます。1 つのエリアに複数の **area range** コマンドを設定できます。このように、OSPF は多くの異なるアドレス範囲セットのアドレスを集約できます。

no area *area_id* **range** *ip_address netmask* **not-advertise** コマンドは、**not-advertise** オプションキーワードのみを削除します。

例

次に、ネットワーク 10.0.0.0 上のすべてのサブネットおよびネットワーク 192.168.110.0 上のすべてのホストに対する 1 つの集約ルートを、ABR によって他のエリアにアドバタイズするように指定する例を示します。

```
ciscoasa(config-router)# area 10.0.0.0 range 10.0.0.0 255.0.0.0
ciscoasa(config-router)# area 0 range 192.168.110.0 255.255.255.0
ciscoasa(config-router)#
```

関連コマンド

コマンド	説明
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 running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

area stub

エリアをスタブエリアとして定義するには、ルータ コンフィギュレーション モードまたはIPv6 ルータ コンフィギュレーション モードで **area stub** コマンドを使用します。スタブエリアを削除するには、このコマンドの **no** 形式を使用します。

area *area_id* **stub** [**no-summary**]
no area *area_id* **stub** [**no-summary**]

構文の説明

area_id	スタブ エリアを識別します。10 進数またはIP アドレスのいずれかを使用して ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。
no-summary	ABR がサマリー リンク アドバタイズメントをスタブ エリアに送信しないようにします。

コマンド デフォルト

デフォルトの動作は次のとおりです。

- スタブ エリアは定義されません。
- サマリー リンク アドバタイズメントはスタブ エリアに送信されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	—	—
IPv6 ルータ 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。
9.0(1)	OSPFv3 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、スタブまたは NSSA に接続された ABR でのみ使用されます。

スタブ エリア ルータ コンフィギュレーション コマンドには、area stub および area default-cost という2つのコマンドがあります。スタブエリアに接続されているすべてのルータおよびアクセスサーバーで、**area stub** コマンドを使用して、エリアをスタブエリアとして設定する必要があります。スタブエリアに接続された ABR でのみ **area default-cost** コマンドを使用します。**area default-cost** コマンドは、ABR によってスタブエリアに生成されるサマリーデフォルトルートのメトリックを提供します。

例

次に、指定したエリアをスタブ エリアとして設定する例を示します。

```
ciscoasa(config-rtr)# area 1 stub
ciscoasa(config-rtr)#
```

関連コマンド

コマンド	説明
area default-cost	スタブまたは NSSA に送信されるデフォルト サマリー ルートのコストを指定します。
area nssa	（任意）エリアを Not-So-Stubby Area として定義します。
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 running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

area virtual-link（IPv6 ルータ OSPF）

OSPFv3 仮想リンクを定義するには、ルータ OSPF コンフィギュレーション モードで **area virtual-link** コマンドを使用します。オプションをリセットするか、または仮想リンクを削除するには、このコマンドの **no** 形式を使用します。

area *area_id* **virtual-link** *router_id* ［ **hello-interval** *seconds* ］［ **retransmit-interval** *seconds* ］［ **transmit-delay** *seconds* ］［ **dead-interval** *seconds* ］［ **ttl-security hops** *hop-count* ］
no area *area_id* **virtual-link** *router_id* ［ **hello-interval** *seconds* ］［ **retransmit-interval** *seconds* ］［ **transmit-delay** *seconds* ］［ **dead-interval** *seconds* ］［ **ttl-security hops** *hop-count* ］

構文の説明

area_id	仮想リンクの中継エリアのエリア ID を指定します。10 進数または有効な IPv6 プレフィックスのいずれかを使用して ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。
hello-interval *seconds*	（オプション）ASA がインターフェイスで送信する hello パケットの間隔を秒単位で指定します。hello 間隔は、hello パケットでアドバタイズされる符号なし整数値です。この値は、共通のネットワークに接続されているすべてのルータおよびアクセス サーバーで同じであることが必要です。有効な値の範囲は、1 ～ 8192 秒です。
retransmit-interval *seconds*	（オプション）インターフェイスに属する隣接ルータの LSA 再送信間の時間を秒単位で指定します。再送信間隔は、接続されているネットワーク上の任意の 2 台のルータ間の予想されるラウンドトリップ遅延です。この値は、予想されるラウンドトリップ遅延よりも大きいことが必要です。有効な値の範囲は、1 ～ 8192 秒です。
router_id	仮想リンク ネイバーに関連付けられているルータ ID を指定します。ルータ ID は **show ipv6 ospf** または **show ipv6 display** コマンドで表示されます。
transmit-delay *seconds*	（オプション）インターフェイス上でリンクステート アップデート パケットを送信するために必要な推定される時間を秒単位で指定します。ゼロよりも大きい整数値を指定します。アップデート パケット内の LSA の経過時間は、転送前にこの値の分だけ増分されます。有効な値の範囲は、1 ～ 8192 秒です。
dead-interval *seconds*	（オプション）hello パケットがどれだけの時間（秒単位）届かなかった場合にネイバーがルータのダウンを示すかを指定します。デッドインターバルは符号なし整数値です。hello 間隔と同様に、この値は、共通のネットワークに接続されているすべてのルータとアクセス サーバーで同じでなければなりません。有効な値の範囲は、1 ～ 8192 秒です。
ttl-security hops *hop-count*	（オプション）仮想リンク上で存続可能時間（TTL）セキュリティを設定します。ホップ カウントの有効な値の範囲は 1 ～ 254 です。

（注） 1 桁のパスワードおよび先頭の数字の後に空白が続くパスワードはサポートされなくなりました。

コマンド デフォルト

デフォルトの設定は次のとおりです。

- *area_id*：エリア ID は事前に定義されていません。
- *router_id*：ルータ ID は事前に定義されていません。
- **hello-interval**：10 秒。
- **retransmit-interval**：5 秒。
- **transmit-delay**：1秒。
- **dead-interval**：40 秒。

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
IPv6 ルータ OSPF コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(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

OSPFv3 では、すべてのエリアはバックボーン エリアに接続している必要があります。バックボーンへの接続が失われた場合は、仮想リンクを確立して修復できます。

hello パケットの間隔が短い場合、トポロジ変化の検出が速くなりますが、ルーティング トラフィックが多くなります。

再送信間隔の設定値はあまり小さくしないでください。小さくすると、不要な再送信が行われます。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。

送信遅延の値では、インターフェイスの送信遅延と伝搬遅延を考慮に入れる必要があります。

（注） 仮想リンクを正しく設定するには、各仮想リンク ネイバーに、中継エリア ID および対応する仮想リンク隣接ルータ ID が含まれている必要があります。ルータ ID を取得するには、**show ipv6 ospf** コマンドを使用します。

例

次に、OSPFv3 で仮想リンクを確立する例を示します。

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-rtr)# log-adjacency-changes
ciscoasa(config-rtr)# area 1 virtual-link 192.168.255.1 hello interval 5
```

area virtual-link（ルータ OSPF）

OSPF 仮想リンクを定義するには、ルータ OSPF コンフィギュレーション モードで **area virtual-link** コマンドを使用します。オプションをリセットするか、または仮想リンクを削除するには、このコマンドの **no** 形式を使用します。

area *area_id* **virtual-link** *router_id* [**authentication** [**key-chain** *key-chain-name* | **message-digest** | **null**]] [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**dead-interval** *seconds* [[[[**authentication-key[0|8]** *key*] | [**message-digest-key** *key_id* **md5[0|8]** *key*]]]]
no area *area_id* **virtual-link** *router_id* [**authentication** [**key-chain** *key-chain-name* | **message-digest** | **null**]] [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**dead-interval** *seconds* [[[[**authentication-key[0|8]** *key*] | [**message-digest-key** *key_id* **md5[0|8]** *key*]]]]

構文の説明

area_id	仮想リンクの中継エリアのエリア ID。10 進数または IP アドレスのいずれかを使用して ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。
authentication	（任意）認証タイプを指定します。
key-chain *key-chain-name*	（任意）認証に使用するキーチェーンを指定します。key-name引数には最大 63 文字の英数字を指定できます。
authentication-key [0 | 8]*key*	（任意）ネイバー ルーティング デバイスで使用する OSPF 認証パスワードを指定します。
dead-interval *seconds*	（任意）helloパケットを受信しない場合に、ネイバー ルーティング デバイスがダウンしたことを宣言するまでの間隔を指定します。有効な値は、1 ～ 65535 秒です。
hello-interval *seconds*	（任意）インターフェイスで送信されるhelloパケット間の間隔を指定します。有効な値は、1 ～ 65535 秒です。
md5 [0 | 8] *key*	（任意）最大 16 バイトの英数字のキーを指定します。
message-digest	（任意）メッセージ ダイジェスト認証を使用することを指定します。
message-digest-key *key_id*	（任意）Message Digest 5（MD5）認証をイネーブルにし、認証キー ID 番号を指定します。有効な値は、1 ～ 255 です。
0	暗号化されていないパスワードが続くことを指定します。
8	暗号化されたパスワードが後に続くことを指定します。
null	（任意）認証を使用しないことを指定します。パスワードまたはメッセージ ダイジェスト認証は、OSPF エリアに設定されている場合、上書きされます。

retransmit-interval *seconds*	（任意）インターフェイスに属している隣接ルータのLSA再送信の間隔を指定します。有効な値は、1 ～ 65535 秒です。
router_id	仮想リンク ネイバーに関連付けられているルータ ID。ルータ ID は、各ルータによって内部でインターフェイスIPアドレスから生成されます。この値は、IP アドレスの形式で入力する必要があります。デフォルトはありません。
transmit-delay *seconds*	（任意）OSPF がトポロジ変更を受信してから、Shortest Path First（SPF）計算を開始するまでの遅延時間を 0 ～ 65535 秒で指定します。デフォルトは 5 秒です。

（注） 1桁のパスワードおよび先頭の数字の後に空白が続くパスワードはサポートされなくなりました。

コマンド デフォルト

デフォルトの設定は次のとおりです。

- *area_id*：エリア ID は事前に定義されていません。
- *router_id*：ルータ ID は事前に定義されていません。
- **hello-interval** *seconds*：10 秒。
- **retransmit-interval** *seconds*：5 秒。
- **transmit-delay** *seconds*：1 秒。
- **dead-interval** *seconds*：40 秒。
- **authentication-key [0 | 8]** *key*：キーは事前定義されていません。
- **message-digest-key** *key_id* **md5 [0 | 8]** *key*：キーは事前定義されていません。

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。

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
ルータ OSPF 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。
9.12(1)	OSPF 認証のローテーション キーをサポートするためにキー チェーン機能が追加されました。

使用上のガイドライン

OSPF では、すべてのエリアがバックボーン エリアに接続されている必要があります。バックボーンへの接続が失われた場合は、仮想リンクを確立して修復できます。

hello 間隔を小さくすればするほど、トポロジ変更の検出が速くなりますが、ルーティング トラフィックが増加します。

再送信間隔の設定値はあまり小さくしないでください。小さくすると、不要な再送信が行われます。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。

送信遅延の値では、インターフェイスの送信遅延と伝搬遅延を考慮に入れる必要があります。

指定した認証キーは、**area** *area_id* **authentication** コマンドでバックボーンに対して認証がイネーブルにされている場合にのみ使用されます。

簡易テキスト認証と MD5 認証という 2 つの認証方式は、相互排他的です。どちらか一方を指定するか、または両方とも指定しないでください。**authentication-key [0 | 8]** *key* または **message-digest-key** *key_id* **md5[0 | 8]** *key* の後に指定したキーワードと引数は、すべて無視されます。したがって、オプションの引数は、これらのキーワードと引数の組み合わせの前に指定します。

インターフェイスに認証タイプが指定されていない場合、インターフェイスでは、エリアに指定されている認証タイプが使用されます。エリアに認証タイプが指定されていない場合、エリアのデフォルトはヌル認証です。

（注） 仮想リンクを正しく設定するには、各仮想リンク ネイバーに、中継エリア ID および対応する仮想リンク ネイバー ルータ ID が含まれている必要があります。ルータ ID を表示するには、**show ospf** コマンドを使用します。

例

次に、MD5 認証の仮想リンクを確立する例を示します。

```
ciscoasa(config-rtr)# area 10.0.0.0 virtual-link 10.3.4.5 message-digest-key 3 md5 8
sa5721bk47
```

次に、ローテーション キー認証で仮想リンクを確立する例を示します。

```
ciscoasa(config-rtr)# area 10.0.0.0 virtual-link 10.3.4.5 authentication key-chain
CHAIN-RTR-OSPFKEY
```

関連コマンド

コマンド	説明
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	OSPF ルーティング プロセスに関する一般情報を表示します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

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。
show ipv6 ospf	OSPFv3 ルーティング プロセスに関する一般情報を表示します。
show running-config ipv6 router	グローバル ルータ コンフィギュレーションの IPv6 コマンドを表示します。

arp

スタティック ARP エントリを ARP テーブルに追加するには、グローバル コンフィギュレーションモードで**arp** コマンドを使用します。スタティックエントリを削除するには、このコマンドの **no** 形式を使用します。

arp *interface_name ip_address mac_address* [**alias**]
no arp *interface_name ip_address mac_address*

構文の説明

alias	（任意）このマッピングに対してプロキシ ARP をイネーブルにします。ASA は、指定された IP アドレスの ARP 要求を受信すると、ASA MAC アドレスで応答します。その IP アドレスを持つホスト宛てのトラフィックを ASA が受信すると、ASA は、トラフィックをこのコマンドで指定されたホスト MAC アドレスに転送します。このキーワードは、ARP を実行しないデバイスがある場合などに役立ちます。 トランスペアレント ファイアウォール モードでは、このキーワードは無視されます。ASA はプロキシ ARP を実行しません。
interface_name	ホスト ネットワークに接続されているインターフェイス。
ip_address	ホストの IP アドレス。
mac_address	ホストの MAC アドレス。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ホストは IP アドレスでパケットの宛先を識別しますが、イーサネットにおける実際のパケット配信は、イーサネット MAC アドレスに依存します。ルータまたはホストは、直接接続され

たネットワークでパケットを配信する必要がある場合、IP アドレスに関連付けられた MAC アドレスを要求する ARP 要求を送信し、ARP 応答に従ってパケットを MAC アドレスに配信します。ホストまたはルータには ARP テーブルが保管されるため、配信が必要なパケットごとに ARP 要求を送信する必要はありません。ARP テーブルは、ARP 応答がネットワーク上で送信されるたびにダイナミックに更新されます。一定期間使用されなかったエントリは、タイムアウトします。エントリが正しくない場合（たとえば、所定の IP アドレスの MAC アドレスが変更された場合など）、エントリは更新される前にタイムアウトします。

スタティック ARP エントリは、MAC アドレスを IP アドレスにマッピングし、ホストに到達するまでに通過するインターフェイスを指定します。スタティック ARP エントリはタイムアウトせず、ネットワーク問題の解決に役立つ場合があります。トランスペアレント ファイアウォール モードでは、ARP インスペクションでスタティック ARP テーブルが使用されます（**arp-inspection** コマンドを参照）。

（注） トランスペアレント ファイアウォール モードでは、ダイナミック ARP エントリが ASA との間のトラフィック（管理トラフィックなど）に使用されます。

例

次に、外部インターフェイス上の 10.1.1.1 と MAC アドレス 0009.7cbe.2100 のスタティック ARP エントリを作成する例を示します。

```
ciscoasa(config)# arp outside 10.1.1.1 0009.7cbe.2100
```

関連コマンド

コマンド	説明
arp timeout	ASA が ARP テーブルを再構築するまでの時間を設定します。
arp-inspection	トランスペアレント ファイアウォール モードで、ARP パケットを調査し、ARP スプーフィングを防止します。
show arp	ARP テーブルを表示します。
show arp statistics	ARP 統計情報を表示します。
show running-config arp	ARP タイムアウトの現在のコンフィギュレーションを表示します。

arp-inspection

トランスペアレント ファイアウォール モードでの ARP インスペクションをイネーブルにするには、グローバル コンフィギュレーション モードで **arp-inspection** コマンドを使用します。ARP インスペクション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。

arp-inspection *interface_name* **enable** [**flood** | **no-flood**]
no arp-inspection *interface_name* **enable**

構文の説明

enable	ARP インスペクションをイネーブルにします。
flood	（デフォルト）スタティック ARP エントリのどの要素とも一致しないパケットをすべてのインターフェイス（発信元インターフェイスを除く）にフラッディングすることを指定します。MAC アドレス、IP アドレス、またはインターフェイス間で不一致がある場合、ASA はパケットをドロップします。 （注） 管理専用のインターフェイス（存在する場合）は、このパラメータが flood に設定されている場合でもパケットをフラッディングしません。
interface_name	ARP インスペクションをイネーブルにするブリッジ グループ メンバー インターフェイス。
no-flood	（任意）スタティック ARP エントリと正確には一致しないパケットをドロップすることを指定します。

コマンド デフォルト

デフォルトでは、ARP インスペクションはすべてのインターフェイスでディセーブルになっています。すべての ARP パケットは ASA を通過できます。ARP インスペクションをイネーブルにすると、一致しない ARP パケットはデフォルトでフラッディングされます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

リリース	変更内容
9.7(1)	Integrated Routing and Bridging（IRB; 統合ルーティングおよびブリッジング）を使用するときに、ルーテッド モードでこのコマンドを設定できるようになりました。

使用上のガイドライン

ARP インスペクションをイネーブルにする前に、**arp** コマンドを使用してスタティック ARP エントリを設定します。

ARP インスペクションでは、すべての ARP パケットをスタティック ARP エントリと照合し（**arp** コマンドを参照）、一致しないパケットをブロックします。この機能により、ARP スプーフィングが防止されます。

ARP インスペクションをイネーブルにすると、ASA は、すべての ARP パケット内の MAC アドレス、IP アドレス、および送信元インターフェイスを ARP テーブル内のスタティックエントリと比較し、次のアクションを実行します。

- IP アドレス、MAC アドレス、および送信元インターフェイスが ARP エントリと一致する場合、パケットを通過させます。
- MAC アドレス、IP アドレス、またはインターフェイス間で不一致がある場合、ASA はパケットをドロップします。
- ARP パケットがスタティック ARP テーブル内のどのエントリとも一致しない場合、パケットをすべてのインターフェイスに転送（フラッディング）するか、またはドロップするように ASA を設定できます。

（注） 専用の管理インターフェイス（存在する場合）は、このパラメータが flood に設定されている場合でもパケットをフラッディングしません。

ARP インスペクションによって、悪意のあるユーザが他のホストやルータになりすます（ARP スプーフィングと呼ばれる）のを防止できます。ARP スプーフィングが許可されていると、「中間者」攻撃を受けることがあります。たとえば、ホストが ARP 要求をゲートウェイルータに送信すると、ゲートウェイルータはゲートウェイルータの MAC アドレスで応答します。ただし、攻撃者は、ルータの MAC アドレスではなく攻撃者の MAC アドレスで別の ARP 応答をホストに送信します。これで、攻撃者は、すべてのホストトラフィックを代行受信してルータに転送できるようになります。

ARP インスペクションを使用すると、正しい MAC アドレスとそれに関連付けられた IP アドレスがスタティック ARP テーブル内にある場合、攻撃者は攻撃者の MAC アドレスで ARP 応答を送信できなくなります。

（注） トランスペアレント ファイアウォール モードでは、ダイナミック ARP エントリが ASA との間のトラフィック（管理トラフィックなど）に使用されます。

例

次に、外部インターフェイスにおけるARPインスペクションをイネーブルにし、スタティック ARP エントリに一致しない ARP パケットをドロップするように ASA を設定する例を示します。

```
ciscoasa(config)# arp outside 209.165.200.225 0009.7cbe.2100
ciscoasa(config)# arp-inspection outside enable no-flood
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
clear configure arp-inspection	ARP インスペクション コンフィギュレーションをクリアします。
firewall transparent	ファイアウォール モードをトランスペアレントに設定します。
show arp statistics	ARP 統計情報を表示します。
show running-config arp	ARP タイムアウトの現在のコンフィギュレーションを表示します。

arp permit-nonconnected

非直接接続サブネットも含まれるように ARP キャッシュをイネーブルにするには、グローバル コンフィギュレーション モードで **arp permit-nonconnected** コマンドを使用します。非直接接続サブネッ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。

arp permit-nonconnected
no arp permit-nonconnected

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

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。

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

コマンド履歴

リリース	変更内容
8.4(5)、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

ASA ARP キャッシュには、直接接続されたサブネットからのエントリだけがデフォルトで含まれています。**no arp permit-nonconnected** コマンドがあり（デフォルト動作）、受信した ARP パケットが接続されているインターフェイスとは別のサブネットに存在する場合は、ASA によって着信 ARP 要求も ARP 応答も拒否されます。

最初のケース（デフォルト動作）では、PAT が ASA で設定され、PAT の仮想 IP アドレス（マップ済み）が接続されているインターフェイスとは別のサブネットに存在する場合に障害が発生します。

また、セキュリティ リスクを認識していない場合は、この機能をイネーブルにすることは推奨しません。この機能は、ASA に対するサービス拒否（DoS）攻撃を助長する場合があります。任意のインターフェイスのユーザーが大量の ARP 応答を送信して、偽エントリで ASA ARP テーブルがあふれる可能性があります。

次の機能を使用する場合は、この機能を使用する必要がある可能性があります。

- セカンデリ サブネット。

- トラフィック転送の隣接ルートのプロキシ ARP。

例

次に、非接続サブネットをイネーブルにする例を示します。

```
ciscoasa(config)# arp permit non-connected
```

デフォルトの動作は、ASA の **debug arp** コマンドの出力で次のように確認できます。

着信 ARP 要求の場合：

```
- larp-in: request at outside from 10.10.2.1 0013.8083.0bb1 for 10.10.2.2 0000.0000.0000
 having smac 0013.8083.0bb1 dmac ffff.ffff.ffff\narp-in: Arp packet received from 10.10.2.1
 which is in different subnet than the connected interface 10.10.1.2/255.255.255.0
```

着信 ARP 応答の場合：

次に、非接続サブネットをイネーブルにする例を示します。

```
ciscoasa(config)# arp permit non-connected

- arp-in: response at outside from 10.10.2.1 0013.8083.0bb1 for 10.10.1.2 0016.4687.9f43
 having smac 0013.8083.0bb1 dmac 0016.4687.9f43\narp-in: Arp packet received from 10.10.2.1
 which is in different subnet than the connected interface 10.10.1.2/255.255.255.0
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。

arp rate-limit

ARP レート制限を設定して 1 秒あたりの ARP パケット数を制御するには、グローバル コンフィギュレーション モードで **arp rate-limit** 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** 形式を使用します。

arp rate-limit *seconds*
no arp rate-limit

構文の説明

seconds	秒数を 10 ～ 32768 の間で指定します。デフォルト値は ASA モデルによって異なります。

コマンド デフォルト

デフォルト値は ASA モデルによって異なります。

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。

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

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

この値は ARP ストーム攻撃を防ぐためにカスタマイズできます。

例

次に、ARP レートを 1 秒あたり 10000 に設定する例を示します。

```
ciscoasa(config)# arp rate-limit 10000
```

関連コマンド

コマンド	説明
show arp rate-limit	ARP レート制限を表示します。

arp timeout

ASA が ARP テーブルを再構築するまでの時間を設定するには、グローバル コンフィギュレーション モードで **arp timeout** コマンドを使用します。デフォルトのタイムアウトに戻すには、このコマンドの **no** 形式を使用します。

arp timeout *seconds*
no arp timeout *seconds*

構文の説明

seconds	ARP テーブルを再構築する間隔の秒数（60 ～ 4294967）。

コマンド デフォルト

デフォルト値は 14,400 秒（4 時間）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

ARP テーブルを再構築すると、自動的に新しいホスト情報が更新され、古いホスト情報が削除されます。ホスト情報は頻繁に変更されるため、タイムアウトを短くすることが必要になる場合があります。

例

次に、ARP タイムアウトを 5,000 秒に変更する例を示します。

```
ciscoasa(config)# arp timeout 5000
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
arp-inspection	トランスペアレント ファイアウォール モードで、ARP パケットを調査し、ARP スプーフィングを防止します。

コマンド	説明
show arp statistics	ARP 統計情報を表示します。
show running-config arp timeout	ARP タイムアウトの現在のコンフィギュレーションを表示します。

asdm disconnect

アクティブな ASDM セッションを終了するには、特権 EXEC モードで **asdm disconnect** コマンドを使用します。

asdm disconnect *session*

構文の説明

session 終了するアクティブな ASDM セッションのセッション ID。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**pdm disconnect** コマンドから **asdm disconnect** コマンドに変更されました。

使用上のガイドライン

アクティブな ASDM セッションとそれに関連付けられているセッション ID のリストを表示するには、**show asdm sessions** コマンドを使用します。特定のセッションを終了するには、**asdm disconnect** コマンドを使用します。

ASDM セッションを終了しても、残りのアクティブな ASDM セッションは、関連付けられているセッション ID を保持します。たとえば、3 つのアクティブな ASDM セッションがあり、それぞれのセッション ID が 0、1、および 2 の場合、セッション 1 を終了すると、残りのアクティブな ASDM セッションはそれぞれセッション ID 0 と 2 を保持します。この例で、次の新しい ASDM セッションにはセッション ID 1 が割り当てられ、その後の新しいセッションにはセッション ID 3 から順に ID が割り当てられます。

例

次に、セッション ID 0 の ASDM セッションを終了する例を示します。**asdm disconnect** コマンドの入力の前後に、**show asdm sessions** コマンドを使用して、アクティブな ASDM セッションを表示しています。

```
ciscoasa# show asdm sessions
0 192.168.1.1
1 192.168.1.2
```

```
ciscoasa# asdm disconnect 0
ciscoasa# show asdm sessions
1 192.168.1.2
```

関連コマンド

コマンド	説明
show asdm sessions	アクティブな ASDM セッションとそれに関連付けられているセッション ID のリストを表示します。

asdm disconnect log_session

アクティブなASDMロギングセッションを終了するには、特権EXECモードで**asdm disconnect log_session**コマンドを使用します。

asdm disconnect log_session *session*

構文の説明

session	終了するアクティブなASDMロギングセッションのセッションID。

コマンドデフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

アクティブなASDMロギングセッションとそれに関連付けられているセッションIDのリストを表示するには、**show asdm log_sessions**コマンドを使用します。特定のロギングセッションを終了するには、**asdm disconnect log_session**コマンドを使用します。

それぞれのアクティブなASDMセッションには、1つ以上の関連するASDMロギングセッションがあります。ASDMは、ロギングセッションを使用して、ASAからSyslogメッセージを取得します。ログセッションを終了すると、アクティブなASDMセッションに悪影響が及ぶ場合があります。不要なASDMセッションを終了するには、**asdm disconnect**コマンドを使用します。

（注） 各ASDMセッションには少なくとも1つのASDMロギングセッションがあるため、**show asdm sessions**および**show asdm log_sessions**の出力は同じように見えることがあります。

ASDMロギングセッションを終了しても、残りのアクティブなASDMロギングセッションは、関連付けられているセッションIDを保持します。たとえば、3つのアクティブなASDMロギングセッションがあり、それぞれのセッションIDが0、1、および2の場合、セッション1を終了すると、残りのアクティブなASDMロギングセッションはそれぞれセッションID 0

と 2 を保持します。この例で、次の新しい ASDM ロギング セッションにはセッション ID 1 が割り当てられ、その後の新しいロギング セッションにはセッション ID 3 から順に ID が割り当てられます。

例

次に、セッション ID 0 の ASDM セッションを終了する例を示します。**asdm disconnect log_sessions** コマンドの入力の前後に、**show asdm log_sessions** コマンドを使用して、アクティブな ASDM セッションを表示しています。

```
ciscoasa# show asdm log_sessions
0 192.168.1.1
1 192.168.1.2
ciscoasa# asdm disconnect 0
ciscoasa# show asdm log_sessions
1 192.168.1.2
```

関連コマンド

コマンド	説明
show asdm log_sessions	アクティブな ASDM ロギング セッションとそれに関連付けられているセッション ID のリストを表示します。

asdm history enable

ASDM 履歴トラッキングをイネーブルにするには、グローバル コンフィギュレーション モードで **asdm history enable** コマンドを使用します。ASDM 履歴トラッキ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。

asdm history enable
no asdm history enable

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 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、**pdm history enable** コマンドから **asdm history enable** コマンドに変更されました。

使用上のガイドライン

ASDM 履歴トラッキングをイネーブルにすることによって取得された情報は、ASDM 履歴バッファに保存されます。この情報を表示するには、**show asdm history** コマンドを使用します。履歴情報は、ASDM によってデバイス モニタリングに使用されます。

例

次に、ASDM 履歴トラッキングをイネーブルにする例を示します。

```
ciscoasa(config)# asdm history enable
ciscoasa(config)#
```

関連コマンド

コマンド	説明
show asdm history	ASDM 履歴バッファの内容を表示します。

asdm image

フラッシュメモリ内の ASDM ソフトウェアイメージの場所を指定するには、グローバル コンフィギュレーション モードで **asdm image** コマンドを使用します。イメージの場所を削除するには、このコマンドの **no** 形式を使用します。

asdm image *url*
no asdm image [*url*]

構文の説明

url フラッシュ メモリ内の ASDM イメージの場所を設定します。次の URL 構文を参照してください。

- **disk0:**/[*path*/]*filename*

ASA 5500 シリーズでは、この URL は内部フラッシュメモリを示します。**disk0** の代わりに **flash** を使用することもできます。これらはエイリアスになります。

- **disk1:**/[*path*/]*filename*

ASA 5500 シリーズでは、この URL は外部フラッシュメモリを示します。

- **flash:**/[*path*/]*filename*

この URL は、内部フラッシュメモリを指定します。

コマンド デフォルト

このコマンドをスタートアップ コンフィギュレーションに含めない場合、ASA は起動時に最初に検出した ASDM イメージを使用します。内部フラッシュ メモリのルート ディレクトリ内を検索した後で、外部フラッシュ メモリを検索します。ASA がイメージを検出した場合は、**asdm image** コマンドを実行コンフィギュレーションに挿入します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

フラッシュ メモリに複数のASDMソフトウェアイメージを保存できます。アクティブなASDMセッションがある状態で **asdm image** コマンドを入力して新しいASDMソフトウェアイメージを指定した場合、アクティブなASDMセッションは中断されず、そのセッションを開始したASDMソフトウェアイメージを引き続き使用します。新しいASDMセッションは、新しいソフトウェア イメージを使用します。**no asdm image** コマンドを入力すると、コンフィギュレーションからコマンドが削除されます。ただし、最後に設定したイメージの場所を使用して、ASAから引き続きASDMにアクセスできます。

このコマンドをスタートアップ コンフィギュレーションに含めない場合、ASAは起動時に最初に検出したASDMイメージを使用します。内部フラッシュ メモリのルート ディレクトリ内を検索した後で、外部フラッシュ メモリを検索します。ASAがイメージを検出した場合は、**asdm image** コマンドを実行コンフィギュレーションに挿入します。**write memory** コマンドを使用して、実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存します。**asdm image** コマンドをスタートアップ コンフィギュレーションに保存しない場合、リブートのたびにASAはASDMイメージを検索し、**asdm image** コマンドを実行コンフィギュレーションに挿入します。Auto Updateを使用する場合は、起動時にこのコマンドが自動的に追加されるため、ASA上のコンフィギュレーションはAuto Update Server上のコンフィギュレーションと一致しなくなります。このような不一致が発生すると、ASAはコンフィギュレーションをAuto Update Serverからダウンロードします。不要なAuto Updateアクティビティを回避するには、**asdm image** コマンドをスタートアップ コンフィギュレーションに保存します。

例

次に、ASDMイメージをasdm.binに設定する例を示します。

```
ciscoasa(config)# asdm image flash:/asdm.bin
ciscoasa(config)#
```

関連コマンド

コマンド	説明
show asdm image	現在のASDMイメージ ファイルを表示します。
boot	ソフトウェア イメージとスタートアップ コンフィギュレーション ファイルを設定します。

asdm location

⚠

注意 このコマンドを手動で設定しないでください。**asdm location** コマンドは ASDM によって実行コンフィギュレーションに追加され、内部通信に使用されます。このコマンドは、情報提供のためだけにこのマニュアルに記載されています。

asdm location *ip_addr netmask if_name*
asdm location *ipv6_addr/prefix if_name*

構文の説明

if_name	最もセキュリティの高いインターフェイスの名前。最もセキュリティの高いインターフェイスが複数ある場合は、任意にインターフェイス名が選択されます。このインターフェイス名は使用されませんが、必須パラメータです。
ip_addr	ネットワーク トポロジを定義するために ASDM によって内部で使用される IP アドレス。
ipv6_addr/prefix	ネットワーク トポロジを定義するために ASDM によって内部で使用される IPv6 アドレスとプレフィックス。
netmask	*ip_addr* のサブネット マスク。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
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)	このコマンドは、**pdm location** コマンドから **asdm location** コマンドに変更されました。

使用上のガイドライン

このコマンドを手動で設定または削除しないでください。

as-path access-list

正規表現を使用して自律システムパスフィルタを設定するには、グローバル コンフィギュレーション モードで as-path access-list コマンドを使用します。自律システムパスフィルタを削除し、これを実行コンフィギュレーション ファイルから削除するには、このコマンドの no 形式を使用します。

as-path access-list *acl-name* { **permit** | **deny** } *regexp*
no as-path access-list *acl-name*

構文の説明

acl-name	AS パス アクセス リストを指定する名前。
permit	一致条件に基づいてアドバタイズメントを許可します。
deny	一致条件に基づいてアドバタイズメントを拒否します。
regexp	AS パス フィルタを定義する正規表現。自律システム番号は 1 ～ 65535 の範囲で表します。 自律システム番号の形式の詳細については、router bgp コマンドの説明を参照してください。 （注） 正規表現の設定の詳細については、『Cisco IOS Terminal Services Configuration Guide』の付録「Regular Expressions」を参照してください。

コマンド デフォルト

自律システム パス フィルタは作成されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
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
9.2(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

自律システムパスフィルタを設定するには、as-path access-list コマンドを使用します。着信と発信の両方の BGP パスに自律システム パス フィルタを適用できます。各フィルタは正規表現

で定義されます。正規表現が、ルートの自律システム パスの ASCII ストリング表現と一致した場合、許可または拒否の条件が適用されます。自律システムパスにはローカル自律システム番号を含めないでください。

シスコが採用している4バイト自律システム番号は、自律システム番号の正規表現のマッチングおよび出力表示形式のデフォルトとして asplain（たとえば、65538）を使用していますが、RFC 5396 に記載されているとおり、4 バイト自律システム番号を asplain 形式および asdot 形式の両方で設定できます。4 バイト自律システム番号の正規表現マッチングと出力表示のデフォルトを asdot 形式に変更するには、bgp asnotation dot コマンドを使用します。デフォルトで asdot 形式がイネーブルにされている場合、正規表現の 4 バイト自律システム番号のマッチングには、すべて asdot 形式を使用する必要があり、使用しない場合正規表現によるマッチングは失敗します。

例

次の例では、自律システム パス アクセス リスト（番号 500）を定義し、自律システム 65535 から、またはこの自律システムを経由して、10.20.2.2 ネイバーにパスをアドバタイズしないように ASA を設定しています。

```
ciscoasa(config)# as-path access-list as-path-acl deny _65535_
ciscoasa(config)# as-path access-list as-path-acl deny ^65535$
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-fmaily ipv4
ciscoasa(config-router-af)# neighbor 192.168.1.1 remote-as 65535
ciscoasa(config-router-af)# neighbor 10.20.2.2 remote-as 40000
ciscoasa(config-router-af)# neighbor 10.20.2.2 filter-list as-path-acl out
```

asp load-balance per-packet

マルチコア ASA の場合、ロードバランシングの動作をパケット単位に変更するには、グローバル コンフィギュレーション モードで **asp load-balance per-packet** コマンドを使用します。デフォルトのロード バランシング メカニズムを復元するには、このコマンドの **no** 形式を使用します。

asp load-balance per-packet [**auto**]
no asp load-balance per-packet

構文の説明

auto	ネットワークの状況に応じて、各インターフェイスの受信リングでパケット単位のロードバランシングを自動的に有効または無効にします。

コマンド デフォルト

パケット単位のロードバランシングはデフォルトで無効になっています。

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。

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

コマンド履歴

リリース	変更内容
8.1(1)	このコマンドが追加されました。
9.3(1)	**auto** オプションが追加されました。
9.8(1)	**auto** オプションが ASA 仮想 に対して使用可能になりました。

使用上のガイドライン

ロード バランサのジョブは、パケットを CPU コアに配布し、パケットの順序を維持することです。デフォルトでは、接続は一度に1つのコアでしか処理できません。この動作により、使用中のインターフェイス/RX リングの数がコアの数に比べて少ない場合、コアは十分に活用されません。たとえば、ASA で 2 つのギガビット イーサネット インターフェイスしか使用されていない場合は、2つのコアだけが使用されます。（10 ギガビット イーサネット インターフェイスには 4 つの RX リングと、1 つの RX リングとしてギガビット イーサネット インターフェイスがあります）。パケット単位のロードバランシングを有効にして、より多くのコアを使用できるようにすることで、ロード バランサを最適化することができます。

デフォルトのロードバランシング動作では、多数のインターフェイスが使用されている場合にシステム全体のパフォーマンスが最適化され、パケット単位のロードバランサでは、アクティブなインターフェイスの数が少ない場合にシステム全体のパフォーマンスが最適化されます。

パケット単位のロードバランシングを有効にすると、1つのコアがインターフェイスからのパケットを処理する場合に、別のコアが同じインターフェイスからの次のパケットを受信して処理できます。したがって、すべてのコアが同じインターフェイスからのパケットを同時に処理することが可能です。

パケット単位のロード バランシングにより、次の場合にパフォーマンスが向上します。

- システムがパケットをドロップする
- **show cpu** コマンドで、CPU 使用率が 100% を大きく下回っていることが示されている。CPU 使用率は、使用されているコアの数を示す良い指標です。たとえば、8 コアシステムで、2 つのコアが使用されている場合、**show cpu** は 25% を示します。4 コアの場合は 50%、6 コアの場合は 75% を示します。
- 使用中のインターフェイスの数が少ない

（注） 通常、ASA に 64 未満の同時フローがある場合、パケット単位のロード バランシングを有効にすると、そのメリットよりもオーバーヘッドが大きくなります。

auto オプションを指定すると、ASA は非対称トラフィックが追加されたかどうかを検出できます。ロード バランシングが必要な場合、インターフェイス受信リングとコアとの 1 対 1 のロックは解放されます。パケット単位のロードバランシングは、すべてのインターフェイス受信リングではなく、高負荷のインターフェイス受信リングでのみ有効になります。この適応型ロード バランス メカニズムは、次の問題の回避に役立ちます。

- フロー上での突発的なトラフィックの増加によって発生するオーバーラン
- 特定のインターフェイス受信リングをオーバーサブスクライブするバルク フローによるオーバーラン
- 比較的高過負荷のインターフェイス受信リングによるオーバーラン（シングル コアでは負荷を維持できません）

auto オプションは、9.7 以前の ASA 仮想 では使用できません。

例

次に、デフォルトのロード バランシング動作を変更する例を示します。

```
ciscoasa(config)# asp load-balance per-packet
```

次に、パケットごとのロードバランシングのオンとオフの自動切り替えをイネーブルにする例を示します。

```
ciscoasa(config)# asp load-balance per-packet auto
```

関連コマンド

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

asp rule-engine transactional-commit

ルールエンジンのトランザクション コミット モデルを有効または無効にするには、**asp rule-engine transactional-commit** コマンドを使用します。

asp rule-engine transactional-commit *option*
no asp rule-engine transactional-commit *option*

構文の説明

option 選択したポリシー用のルールエンジンのトランザクション コミット モデルをイネーブルにします。次のオプションがあります。

- **access-group**：グローバルに、またはインターフェイスに適用されるアクセスルール。
- **nat**：ネットワークアドレス変換ルール。

コマンド デフォルト

デフォルトでは、トランザクション コミット モデル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。

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

コマンド履歴

リリース	変更内容
9.1(5)	このコマンドが追加されました。
9.3(1)	**nat**キーワードが追加されました。

使用上のガイドライン

デフォルトでは、ルール ベースのポリシー（アクセス ルールなど）を変更した場合、変更はただちに有効になります。ただし、この即時性にはパフォーマンスにわずかなコストがかかります。パフォーマンス コストは、1秒あたりの接続数が多い環境で大量のルール リストがある場合に顕著です。たとえば、ASA が 1 秒あたり 18,000 個の接続を処理しながら、25,000 個のルールがあるポリシーを変更する場合などです。

パフォーマンスに影響するのは、ルール検索を高速化するためにルール エンジンがルールをコンパイルするためです。デフォルトでは、新しいルールを適用できるように、接続試行を評価

するときに未コンパイルのルールも検索されます。新しいルールはコンパイルされていないため、検索に時間がかかります。

ルール変更を実装するときにルール エンジンがトランザクション モデルを使用するように、この動作を変更できます。これにより、新しいルールがコンパイルされ、使用できるようになるまで、引き続き古いルールが使用されます。トランザクション モデルを使用すると、ルールのコンパイル中、パフォーマンスは低下しないはずです。次の表は、その動作の違いを明確にします。

モデル	コンパイル前	コンパイル中	コンパイル後
デフォルト	古いルールと照合します。	新しいルールと照合します。 （接続数/秒が削減されます）	新しいルールと照合します。
トランザクション	古いルールと照合します。	古いルールと照合します。 （接続数/秒は影響を受けません）	新しいルールと照合します。

トランザクション モデルのメリットにはこのほか、インターフェイスでACLを置き換える際、古い ACL の削除と新しいポリシーの適用との間にギャップが生じないことがあります。これにより、動作中に許容可能な接続がドロップされる確率が減少します。

ヒント ルール タイプのトランザクション モデルをイネーブルにした場合、コンパイルの先頭と末尾をマークする syslog メッセージが存在します。これらのメッセージには、780001 以降の番号が付けられます。

例

次に、アクセス グループのトランザクション コミット モデルをイネーブルにする例を示します。

```
ciscoasa(config)# asp rule-engine transactional-commit access-group
```

関連コマンド

コマンド	説明
clear conf asp rule-engine transactional-commit	ルール エンジンのトランザクション コミット設定をクリアします。
show run asp rule-engine transactional-commit	ルール エンジンの実行コンフィギュレーションを表示します。

asr-group

非対称ルーティング インターフェイス グループ ID を指定するには、インターフェイス コンフィギュレーション モードで **asr-group** コマンドを使用します。ID を削除するには、このコマンドの **no** 形式を使用します。

asr-group *group_id*
no asr-group *group_id*

構文の説明

group_id	非対称ルーティング グループ ID。有効な値は、1 ～ 32 です。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

使用上のガイドライン

Active/Active フェールオーバーがイネーブルの場合、ロードバランシングにより、発信接続のリターン トラフィックがピア ユニット上のアクティブなコンテキストを介してルーティングされることがあります。このピアユニットでは、発信接続のコンテキストはスタンバイ グループ内にあります。

asr-group コマンドを使用すると、着信インターフェイスのフローが見つからない場合に、着信パケットが同じ ASR グループのインターフェイスで再分類されます。再分類により別のインターフェイスのフローが見つかり、関連付けられているコンテキストがスタンバイ状態の場合、パケットは処理のためにアクティブなユニットに転送されます。

このコマンドを有効にするには、ステートフル フェールオーバーをイネーブルにする必要があります。

ASR 統計情報は、**show interface detail** コマンドを使用して表示できます。この統計情報には、インターフェイス上で送信、受信、およびドロップされた ASR パケットの数が含まれます。

（注） 同じコンテキスト内の 2 個のインターフェイスを、同じ ASR グループ内で設定してはなりません。

例

次に、選択したインターフェイスを非対称ルーティング グループ 1 に割り当てる例を示します。

コンテキスト ctx1 のコンフィギュレーション：

```
ciscoasa/ctx1(config)# interface Ethernet2
ciscoasa/ctx1(config-if)# nameif outside
ciscoasa/ctx1(config-if)# ip address 192.168.1.11 255.255.255.0 standby 192.168.1.21
ciscoasa/ctx1(config-if)# asr-group 1
```

コンテキスト ctx2 のコンフィギュレーション：

```
ciscoasa/ctx2(config)# interface Ethernet3
ciscoasa/ctx2(config-if)# nameif outside
ciscoasa/ctx2(config-if)# ip address 192.168.1.31 255.255.255.0 standby 192.168.1.41
ciscoasa/ctx2(config-if)# asr-group 1
```

関連コマンド

コマンド	説明
interface	インターフェイス コンフィギュレーション モードを開始します。
show interface	インターフェイス統計情報を表示します。

assertion-consumer-url（廃止）

（注） このコマンドをサポートする最後のリリースは、Version 9.5(1) でした。

セキュリティデバイスがアサーション コンシューマ サービスに接続するためにアクセスするURL を指定するには、webvpn コンフィギュレーション モードで、特定の SAML-type SSO サーバーに対して **assertion-consumer-url** コマンドを使用します。この URL をアサ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。

assertion-consumer-url *url*
no assertion-consumer-url [*url*]

構文の説明

url SAML-type SSO サーバーで使用するアサーション コンシューマ サービスの URL を指定します。URL は http:// または https:// で始まり、255 文字未満の英数字である必要があります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
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。
9.5(2)	このコマンドは、SAML 2.0 のサポートの導入に伴って廃止されました。

使用上のガイドライン

シングル サインオン（SSO）は、WebVPN でのみサポートされています。これにより、ユーザーはユーザー名とパスワードを一度だけ入力すれば、別のサーバーでさまざまなセキュアなサービスにアクセスできます。ASA は現在、SAML POST-type の SSO サーバーと SiteMinder-type の SSO サーバーをサポートしています。

このコマンドは、SAML-type の SSO サーバーのみに適用されます。

URL が HTTPS で始まる場合は、アサーション コンシューマ サービス SSL 証明書のルート証明書をインストールする必要があります。

例

次に、SAML-type の SSO サーバーのアサーション コンシューマ URL を指定する例を示します。

```
ciscoasa(config-webvpn)# sso server myhostname type saml-v1.1-post
ciscoasa(config-webvpn-sso-saml# assertion-consumer-url https://saml-server/postconsumer
ciscoasa(config-webvpn-sso-saml#
```

関連コマンド

コマンド	説明
issuer	SAML-type の SSO サーバーのセキュリティ デバイス名を指定します。
request-timeout	SSO 認証の試行に失敗したときにタイムアウトになるまでの秒数を指定します。
show webvpn sso-server	セキュリティ デバイスに設定されているすべての SSO サーバーの運用統計情報を表示します。
sso-server	WebVPN SSO サーバーを作成します。
trustpoint	SAML-type のブラウザ アサーションへの署名に使用する証明書を含むトラストポイント名を指定します。

attribute bind

属性ベースのネットワークオブジェクトのIP-to-attributeバインディングを変更するには、EXECモードで **attribute bind** コマンドを使用します。

attribute bind *agent-name* **binding** *ip-address* **type** *attribute-type* **value** *attribute-value*

構文の説明

agent-name	属性をモニターする VM 属性エージェントの名前を指定します。
ip-address	管理対象の属性ベースのネットワーク オブジェクトの IP アドレスを指定します。
attribute-type	更新する属性タイプを識別する文字列を指定します。
attribute-value	属性タイプに割り当てる新しい値を識別する文字列を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

例

次に、SAML-type の SSO サーバーのアサーション コンシューマ URL を指定する例を示します。

```
ciscoasa(config)# attribute bind VMAgent binding 10.10.1.19 type custom.location value global
```

関連コマンド

コマンド	説明
attribute source-group	VM 属性エージェントを設定します。
object network attribute	属性ベースのネットワーク オブジェクトを設定します。

コマンド	説明
show attribute object-map	object-to-attribute バインディングを示します。
show attribute host-map	host-to-attribute バインディングのマップを示します。

attribute source-group

VMware vCenter または単一の ESXi ホストと通信するように VM 属性エージェントを設定するには、EXEC モードで **attribute source-group** コマンドを使用します。エージェントを削除するには、このコマンドの **no** 形式を使用します。

attribute source-group *agent-name* **type** *agent-type*
no attribute source-group *agent-name*

構文の説明

agent-name	VM 属性エージェントの名前を指定します。
agent-type	属性エージェントのタイプを指定します。現在、サポートされるエージェント タイプは ESXi のみです。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

例

次に、VM 属性エージェントを設定する例を示します。

```
ciscoasa(config)# attribute source-group VMAgent type esxi
```

関連コマンド

コマンド	説明
object network attribute	属性ベースのネットワーク オブジェクトを設定します。
show attribute source-group	設定した属性エージェントに関する情報を表示します。
show attribute object-map	object-to-attribute バインディングを示します。
show attribute host-map	host-to-attribute バインディングのマップを示します。

attribute source-group host

VM 属性エージェントが vCenter または単一の ESXi ホストと通信できるように VMware vCenter ホストクレデンシャルを設定するには、属性エージェント コンフィギュレーション モードで **attribute source-group host** コマンドを使用します。ホストクレデンシャルを削除するには、このコマンドの **no** 形式を使用します。

host *ip-address* **username** *ESXi-username* **password** *ESXi-password*
no host *ip-address*

構文の説明

ip-address	VM 属性エージェントの名前を指定します。
ESXi-username	vCenter ホストのユーザー名を指定します。
ESXi-password	vCenter ホストのパスワードを指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

属性エージェントを設定または変更した後に、このコマンドを使用します。

例

次に、属性エージェントにホスト クレデンシャルを設定する例を示します。

```
ciscoasa(config)# attribute source-group VMAgent
ciscoasa(config-attr)# host 10.122.202.217 user admin password Cisco123
```

関連コマンド

コマンド	説明
attribute source-group	VM 属性エージェントを設定します。
object network attribute	属性ベースのネットワーク オブジェクトを設定します。
show attribute source-group	設定した属性エージェントに関する情報を表示します。
show attribute object-map	object-to-attribute バインディングを示します。
show attribute host-map	host-to-attribute バインディングのマップを示します。

attribute source-group keepalive

VMware vCenter 通信のキープアライブ設定を構成するには、属性エージェント コンフィギュレーション モードで **attribute source-group keepalive** 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。

keepalive retry-interval *interval* **retry-count** *count*
no keepalive

構文の説明

interval 属性エージェントから vCenter へのキープアライブ メッセージの間隔を指定します。キープアライブ メッセージが送信元からの応答を受信するたびに、エージェントは送信元との接続が有効になっているとみなされ、そのエージェントのキープアライブ タイマーが再起動されます。デフォルトは 30 秒です。

count キープアライブ メッセージが受信されなかった場合の再試行回数を指定します。タイマーがキープアライブを受信せずに期限切れになるたびに、そのエージェントの再試行回数が増分されます。再試行回数が設定されたしきい値に達すると、エージェントは送信元との接触が失われたことを宣言します。デフォルトは 3 です。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

属性エージェントを設定または変更した後に、このコマンドを使用します。

例

次に、SAML-type の SSO サーバーのアサーション コンシューマ URL を指定する例を示します。

```
ciscoasa(config)# attribute source-group VMAgent
ciscoasa(config-attr)# keepalive retry-timer 100 retry-count 5
```

関連コマンド

コマンド	説明
attribute source-group	VM 属性エージェントを設定します。
object network attribute	属性ベースのネットワーク オブジェクトを設定します。
show attribute source-group	設定した属性エージェントに関する情報を表示します。
show attribute object-map	object-to-attribute バインディングを示します。
show attribute host-map	host-to-attribute バインディングのマップを示します。

attributes

ASA が DAP 属性データベースに書き込む属性値ペアを指定するには、DAP テスト属性モードで **attributes** コマンドを使用します。

attributes *name value*

構文の説明

name	ウェルノウン属性名、または「label」タグを組み込む属性を指定します。label タグは、DAP レコード内のファイル、レジストリ、プロセス、アンチウイルス、アンチスパイウェア、およびパーソナル ファイアウォールのエンドポイント属性に対して設定するエンドポイント ID に対応します。
value	AAA 属性に割り当てられた値。

コマンド デフォルト

デフォルトの値や動作はありません。

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
DAP 属性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
8.0(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

複数の属性値ペアを入力するには、このコマンドを複数回使用します。

通常、ASA は AAA サーバーからユーザー認可属性を取得し、Cisco Secure Desktop、Host Scan、CNA または NAC からエンドポイント属性を取得します。test コマンドの場合、ユーザー認可属性とエンドポイント属性をこの属性モードで指定します。ASA は、これらの属性を、DAP サブシステムが DAP レコードの AAA 選択属性およびエンドポイント選択属性を評価するときに参照する属性データベースに書き込みます。

例

次の例では、認証されたユーザーが SAP グループのメンバーで、エンドポイントシステムにアンチウイルスソフトウェアがインストールされている場合に、ASA が 2 つの DAP レコードを選択することを前提としています。アンチウイルス ソフトウェアのエンドポイント ルールのエンドポイント ID は *nav* です。

DAP レコードには、次のポリシー属性があります。

DAP レコード 1	DAP レコード 2
action = continue	action = continue
port-forward = enable hostlist1	url-list = links2
—	url-entry = enable

```
ciscoasa
 #
test dynamic-access-policy attributes
ciscoasa
(config-dap-test-attr)#
attributes aaa.ldap.memberof SAP
ciscoasa
(config-dap-test-attr)#
 attributes endpoint.av.nav.exists true
ciscoasa
(config-dap-test-attr)#
exit
ciscoasa
 #
test dynamic-access-policy execute
Policy Attributes:
action = continue
port-forward = enable hostlist1
url-list = links2
url-entry = enable
ciscoasa
 #
```

関連コマンド

コマンド	説明
display	現在の属性リストを表示します。
dynamic-access-policy-record	DAP レコードを作成します。
test dynamic-access-policy attributes	属性を入力します。
test dynamic-access-policy execute	DAP を生成するロジックを実行し、生成されたアクセスポリシーをコンソールに表示します。

auth-cookie-name

認証クッキーの名前を指定するには、AAA サーバー ホスト コンフィギュレーション モードで **auth-cookie-name** コマンドを使用します。これは HTTP フォームのコマンドを使用した SSO です。

auth-cookie-name

構文の説明

name 認証クッキーの名前。名前の最大の長さは 128 文字です。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

ASA の WebVPN サーバーは、シングルサインオン（SSO）サーバーにシングルサインオン認証要求を送信することに HTTP POST 要求を使用します。認証が成功すると、認証 Web サーバーは、認証クッキーをクライアント ブラウザに戻します。クライアント ブラウザは、その認証クッキーを提示して、SSO ドメイン内の他の Web サーバーの認証を受けます。**auth-cookie-name** コマンドは、 ASA によって SSO に使用される認証クッキーの名前を設定します。

一般的な認証クッキーの形式は、Set-Cookie: *cookie name=cookie value* [;*cookie attributes*] です。次の認証クッキーの例では、SMSESSION が **auth-cookie-name** コマンドで設定される名前です。

```
Set-Cookie:
```

例

次に、example.com という名前の Web サーバーから受信した認証クッキーに認証クッキー名 SMSESSION を指定する例を示します。

```
ciscoasa(config)# aaa-server testgrp1 host example.com
ciscoasa(config-aaa-server-host)# auth-cookie-name SMSESSION
ciscoasa(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
action-uri	シングルサインオン認証用のユーザー名およびパスワードを受信するための Web サーバー URI を指定します。
hidden-parameter	認証 Web サーバーと交換するための非表示パラメータを作成します。
password-parameter	SSO 認証用にユーザー パスワードを送信する必要がある HTTP POST 要求パラメータの名前を指定します。
start-url	プリログイン クッキーを取得する URL を指定します。
user-parameter	ユーザー名パラメータを SSO 認証に使用される HTTP POST 要求の一部として送信する必要があることを指定します。

authenticated-session-username

二重認証がイネーブルになっている場合に、セッションに関連付ける認証ユーザー名を指定するには、トンネルグループ一般属性モードで **authenticated-session-username** コマンドを使用します。コンフィギュレーションから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。

authenticated-session-username { **primary** | **secondary** }
no authenticated-session-username

構文の説明

primary	プライマリ認証サーバーからのユーザー名を使用します。
secondary	セカンダリ認証サーバーからのユーザー名を使用します。

コマンド デフォルト

デフォルト値は **primary** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
トンネル グループ一般属性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
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、二重認証がイネーブルになっている場合に限り有効です。**authenticated-session-username** コマンドは、ASA がセッションに関連付けるユーザー名を抽出する認証サーバーを選択します。

例

次に、グローバル コンフィギュレーション モードで、remotegrp という名前の IPsec リモート アクセス トンネル グループを作成し、接続にセカンダリ認証サーバーからのユーザー名を使用することを指定する例を示します。

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp general-attributes
```

```
ciscoasa(config-tunnel-webvpn)# authenticated-session-username secondary
ciscoasa(config-tunnel-webvpn)#
```

関連コマンド

コマンド	説明
pre-fill-username	ユーザー名の事前入力機能をイネーブルにします。
show running-config tunnel-group	指定されたトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般属性を指定します。
username-from-certificate	認可時のユーザー名として使用する証明書内のフィールドを指定します。

authentication（bfd-template）

シングルホップおよびマルチホップセッション用のBFDテンプレートで認証を設定するには、BFD コンフィギュレーション モードで authentication コマンドを使用します。シングルホップまたはマルチホップセッション用の BFD テンプレートで認証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。

authentication *authentication-type* ［ **0|8** ］ *key-string* **key-id** *id*

構文の説明

authentication-type	認証タイプを指定します。有効な値は **md5**、**meticulous-md5**、**meticulous-sha-1**、および **sha-1** です。
0|8	0：暗号化されていないパスワードが後に続くことを示します。8：暗号化されたパスワードが後に続くことを示します。
key-string	認証されるルーティングプロトコルを使用してパケットで送信および受信される必要のある認証文字列を指定します。有効な範囲は、1～17文字の大文字と小文字の英数字です。ただし、最初の文字は数字にはできません。
id	キー文字列に一致する共有キー ID を指定します。

コマンド デフォルト

このコマンドにデフォルトの動作または値はありません。

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
BFD 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
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、BFD シングルホップおよびマルチホップ テンプレートで認証を設定するために使用します。セキュリティを強化するために認証を設定することをお勧めします。

認証は、BFDの送信元と宛先のペアごとに設定する必要があり、認証パラメータは両方のデバイスで同じである必要があります。

例

次に、シングルホップ BFD テンプレートで認証を設定する例を示します。

```
ciscoasa(config)# bfd single-hop sh-template
ciscoasa(config-bfd)# authentication sha-1 0 cisco key-id 10
```

次に、マルチホップ BFD テンプレートで認証を設定する例を示します。

```
ciscoasa(config)# bfd multi-hop mh-template
ciscoasa(config-bfd)# authentication shat-1 0 cisco key-id 10
```

関連コマンド

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

authentication

WebVPN と電子メールプロキシの認証方式を設定するには、各モードで **authentication** コマンドを使用します。デフォルトの方式に戻すには、このコマンドの **no** 形式を使用します。ASA は、ユーザーを認証してユーザー ID を確認します。

authentication [{ [**aaa**] [**certificate**] [**multiple certificate**] [**saml**] [**mailhost**] [**piggyback**] }
no authentication [[**aaa**] [**certificate**] [**multiple certificate**] [**saml**] [**mailhost**] [**piggyback**]

構文の説明

aaa	ASA が設定済みの AAA サーバーと照合するユーザー名およびパスワードを指定します。
certificate	SSL ネゴシエーション時の証明書を指定します。
mailhost	SMTPS の場合のみ、リモート メール サーバーで認証します。IMAP4S および POP3S の場合、メールホスト認証は必須であり、設定可能なオプションとして表示されません。
multiple certificate	SSL ネゴシエーション時の複数証明書オプションを指定します。
piggyback	HTTPS WebVPN セッションがすでに存在している必要があります。ピギーバック認証は、電子メール プロキシでのみ使用できます。
saml	SAML 認証方式は相互に排他的です。

コマンド デフォルト

次の表に、WebVPN および電子メール プロキシのデフォルトの認証方式を示します。

プロトコル	デフォルトの認証方式
IMAP4S	メールホスト（必須）
POP3S	メールホスト（必須）
SMTPS	AAA
WebVPN	AAA

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
Imap4s コンフィギュレーション	• 対応	—	• 対応	—	—
Pop3s コンフィギュレーション	• 対応	—	• 対応	—	—
smtps コンフィギュレーション	• 対応	—	• 対応	—	—
webvpn コンフィギュレーション	• 対応	—	• 対応		
トンネルグループ 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。
7.1(1)	このコマンドは、webvpn コンフィギュレーション モードでは廃止され、WebVPN 用のトンネル グループ webvpn 属性コンフィギュレーション モードに置き換えられました。
8.0(2)	このコマンドは、証明書認証要件の変更を反映するように変更されました。
9.5(2)	このコマンドは、SAML 2.0 のサポートを反映して変更されました。
9.7(1)	既存の認証属性は、複数証明書認証のオプションを含めるように変更されます。

使用上のガイドライン

少なくとも 1 つの認証方式が必要です。たとえば、WebVPN の場合、AAA 認証と証明書認証のいずれか一方または両方を指定できます。任意の順序でこれらのコマンドを入力できます。

WebVPN 証明書認証では、それぞれのインターフェイスに対して HTTPS ユーザー証明書を要求する必要があります。つまり、この選択が機能するには、証明書認証を指定する前に、**authentication-certificate** コマンドでインターフェイスを指定しておく必要があります。

このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ webvpn 属性コンフィギュレーション モードの同等のコマンドに変換されます。

WebVPN の場合、AAA 認証と証明書認証の両方を要求できます。この場合、ユーザーは証明書とユーザー名/パスワードの両方を指定する必要があります。電子メール プロキシ認証の場合、複数の認証方式を要求できます。このコマンドを再び指定すると、現在のコンフィギュレーションが上書きされます。

例

次に、WebVPN ユーザーに認証のための証明書を要求する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# authentication certificate
```

例

次に、WebVPN ユーザーに認証のための証明書を要求する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# authentication certificate
```

関連コマンド

コマンド	説明
authentication-certificate	接続を確立する WebVPN クライアントからの証明書を要求します。
show running-config	現在のトンネル グループ コンフィギュレーションを表示します。
clear configure aaa	設定した AAA の値を削除またはリセットします。
show running-config aaa	AAA コンフィギュレーションを表示します。

authentication eap-proxy

L2TP over IPsec 接続に対して EAP をイネーブルにし、ASA が PPP 認証プロセスを外部の RADIUS 認証サーバーにプロキシできるようにするには、トンネルグループ ppp 属性コンフィギュレーション モードで **authentication eap-proxy** コマンドを使用します。コマンドをデフォルト設定に戻すには（CHAP および MS-CHAP を許可）、このコマンドの **no** 形式を使用します。

authentication eap-proxy
no authentication eap-proxy

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

デフォルトでは、EAP は認証プロトコルとして許可されていません。

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。

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
トンネル グループ PPP 属性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

この属性は、L2TP または IPsec トンネル グループ タイプのみに適用できます。

例

次に、設定 ppp コンフィギュレーション モードで、pppremotegrp という名前のトンネル グループの PPP 接続に対して EAP を許可する例を示します。

```
ciscoasa(config)# tunnel-group pppremotegrp type IPSec/IPSec
ciscoasa(config)# tunnel-group pppremotegrp ppp-attributes
ciscoasa(config-ppp)# authentication eap
ciscoasa(config-ppp)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel-group	指定した証明書マップ エントリを表示します。
tunnel-group-map default-group	**crypto ca certificate map** コマンドを使用して作成された証明書マップ トンネルをトンネル グループに関連付けます。

authentication key

IS-IS での認証をイネーブルにするには、ルータ ISIS コンフィギュレーション モードで **authentication key** コマンドを使用します。このような認証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。

authentication key [**0** | **8**] *password* [**level-1** | **level-2**]
no authentication key [**0** | **8**] *password* [**level-1** | **level-2**]

構文の説明

password	認証をイネーブルにし、 キーを指定します。
level-1	（任意）レベル 1 パケットについてだけ認証をイネーブルにします。
level-2	（任意）レベル 2 パケットについてだけ認証をイネーブルにします。

コマンド デフォルト

ルータ レベルでは、IS-IS パケットにキー認証は適用されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ isis 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
9.6(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

key コマンドで設定されたパスワードが存在しない場合、キー認証は行われません。

キー認証は、クリア テキスト認証または MD5 認証に適用できます。モードは authentication mode コマンドで設定されます。

IS-IS に一度に適用できる認証キーは 1 つだけです。つまり、2 番めの authentication key コマンドを設定すると、最初のコマンドは上書きされます。

キーワード **level-1** および **level-2** のいずれも設定されていない場合、パスワードは両方のレベルに適用されます。

isis authentication key コマンドを使用することにより、個々の IS-IS インターフェイスに認証を指定できます。

（注） IS-IS では、**authentication key-chain** コマンドを使用してグローバルに設定されたキーチェーンの有効期限を選択します。ASA のキーチェーンインフラストラクチャが存在しないため、このコマンドとともにキーを提供します。

例

次に、site1 という名前のキーチェーンに属する任意のキーを受け入れ、送信するように IS-IS を設定する例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# net 49.0000.0101.0101.0101.00
ciscoasa(config-router)# is-type level-1
ciscoasa(config-router)# authentication mode md5 level-1
ciscoasa(config-router)# authentication key 0 site1 level-1
```

関連コマンド

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

コマンド	説明
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。

コマンド	説明
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更（アップまたはダウン）する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が ASA のデータベースに更新されずに存在する最長時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト（TLV）を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。

コマンド	説明
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

authentication key eigrp

EIGRP パケットの認証をイネーブルにし、認証キーを指定するには、インターフェイス コンフィギュレーション モードで **authentication key eigrp** コマンドを使用します。EIGRP 認証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。

authentication key eigrp *as-number key* **key-id** *key-id*
no authentication key eigrp *as-number*

構文の説明

as-number	認証する EIGRP プロセスの自律システム番号。これは、EIGRP ルーティング プロセスに設定されている値と同じにする必要があります。
key	EIGRP 更新を認証するキー。このキーには、最大 16 文字を含めることができます。
key-id*key-id*	キー ID 値。有効な値の範囲は 1 ～ 255 です。

コマンド デフォルト

EIGRP 認証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。

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
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
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

EIGRP メッセージ認証をイネーブルにするには、**authentication mode eigrp** および **authentication key eigrp** コマンドの両方をインターフェイスに設定する必要があります。インターフェイスに設定された **authentication** コマンドを表示するには、**show running-config interface** コマンドを使用します。

例

次に、インターフェイス GigabitEthernet0/3 に設定された EIGRP 認証の例を示します。

```
ciscoasa(config)# interface Gigabit0/3
ciscoasa(config-if)# authentication mode eigrp md5
ciscoasa(config-if)# authentication key eigrp 100 thisismykey key_id 5
```

関連コマンド

コマンド	説明
authentication mode eigrp	EIGRP認証に使用する認証のタイプを指定します。

authentication mode

IS-IS インスタンスに対する IS-IS パケットで使用される認証のタイプを指定するには、ルータ ISIS コンフィギュレーション モードで **authentication mode** コマンドを使用します。クリアテキスト認証に戻すには、このコマンドの **no** 形式を使用します。

authentication mode { **md5** | **text** } [**level-1** | **level-2**]
no authentication mode

構文の説明

md5	Message Digest 5（MD5）認証。
text	平文認証
level-1	（任意）レベル 1 パケットについてだけ、指定された認証をイネーブルにします。
level-2	（任意）レベル 2 パケットについてだけ、指定された認証をイネーブルにします。

コマンド デフォルト

クリアテキスト（プレーンテキスト）認証は **area-password** コマンドや **domain-password** コマンドなど、その他の方法でも設定できますが、このコマンドを使用すると、ルータ レベルでは IS-IS パケットに対する認証は提供されません。

コマンド モード

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
ルータ isis コンフィギュレーション	• 対応	—	• 対応	• 対応	—

使用上のガイドライン

キーワード **level-1** および **level-2** のいずれも設定されていない場合、パスワードは両方のレベルに適用されます。

isis authentication mode コマンドを使用することにより、認証のタイプとそのタイプが 1 つの IS-IS インターフェイスに対して（IS-IS インスタンス単位ではなく）適用されるレベルを指定できます。

area-password または **domain-password** コマンドを使用してクリアテキスト認証が設定されている場合、これらのコマンドよりも authentication mode コマンドが優先されます。

authentication mode コマンドを設定した後で、**area-password** または **domain-password** コマンドを設定しようとしてもできません。**area-password** または **domain-password** コマンドを使用してクリアテキスト認証を設定しなければならない場合は、まず、**no authentication mode** コマンドを使用する必要があります。

例

次に、レベル 1 パケットに対する IS-IS インスタンスの MD5 認証を設定する例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# net 49.0000.0101.0101.0101.00
ciscoasa(config-router)# is-type level-1
ciscoasa(config-router)# authentication mode md5 level-1
ciscoasa(config-router)# authentication key 0 site1 level-1
```

関連コマンド

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

コマンド	説明
lsp-full suppress	PDUがフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSPが更新されずにASAのデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべてのIS-ISインターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト（TLV）を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成してLSPデータベースをクリアすることができないように、IS-ISプロトコルをグローバルで無効にします。
redistribute isis	特にレベル1からレベル2へ、またはレベル2からレベル1へ、IS-IS ルートを再配布します。
route priority high	IS-IS IPプレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
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。

コマンド	説明
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

authentication ms-chap-v1

L2TP over IPsec 接続に対して PPP の Microsoft CHAP Version 1 認証をイネーブルにするには、トンネルグループ ppp 属性コンフィギュレーションモードで **authentication ms-chap-v1** コマンドを使用します。コマンドをデフォルト設定に戻すには（CHAP および MS-CHAP を許可）、このコマンドの **no** 形式を使用します。Microsoft CHAP Version 1 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。

authentication ms-chap-v1
no authentication ms-chap-v1

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

この属性は、L2TP または IPsec トンネル グループ タイプのみに適用できます。このプロトコルは CHAP と類似していますが、CHAP のようなクリアテキスト パスワードではなく、暗号化されたパスワードのみをサーバーが格納して比較するために、よりセキュアです。また、このプロトコルはデータ暗号化のためのキーを MPPE によって生成します。

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループ データベース全体または指定されたトンネル グループだけをクリアします。

コマンド	説明
show running-config tunnel-group	指定されたトンネル グループまたはすべてのトンネル グループの現在実行されているトンネル グループ コンフィギュレーションを表示します。
tunnel-group	IPsec および WebVPN トンネルの接続固有レコードのデータベースを作成および管理します。

authentication ms-chap-v2

L2TP over IPsec 接続に対して PPP の Microsoft CHAP Version 2 認証をイネーブルにするには、トンネルグループ ppp 属性コンフィギュレーション モードで **authentication ms-chap-v1** コマンドを使用します。コマンドをデフォルト設定に戻すには（CHAP および MS-CHAP を許可）、このコマンドの **no** 形式を使用します。

authentication ms-chap-v2
no authentication ms-chap-v2

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

この属性は、L2TP または IPsec トンネル グループ タイプのみに適用できます。

このプロトコルは CHAP と類似していますが、CHAP のようなクリアテキスト パスワードではなく、暗号化されたパスワードのみをサーバーが格納して比較するために、よりセキュアです。また、このプロトコルはデータ暗号化のためのキーを MPPE によって生成します。

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループ データベース全体または指定されたトンネル グループだけをクリアします。

コマンド	説明
show running-config tunnel-group	指定されたトンネル グループまたはすべてのトンネル グループの現在実行されているトンネル グループ コンフィギュレーションを表示します。
tunnel-group	IPsec および WebVPN トンネルの接続固有レコードのデータベースを作成および管理します。

authentication pap

L2TP over IPsec 接続に対して PPP の PAP 認証を許可するには、トンネルグループ ppp 属性コンフィギュレーション モードで **authentication pap** コマンドを使用します。コマンドをデフォルト設定に戻すには（CHAP および MS-CHAP を許可）、このコマンドの **no** 形式を使用します。

authentication pap
no authentication pap

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

デフォルトでは、PAP は認証プロトコルとして許可されていません。

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。

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
トンネル グループ PPP 属性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

この属性は、L2TP または IPsec トンネル グループ タイプのみに適用できます。

このプロトコルは、認証時にクリアテキストのユーザー名とパスワードを渡すため、安全ではありません。

例

次に、設定 ppp コンフィギュレーション モードで、pppremotegrp という名前のトンネル グループの PPP 接続に対して PAP を許可する例を示します。

```
ciscoasa(config)# tunnel-group pppremotegrp type IPSec/IPSec
ciscoasa(config)# tunnel-group pppremotegrp ppp-attributes
ciscoasa(config-ppp)# authentication pap
ciscoasa(config-ppp)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel-group	指定した証明書マップ エントリを表示します。
tunnel-group-map default-group	**crypto ca certificate map** コマンドを使用して作成された証明書マップ トンネルをトンネル グループに関連付けます。

authentication send-only

IS-IS インスタンスについて、受信ではなく送信される IS-IS パケットに対してのみ認証が実行されるように指定するには、ルータ ISIS コンフィギュレーション モードで **authentication send-only** コマンドを使用します。送信および受信されるパケットに対して認証が実行されるように設定するには、このコマンドの**no** 形式を使用します。

authentication send-only [**level-1** | **level-2**]
no authentication send-only

構文の説明

level-1	（任意）認証は受信ではなく、送信されるレベル 1 パケットだけに実行されます。
level-2	（任意）認証は受信ではなく、送信されるレベル 2 パケットだけに実行されます。

コマンド デフォルト

認証がルータ レベルで設定されている場合、その認証が送信と受信の IS-IS パケットに適用されます。

コマンド モード

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
ルータ isis コンフィギュレーション	• 対応	—	• 対応	• 対応	—

使用上のガイドライン

このコマンドは、認証モードおよび認証キー チェーンを設定する前に使用します。これにより、認証の実装がスムーズに進むようになります。送信されるパケットだけに認証が挿入され、受信されるパケットではチェックされない場合、各ルータでキーの設定に費やせる時間が長くなります。このコマンドを使用して、通信を必要とするルータすべてを設定した後で、ルータごとに、認証モードとキー チェーンをイネーブルにします。その後、**no authentication send-only** コマンドを指定して、send-only 機能をディセーブルにします。

キーワード **level-1** および **level-2** のいずれも設定されていない場合、send-only 機能は両方のレベルに適用されます。

このコマンドは、クリアテキスト認証またはMD5認証に適用できます。モードは**authentication mode** コマンドで設定されます。

例

次に、受信ではなく送信されるパケットでクリア テキスト認証が使用されるように IS-IS レベル 1 パケットを設定する例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# net 49.0000.0101.0101.0101.00
ciscoasa(config-router)# is-type level-1
```

```
ciscoasa(config-router)# authentication send-only level-1
ciscoasa(config-router)# authentication key-chain site1 level-1
```

関連コマンド

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

コマンド	説明
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。

コマンド	説明
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト（TLV）を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
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。

コマンド	説明
summary-address	IS-IS の集約アドレスを作成します。

authentication-attr-from-server

二重認証がイネーブルになっている場合に、接続に適用する認証サーバーの認可属性を指定するには、トンネルグループ一般属性モードで **authentication-attr-from-server** コマンドを使用します。コンフィギュレーションから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。

authentication-attr-from-server { **primary** | **secondary** }
no authentication-attr-from-server

構文の説明

primary	プライマリ認証サーバーを使用します。
secondary	セカンダリ認証サーバーを使用します。

コマンド デフォルト

デフォルト値は **primary** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
トンネル グループ一般属性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
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、二重認証がイネーブルになっている場合に限り有効です。**authentication-attr-from-server** コマンドは、ASA が接続に適用する認可属性を抽出する認証サーバーを選択します。

例

次に、グローバル コンフィギュレーション モードで、remotegrp という名前の IPsec リモート アクセス トンネル グループを作成し、接続に適用する認可属性をセカンダリ認証サーバーから入手する必要があることを指定する例を示します。

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp general-attributes
```

```
ciscoasa(config-tunnel-webvpn)# authentication-attr-from-server secondary
ciscoasa(config-tunnel-webvpn)#
```

関連コマンド

コマンド	説明
pre-fill-username	ユーザー名の事前入力機能をイネーブルにします。
show running-config tunnel-group	指定されたトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般属性を指定します。
username-from-certificate	認可時のユーザー名として使用する証明書内のフィールドを指定します。

authentication-certificate

接続を確立している WebVPN クライアントから証明書を要求するには、webvpn コンフィギュレーション モードで **authentication-certificate** コマンドを使用します。クライアント証明書の要求をキャンセルするには、このコマンドの **no** 形式を使用します。

authentication-certificate *interface-name*
no authentication-certificate [*interface-name*]

構文の説明

interface-name 接続を確立するために使用するインターフェイスの名前。使用可能なインターフェイス名は、次のとおりです。

- **inside** インターフェイス GigabitEthernet0/1 の名前
- **outside** インターフェイス GigabitEthernet0/0 の名前

コマンド デフォルト

authentication-certificate コマンドを省略すると、クライアント証明書認証はディセーブルになります。インターフェイス名を **authentication-certificate** コマンドで指定しない場合、デフォルトのインターフェイス名は **inside** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

このコマンドを有効にするには、WebVPN が対応するインターフェイスですでに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設定して名前を付けるには、**interface**、**IP address**、および **nameif** コマンドを使用します。

このコマンドは、WebVPN クライアント接続にのみ適用されます。ただし、管理接続のクライアント証明書認証を **http authentication-certificate** コマンドを使用して指定することは、WebVPN をサポートしないものも含めてすべてのプラットフォームで可能です。

ASAは、PKIトラストポイントを使用して証明書を検証します。証明書が検証に合格しない場合、次のいずれかのアクションが実行されます。

条件	実行されるアクション
ASA に組み込まれているローカル CA がイネーブルでない場合。	ASA は SSL 接続を閉じます。
ローカル CA はイネーブルであるが、AAA 認証がイネーブルでない場合。	ASA は証明書を取得するために、クライアントをローカルCAの証明書登録ページにリダイレクトします。
ローカルCA と AAA 認証の両方がイネーブルの場合。	クライアントは AAA 認証ページにリダイレクトされます。設定されている場合、ローカルCA の登録ページのリンクもクライアントに表示します。

例

次に、外部インターフェイスの WebVPN ユーザー接続の証明書認証を設定する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# authentication-certificate outside
ciscoasa(config-webvpn)#
```

関連コマンド

コマンド	説明
authentication (tunnel-group webvpn configuration mode)	トンネル グループのメンバーが認証にデジタル証明書を使用する必要があることを指定します。
http authentication-certificate	ASA への ASDM 管理接続に証明書による認証を指定します。
interface	接続を確立するために使用するインターフェイスを設定します
show running-config ssl	現在設定されている一連の SSL コマンドを表示します。
ssl trust-point	SSL 証明書トラストポイントを設定します。

authentication-exclude

エンドユーザーがクライアントレス SSL VPN にログインせずに設定済みリンクを参照できるようにするには、webvpn コンフィギュレーション モードで **authentication-exclude** コマンドを使用します。複数のサイトへのアクセスを許可するには、このコマンドを複数回使用します。

authentication-exclude *url-fnmatch*

構文の説明

url-fnmatch	クライアントレス SSL VPN へのログインの要件を免除するリンクを指定します。

コマンド デフォルト

ディセーブル

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
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

この機能は、一部の内部リソースを SSL VPN 経由で一般利用できるようにする場合に便利です。

リンクに関する情報を、SSL VPN マングリングした形式でエンド ユーザーに配布する必要があります。たとえば、SSL VPN を使用してこれらのリソースを参照し、配布するリンクに関する情報に結果の URL をコピーします。

例

次に、2 つのサイトに対して認証要件を免除する例を示します。

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 authentication-exclude http://www.example.com/public/*
ciscoasa
(config-webvpn)#
authentication-exclude *example.html
```

```
ciscoasa
(config-webvpn)#
ciscoasa
 #
```

authentication-port

特定のホストのRADIUS認証に使用するポート番号を指定するには、AAAサーバーホストコンフィギュレーション モードで **authentication-port** コマンドを使用します。認証ポート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。

authentication-port *port*
no authentication-port

構文の説明

port RADIUS認証用のポート番号（1～65535）。

コマンド デフォルト

デフォルトでは、デバイスはポート1645でRADIUSをリッスンします（RFC 2058に準拠）。ポートが指定されていない場合、RADIUS認証のデフォルト ポート番号1645が使用されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
AAAサーバーホスト 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)	このコマンドのセマンティックが変更され、RADIUS サーバーを含むサーバー グループでホストごとにサーバー ポートを指定できるようになりました。

使用上のガイドライン

このコマンドは、認証機能の割り当て先となるリモートRADIUS サーバー ホストの宛先TCP/UDP ポート番号を指定します。RADIUS 認証サーバーで1645以外のポートが使用されている場合は、**aaa-server** コマンドでRADIUS サービスを開始する前に、適切なポートをASAに設定する必要があります。

このコマンドは、RADIUS用に設定されているサーバー グループに限り有効です。

例

次に、ホスト「1.2.3.4」に「srvgrp1」というRADIUS AAAサーバーを設定し、タイムアウトを9秒、再試行間隔を7秒、さらに認証ポートを1650に設定する例を示します。

```
ciscoasa
```

```
(config)# aaa-server svrgrp1 protocol radius
ciscoasa
(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# timeout 9
ciscoasa
(config-aaa-server-host)# retry-interval 7
ciscoasa
(config-aaa-server-host)#
authentication-port 1650
ciscoasa
(config-aaa-server-host)#
exit
ciscoasa
(config)#
```

関連コマンド

コマンド	説明
aaa authentication	aaa-server コマンドまたは ASDM ユーザー認証により指定されたサーバー上の LOCAL、TACACS+、または RADIUS ユーザー認証をイネーブルまたはディセーブルにします。
aaa-server host	AAA サーバー ホスト 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、ホストに固有の AAA サーバーパラメータを設定できます。
clear configure aaa-server	すべての AAA コマンド ステートメントをコンフィギュレーションから削除します。
show running-config aaa-server	すべての AAA サーバー、特定のサーバー グループ、特定のグループ内の特定のサーバー、または特定のプロトコルの AAA サーバー統計情報を表示します。

authentication-server-group（imap4s、pop3s、smtps）（廃止）

（注） このコマンドをサポートする最後のリリースは、Version 9.5(1) でした。

電子メールプロキシに使用する認証サーバーのセットを指定するには、各モードで **authentication-server-group** コマンドを使用します。認証サーバー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。

authentication-server-group *group_tag*
no authentication-server-group

構文の説明

group_tag 事前に設定済みの認証サーバーまたはサーバー グループを指定します。

コマンド デフォルト

デフォルトでは、認証サーバーは設定されていません。

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。

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
Imap4s コンフィギュレーション	• 対応	—	• 対応	—	—
Pop3s コンフィギュレーション	• 対応	—	• 対応	—	—
smtps 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。
9.5(2)	このコマンドは廃止されました。

使用上のガイドライン

ASA は、ユーザーを認証してユーザー ID を確認します。

AAA 認証を設定する場合は、この属性も設定する必要があります。設定しないと、認証は常に失敗します。

認証サーバーを設定するには、**aaa-server** コマンドを使用します。

例

次に、「IMAP4SSVRS」という名前の認証サーバーのセットを使用するようにIMAP4S 電子メール プロキシを設定する例を示します。

```
ciscoasa
(config)#
 imap4s
ciscoasa(config-imap4s)# authentication-server-group IMAP4SSVRS
```

関連コマンド

コマンド	説明
aaa-server host	認証、許可、およびアカウンティング サーバーを設定します。

authentication-server-group（トンネル グループ一般属性）

トンネルグループでユーザー認証に使用する AAA サーバーグループを指定するには、トンネルグループ一般属性コンフィギュレーション モードで **authentication-server-group** コマンドを使用します。この属性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。

authentication-server-group [(*interface_name*)] *server_group* [**LOCAL**]
authentication-server-group [(*interface_name*)] *server_group*

構文の説明

interface_name	（オプション）IPsec トンネルが終端するインターフェイスを指定します。
LOCAL	（オプション）通信障害によりサーバー グループにあるすべてのサーバーが非アクティブになった場合に、ローカル ユーザー データベースを使用した認証を要求します。
server_group	事前に設定済みの認証サーバーまたはサーバー グループを指定します。

コマンド デフォルト

このコマンドのサーバーグループのデフォルト設定は **LOCAL** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
トンネル グループ一般属性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。
7.1(1)	このコマンドは、webvpn コンフィギュレーション モードでは廃止され、トンネル グループ一般属性コンフィギュレーション モードに移動されました。
8.0(2)	このコマンドは、インターフェイス単位で IPsec 接続の認証を行えるように拡張されました。

使用上のガイドライン

この属性は、すべてのトンネル グループ タイプに適用できます。

認証サーバーを設定するには **aaa-server** コマンドを使用し、設定済みの AAA サーバーグループにサーバーを追加するには **aaa-server-host** コマンドを使用します。

例

次に、設定一般コンフィギュレーション モードで、remotegrp という名前の IPsec リモート アクセス トンネル グループに aaa-server456 という名前の認証サーバー グループを設定する例を示します。

```
ciscoasa(config)# tunnel-group remotegrp type ipsec-ra
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-general)# authentication-server-group aaa-server456
ciscoasa(config-tunnel-general)#
```

関連コマンド

コマンド	説明
aaa-server	AAA サーバー グループを作成し、グループ固有の AAA サーバー パラメータとすべてのグループ ホストに共通の AAA サーバー パラメータを設定します。
aaa-server host	設定済みの AAA サーバー グループにサーバーを追加し、ホスト固有の AAA サーバー パラメータを設定します。
clear configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。

authorization-required

接続前にユーザーが正常に認可されることを求めるには、各モードで **authorization-required** コマンドを使用します。コンフィギュレーションから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。

authorization-required
no authorization-required

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

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。

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
Imap4s コンフィギュレーション	• 対応	—	• 対応	—	—
Pop3s コンフィギュレーション	• 対応	—	• 対応	—	—
smtps コンフィギュレーション	• 対応	—	• 対応	—	—
トンネル グループ一般属性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。
7.1(1)	このコマンドは、webvpn コンフィギュレーション モードでは廃止され、トンネル グループ一般属性コンフィギュレーション モードに移動されました。

リリース	変更内容
7.2(1)	webvpn コンフィギュレーション モードが imap4s、pop3s、および smtps コンフィギュレーション モードに置き換えられました。
9.5(2)	このコマンドは、imap4s モード、pop3s モード、および smtps モードについては廃止されました。

例

次に、remotegrp という名前のリモート アクセス トンネル グループを介して接続するユーザーに、完全なDNに基づく認可を要求する例を示します。最初のコマンドでは、remotegrp という名前のリモート グループのトンネル グループ タイプを ipsec_ra（IPsec リモート アクセス）と設定しています。2 番目のコマンドで、指定したトンネル グループのトンネル グループ一般属性コンフィギュレーション モードを開始し、最後のコマンドで、指定したトンネル グループに認可が必要であることを指定しています。

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-general)# authorization-required
ciscoasa(config-tunnel-general)#
```

関連コマンド

コマンド	説明
authorization-dn-attributes	認可用のユーザー名として使用するプライマリおよびセカンダリ サブジェクト DN フィールドを指定します。
clear configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel-group	指定した証明書マップ エントリを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般属性を指定します。

authorization-server-group（imap4s、pop3s、smtps）（廃止）

（注） このコマンドをサポートする最後のリリースは、Version 9.5(1) でした。

すべてのリモートアクセス VPN のトンネルグループに使用する認可サーバーのセットを指定するには、各モードで **authorization-server-group** コマンドを使用します。認可サーバー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。

authorization-server-group *group_tag*
no authorization-server-group

構文の説明

group_tag 設定済みの認可サーバーまたはサーバー グループを指定します。認可サーバーを設定するには、**aaa-server** コマンドを使用します。

コマンド デフォルト

デフォルトでは、認可サーバーは設定されていません。

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。

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
Imap4s コンフィギュレーション	• 対応	—	• 対応	—	—
Pop3s コンフィギュレーション	• 対応	—	• 対応	—	—
smtps 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。

リリース	変更内容
7.1(1)	このコマンドは、webvpn コンフィギュレーション モードでは廃止され、トンネル グループ一般属性コンフィギュレーション モードに移動されました。
9.5(2)	このコマンドは廃止されました。

使用上のガイドライン

ASA では、認可を使用して、ユーザーに許可されているネットワークリソースへのアクセスレベルを確認します。**aaa-server** コマンドで使用する認可用のサーバー設定を使用します。

このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ一般属性モードの同等のコマンドに変換されます。

VPN 認可が LOCAL と定義されている場合、デフォルト グループ ポリシー DfltGrpPolicy に設定されている属性が適用されます。

例

次に、「POP3Spermit」という名前の許可サーバーのセットを使用するように POP3S 電子メール プロキシを設定する例を示します。

```
ciscoasa
(config)#
 pop3s
ciscoasa(config-pop3s)# authorization-server-group POP3Spermit
```

関連コマンド

コマンド	説明
aaa-server host	認証、許可、およびアカウンティング サーバーを設定します。
clear configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般属性を指定します。

authorization-server-group（トンネル グループ一般属性）

すべてのリモートアクセス VPN のトンネルグループに使用する認可サーバーのセットを指定するには、各モードで **authorization-server-group** コマンドを使用します。認可サーバー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。

authorization-server-group [（ *if_name* ）] *group_tag*
no authorization-server-group

構文の説明

group_tag	設定済みの認可サーバーまたはサーバー グループを指定します。認可サーバーを設定するには、**aaa-server** コマンドを使用します。
(*if_name*)	（任意）トンネルが終了するインターフェイスの名前。カッコを含める必要があります。

コマンド デフォルト

デフォルトでは、認可サーバーは設定されていません。

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。

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
トンネル グループ一般属性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。
7.1(1)	このコマンドは、webvpn コンフィギュレーション モードでは廃止され、トンネル グループ一般属性コンフィギュレーション モードに移動されました。

使用上のガイドライン

ASA では、認可を使用して、ユーザーに許可されているネットワークリソースへのアクセスレベルを確認します。aaa-server コマンドで使用する認可用のサーバー設定を使用します。

このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ一般属性モードの同等のコマンドに変換されます。

VPN 認可が LOCAL と定義されている場合、デフォルト グループ ポリシー DfltGrpPolicy に設定されている属性が適用されます。

例

次に、トンネル一般コンフィギュレーション モードで、「remotegrp」という名前の IPsec リモート アクセス トンネル グループに「aaa-server78」という名前の認可サーバー グループを設定する例を示します。

```
ciscoasa(config)# tunnel-group remotegrp type ipsec-ra
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-general)# authorization-server-group aaa-server78
ciscoasa(config-tunnel-general)#
```

関連コマンド

コマンド	説明
aaa-server host	認証、許可、およびアカウンティング サーバーを設定します。
clear configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般属性を指定します。

authorize-only

RADIUS AAA サーバーグループに対して authorize-only モードをイネーブルにするには、AAA サーバー グループ コンフィギュレーション モードで **authorize-only** コマンドを使用します。authorize-only モード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。

authorize-only
no authorize-only

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

authorize-only モードはイネーブルになっていません。

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		
	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
aaa サーバー 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)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、ISE 認可変更（CoA）のために RADIUS サーバー グループを authorize-only モードで設定するために使用します。authorize-only モードを使用すると、RADIUS ホスト用に設定された RADIUS 共通パスワードはすべて無視されます。

ISE Change of Authorization（CoA）機能は、認証、認可、およびアカウンティング（AAA）セッションの属性を、セッション確立後に変更するためのメカニズムを提供します。AAA のユーザーまたはユーザー グループのポリシーを変更すると、ISE から ASA へ CoA パケットを直接送信して認証を再初期化し、新しいポリシーを適用できます。インライン ポスチャ実施ポイント（IPEP）で、ASA と確立された各 VPN セッションのアクセス コントロール リスト（ACL）を適用する必要がなくなりました。

エンド ユーザーが VPN 接続を要求すると、ASA はユーザーに対して ISE 認証を実行し、ネットワークへの制限付きアクセスを提供する ACL を受領します。アカウンティング開始メッセージが ISE に送信され、セッションが登録されます。ポスチャ アセスメントが NAC エージェントと ISE 間で直接行われます。このプロセスは、ASA に透過的です。ISE が CoA の「ポリシー

プッシュ」を介して ASA にポリシーの更新を送信します。これにより、ネットワーク アクセス権限を高める新しいユーザー ACL が識別されます。後続の CoA 更新を介し、接続のライフタイム中に追加のポリシー評価が ASA に透過的に行われる場合があります。

例

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。サーバー グループは認証用に使用されないため、**authorize-only** コマンドをサーバー 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
dynamic-authorization	RADIUS サーバー グループ用のダイナミック認可をイネーブルにします。
interim-accounting-update	RADIUS 中間アカウンティング アップデート メッセージの生成をイネーブルにします。
without-csd	特定のトンネル グループに行われる接続のホストスキャン処理をオフに切り替えます。

auth-prompt

ASA を介したユーザーセッションの AAA チャレンジテキストを指定または変更するには、グローバル コンフィギュレーション モードで **auth-prompt** コマンドを使用します。認証チャレンジテキストを削除するには、このコマンドの **no** 形式を使用します。

auth-prompt prompt [**prompt** | **accept** | **reject**] *string*
no auth-prompt prompt [**prompt** | **accept** | **reject**]

構文の説明

accept	Telnet 経由のユーザー認証を受け入れる場合、プロンプトとして string を表示します。
prompt	このキーワードの後に AAA チャレンジ プロンプトのストリングを入力します。
reject	Telnet 経由のユーザー認証を拒否する場合、プロンプトとして string を表示します。
string	最大 235 文字の英数字または 31 単語のストリング。最初に達した、いずれかの最大数により制限されます。特殊文字、スペース、および句読点を使用できます。疑問符を入力するか、または Enter キーを押すと、ストリングが終了します（疑問符はストリングに含まれます）。

コマンド デフォルト

認証プロンプトを指定しない場合は、次のようになります。

- FTP ユーザーには FTP authentication が表示されます。
- HTTP ユーザーには HTTP Authentication が表示されます。
- Telnet ユーザーにはチャレンジ テキストが表示されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
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
7.0(1)	セマンティックに小さな変更が加えられました。

使用上のガイドライン

auth-prompt コマンドを使用すると、TACACS+ サーバーまたは RADIUS サーバーからのユーザー認証が必要な場合に、ASA 経由の HTTP、FTP、および Telnet アクセス用の AAA チャレンジテキストを指定できます。このテキストは飾りのようなもので、ユーザーのログイン時に、ユーザー名プロンプトとパスワード プロンプトの上に表示されます。

Telnetからのユーザー認証が行われる場合、acceptオプションとrejectオプションを使用して、認証試行が AAA サーバーによって受け入れられたか拒否されたかを示す各ステータス プロンプトを表示できます。

AAA サーバーがユーザーを認証すると、ASA は auth-prompt accept テキスト（指定されている場合）をユーザーに表示します。ユーザーが認証されない場合は、reject テキスト（指定されている場合）を表示します。HTTP セッションおよびFTP セッションの認証では、プロンプトにチャレンジ テキストのみが表示されます。accept および reject テキストは表示されません。

（注） Microsoft Internet Explorer では、認証プロンプトに最大 37 文字表示されます。Telnet および FTP では、認証プロンプトに最大 235 文字表示されます。

例

次に、認証プロンプトを「Please enter your username and password」という文字列に設定する例を示します。

```
ciscoasa(config)# auth
-prompt prompt Please enter your username and password
```

このストリングがコンフィギュレーションに追加されると、ユーザーには次のように表示されます。

```
Please enter your username and password
User Name:
Password:
```

Telnet ユーザーに対しては、ASA が認証試行を受け入れたときに表示されるメッセージと拒否したときに表示されるメッセージを別々に指定できます。次に例を示します。

```
ciscoasa(config)# auth-prompt reject Authentication failed. Try again.
ciscoasa(config)# auth-prompt accept Authentication succeeded.
```

次に、認証に成功した場合の認証プロンプトを「You'reOK.」という文字列に設定する例を示します。

```
ciscoasa(config)# auth-prompt accept You’re OK.
```

認証に成功すると、ユーザーには次のメッセージが表示されます。

```
You’re OK.
```

関連コマンド

コマンド	説明
clear configure auth-prompt	指定済みの認証プロンプトチャレンジテキスト（ある場合）を削除し、デフォルト値に戻します。
show running-config auth-prompt	現在の認証プロンプト チャレンジ テキストを表示します。

auto-signon

クライアントレス SSL VPN 接続用のユーザー ログイン クレデンシャルを内部サーバーに自動的に渡すように ASA を設定するには、webvpn コンフィギュレーション モード、webvpn グループ コンフィギュレーション モード、または webvpn ユーザー名コンフィギュレーション モードのいずれかのモードで **auto-signon** コマンドを使用します。特定のサーバーへの自動サインオンをディセーブルにするには、元の **ip**、**uri**、および **auth-type** 引数を指定して、このコマンドの **no** 形式を使用します。すべてのサーバーへの自動サインオンをディセーブルにするには、このコマンドの **no** 形式を引数なしで使用します。

auto-signon allow { **ip** *ip-address ip-mask* | **uri** *resource-mask* } **auth-type** { **basic** | **ftp** | **ntlm** | **all** }
no auto-signon [**allow** { **ip** *ip-address ip-mask* | **uri** *resource-mask* } **auth-type** { **basic** | **ftp** | **ntlm** | **all** }]

構文の説明

all	NTLM と HTTP 基本認証の両方の方式を指定します。
allow	特定のサーバーに対する認証をイネーブルにします。
auth-type	認証方式の選択をイネーブルにします。
basic	HTTP 基本認証方式を指定します。
ftp	FTP および CIFS 認証タイプ。
ip	IP アドレスとマスクで認証先のサーバーを特定することを指定します。
ip-address	*ip-mask* とともに使用して、認証先のサーバーの IP アドレス範囲を特定します。
ip-mask	*ip-address* とともに使用して、認証先のサーバーの IP アドレス範囲を特定します。
ntlm	NTLMv1 認証方式を指定します。
resource-mask	認証先のサーバーの URI マスクを指定します。
uri	URI マスクで認証先のサーバーを特定することを指定します。

コマンド デフォルト

デフォルトでは、この機能はすべてのサーバー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。

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
webvpn コンフィギュレーション（グローバル）	• 対応	—	• 対応	—	—
webvpn グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—
WebVPN ユーザー名コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。
8.0(1)	NTLMv2 のサポートが追加されました。**ntlm** キーワードには NTLMv1 と NTLMv2 の両方が含まれます。

使用上のガイドライン

auto-signon コマンドは、クライアントレス SSL VPN ユーザーのためのシングル インオン方式です。この方式では、ログイン クレデンシャル（ユーザー名とパスワード）を NTLM 認証と HTTP 基本認証のいずれか一方または両方を使用する認証用の内部サーバーに渡します。複数の auto-signon コマンドを入力でき、それらのコマンドは入力順に処理されます（先に入力したコマンドが優先されます）。

auto-signon 機能は、webvpn コンフィギュレーション グループ ポリシー モード、webvpn コンフィギュレーション モード、または webvpn ユーザー名コンフィギュレーション モードの 3 つのモードで使用できます。一般的な優先動作が適用されます。つまり、グループよりもユーザー名が優先され、グローバルよりもグループが優先されます。モードは、認証の目的範囲に基づいて選択します。

モード	スコープ
webvpn コンフィギュレーション	すべての WebVPN ユーザー（グローバル）
webvpn グループ コンフィギュレーション	グループ ポリシーで定義される WebVPN ユーザーのサブセット

モード	スコープ
WebVPNユーザー名コンフィギュレーション	個々の WebVPN ユーザー

例

次に、NTLM認証を使用して、すべてのクライアントレス ユーザーに自動サインオンを設定する例を示します。認証先のサーバーのIPアドレス範囲は、10.1.1.0 ～ 10.1.1.255です。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# auto-signon allow ip 10.1.1.0
 255.255.255.0
 auth-type ntlm
```

次に、HTTP 基本認証を使用して、すべてのクライアントレス ユーザーに自動サインオンを設定する例を示します。認証先のサーバーは、URIマスク https://*.example.com/* で定義されています。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# auto-signon allow uri https://*.example.com/* auth-type basic
The following example configures auto-signon for clientless users ExamplePolicy group
policy, using either HTTP Basic or NTLM authentication, to servers defined by the URI
mask https://*.example.com/*:
ciscoasa(config)# group-policy ExamplePolicy attributes

ciscoasa(config-group-policy)# webvpn

ciscoasa(config-group-webvpn)# auto-signon allow uri https://*.example.com/* auth-type
all
```

次に、HTTP基本認証を使用して、Anyuserという名前のユーザーに自動サインオンを設定する例を示します。認証先のサーバーのIPアドレス範囲は、10.1.1.0 ～ 10.1.1.255です。

```
ciscoasa(config)# username Anyuser attributes
ciscoasa(config-username)# webvpn
ciscoasa(config-username-webvpn)# auto-signon allow ip 10.1.1.0
 255.255.255.0
 auth-type basic
```

関連コマンド

コマンド	説明
show running-config webvpn auto-signon	実行コンフィギュレーションの自動サインオンの割り当てを表示します。

auto-summary

ネットワークレベルルートへのサブネットルートの自動集約をイネーブルにするには、ルータコンフィギュレーション モードで **auto-summary** コマンドを使用します。ルート集約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。

auto-summary
no auto-summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

ルート集約は、RIP バージョン 1、RIP バージョン 2、および EIGRP で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。

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
ルータ 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。
8.0(2)	EIGRP のサポートが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

ルート集約により、ルーティング テーブルにおけるルーティング情報の量が少なくなります。

RIP バージョン 1 では、常に自動集約が使用されます。RIP バージョン 1 に対して自動集約をディセーブルにすることはできません。

RIP バージョン 2 を使用している場合は、**no auto-summary** コマンドを指定して、自動集約をオフにすることができます。切断されているサブネット間のルーティングを実行する必要がある場合は、自動サマライズを無効にします。自動サマライズを無効にすると、サブネットがアドバタイズされます。

EIGRP 集約ルートには、アドミニストレーティブ ディスタンス値 5 が割り当てられます。この値は設定できません。

実行コンフィギュレーションではこのコマンドの **no** 形式のみが表示されます。

例

次に、RIP ルート集約をディセーブルにする例を示します。

```
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# version 2
ciscoasa(config-router)# no auto-summary
```

次に、自動 EIGRP ルート集約をディセーブルにする例を示します。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# no auto-summary
```

関連コマンド

コマンド	説明
clear configure router	実行コンフィギュレーションからすべての **router** コマンドとルータ コンフィギュレーション モード コマンドをクリアします。
router eigrp	EIGRP ルーティング プロセスをイネーブルにし、EIGRP ルータ コンフィギュレーション モードを開始します。
router rip	RIP ルーティング プロセスをイネーブルにし、RIP ルータ コンフィギュレーション モードを開始します。
show running-config router	実行コンフィギュレーション内の **router** コマンドとルータ コンフィギュレーション モード コマンドを表示します。

auto-update device-id

Auto Update Server で使用する ASA のデバイス ID 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 **auto-update device-id** コマンドを使用します。デバイス ID を削除するには、このコマンドの **no** 形式を使用します。

auto-update device-id [**hardware-serial** | **hostname** | **ipaddress** | [*if_name*] | **mac-address** [*if_name*] | **string** *text*]
no auto-update device-id [**hardware-serial** | **hostname** | **ipaddress** | [*if_name*] | **mac-address** [*if_name*] | **string** *text*]

構文の説明

hardware-serial	ASA のハードウェアシリアル番号を使用して、デバイスを一意に識別します。
hostname	ASA のホスト名を使用して、デバイスを一意に識別します。
ipaddress [*if_name*]	ASA の IP アドレスを使用して、ASA を一意に識別します。デフォルトでは、ASA は Auto Update Server との通信に使用するインターフェイスを使用します。別の IP アドレスを使用する場合は、*if_name* オプションを指定します。
mac-address [*if_name*]	ASA の MAC アドレスを使用して、ASA を一意に識別します。デフォルトでは、ASA は Auto Update Server との通信に使用するインターフェイスの MAC アドレスを使用します。別の MAC アドレスを使用する場合は、*if_name* オプションを指定します。
string *text*	テキスト ストリングを指定して、デバイスを Auto Update Server に対して一意に識別します。

コマンド デフォルト

デフォルト ID はホスト名です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

例

次に、デバイス ID をシリアル番号に設定する例を示します。

```
ciscoasa(config)# auto-update device-id hardware-serial
```

関連コマンド

auto-update poll-period	Auto Update Server からのアップデートを ASA が確認する頻度を設定します。
auto-update server	Auto Update Server を指定します。
auto-update timeout	タイムアウト期間内に Auto Update Server に接続されない場合、ASA を通過するトラフィックを停止します。
clear configure auto-update	Auto Update Server コンフィギュレーションをクリアします。
show running-config auto-update	Auto Update Server コンフィギュレーションを表示します。

auto-update poll-at

ASA が Auto Update Server をポーリングする特定の日時をスケジューリングするには、グローバル コンフィギュレーション モードで **auto-update poll-at** コマンドを使用します。ASA が Auto Update Server をポーリングするようにスケジューリングした日時のうち、指定した日時をすべて削除するには、このコマンドの **no** 形式を使用します。

auto-update poll-at *days-of-the-week time* ［ **randomize** *minutes* ［ *retry_count* ［ *retry_period* ］］
no auto-update poll-at *days-of-the-week time* ［ **randomize** *minutes* ［ *retry_count* ［ *retry_period* ］］

構文の説明

days-of-the-week	任意の 1 つの曜日（Monday、Tuesday、Wednesday、Thursday、Friday、Saturday、および Sunday）または曜日の組み合わせ。その他の指定可能な値は、daily（月曜日から日曜日まで）、weekdays（月曜日から金曜日まで）、および weekend（土曜日と日曜日）です。
randomize >*minutes*	指定した開始日時の後に、不定期にポーリングする期間を 1 ～ 1,439 分で指定します。
>*retry_count*	Auto Update Server への接続の初回試行が失敗した場合に、再接続を何回試行するかを指定します。デフォルトは 0 です。
>*retry_period*	接続試行の間隔を指定します。デフォルトは 5 分です。指定できる範囲は 1 ～ 35791 分です。
>*time*	ポーリングを開始する時刻を HH:MM 形式で指定します。たとえば、8:00 は午前 8 時で、20:00 は午後 8 時です。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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

auto-update poll-at コマンドでは、アップデートをポーリングする時刻を指定します。**randomize** オプションをイネーブルにすると、最初の *>time* オプションの時刻から指定した期間（分単位）内に、ポーリングが不定期に実行されます。**auto-update poll-at** および **auto-update poll-period** コマンドは、同時に使用できません。いずれか 1 つのみを設定できます。

例

次の例では、ASA は、毎週金曜日と土曜日の午後 10 時から午後 11 時までの間、不定期に Auto Update Server をポーリングします。ASA がサーバーに接続できない場合は、10 分おきにさらに 2 回、接続を試行します。

```
ciscoasa(config)# auto-update poll-at Friday Saturday 22:00 randomize 60 2 10
ciscoasa(config)# auto-update server http://192.168.1.114/aus/autoupdate.asp
```

関連コマンド

auto-update device-id	Auto Update Server で使用するための ASA デバイス ID を設定します。
auto-update poll-period	Auto Update Server からのアップデートを ASA が確認する頻度を設定します。
auto-update timeout	タイムアウト期間内に Auto Update Server に接続されない場合、ASA を通過するトラフィックを停止します。
clear configure auto-update	Auto Update Server コンフィギュレーションをクリアします。
management-access	ASA の内部管理インターフェイスへのアクセスをイネーブルにします。
show running-config auto-update	Auto Update Server コンフィギュレーションを表示します。

auto-update poll-period

ASA が Auto Update Server からのアップデートを確認する頻度を設定するには、グローバル コンフィギュレーション モードで **auto-update poll-period** コマンドを使用します。パラメータをデフォルト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。

auto-update poll-period *poll_period* [*retry_count* [*retry_period*]]
no auto-update poll-period *poll_period* [*retry_count* [*retry_period*]]

構文の説明

poll_period	Auto Update Server をポーリングする頻度を分単位（1 ～ 35791）で指定します。デフォルトは 720 分（12 時間）です。
retry_count	Auto Update Server への接続の初回試行が失敗した場合に、再接続を何回試行するかを指定します。デフォルトは 0 です。
retry_period	接続試行の間隔を分単位（1 ～ 35791）で指定します。デフォルトは 5 分です。

コマンド デフォルト

デフォルトのポーリング期間は、720 分（12 時間）です。

Auto Update Server への最初の接続試行に失敗した場合に再接続を試行するデフォルトの回数は 0 です。

接続試行のデフォルト間隔は 5 分です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

auto-update poll-at および **auto-update poll-period** コマンドは、同時に使用できません。いずれか 1 つのみを設定できます。

例

次に、ポーリング期間を 360 分に、再試行回数を 1 回に、再試行間隔を 3 分に設定する例を示します。

```
ciscoasa(config)# auto-update poll-period 360 1 3
```

関連コマンド

auto-update device-id	Auto Update Server で使用するための ASA デバイス ID を設定します。
auto-update server	Auto Update Server を指定します。
auto-update timeout	タイムアウト期間内に Auto Update Server に接続されない場合、ASA を通過するトラフィックを停止します。
clear configure auto-update	Auto Update Server コンフィギュレーションをクリアします。
show running-config auto-update	Auto Update Server コンフィギュレーションを表示します。

auto-update server

Auto Update Server を指定するには、グローバル コンフィギュレーション モードで **auto-update server** コマンドを使用します。サーバーを削除するには、このコマンドの **no** 形式を使用します。

auto-update server *url* ［ **source** *interface* ］{ **verify-certificate** | **no-verification** }
no auto-update server *url* ［ **source** *interface* ］{ **verify-certificate** | **no-verification** }

構文の説明

no-verification	Auto Update Server 証明書を確認しません。
source *interface*	要求を Auto Update Server に送信するときに使用するインターフェイスを指定します。**management-access** コマンドで指定したインターフェイスと同じインターフェイスを指定すると、Auto Update 要求は管理アクセスに使用されるのと同じ IPsec VPN トンネルを通過します。
url	次の構文を使用して、Auto Update Server の場所を指定します。 **https:**[[*user:password@location* [:*port*]] */pathname*
verify-certificate	HTTPS の場合、Auto Update Server から返された証明書を確認します。この設定は、デフォルトです。

コマンド デフォルト

9.1 以前：証明書の確認はディセーブルになっています。

9.2(1) 以降：**verify-certificate** オプションはデフォルトで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。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(1)	複数のサーバーをサポートできるようにコマンドが変更されました。
9.2(1)	Auto Update Server 証明書の確認がデフォルトでイネーブルになりました。 **no-verification** キーワードが追加されました。

使用上のガイドライン

ASA は、定期的に Auto Update Server にアクセスして、コンフィギュレーション、オペレーティングシステム、および ASDM の更新がないか調べます。

自動アップデート用に複数のサーバーを設定できます。アップデートを確認するときに、最初のサーバーに接続しますが、接続に失敗した場合は、次のサーバーに接続します。このプロセスは、すべてのサーバーを試行するまで続行されます。どのサーバーにも接続できなかった場合は、auto-update poll-period が接続を再試行するように設定されていれば、最初のサーバーから順に接続が再試行されます。

自動アップデート機能を正しく動作させるには、**boot system configuration** コマンドを使用して、有効なブートイメージを指定する必要があります。また、ASDM ソフトウェアイメージを更新するには、auto-update とともに**asdm image** コマンドを使用する必要があります。

source *interface* 引数で指定されたインターフェイスが **management-access** コマンドで指定されたインターフェイスと同じである場合、Auto Update Server への要求は VPN トンネルを介して送信されます。

9.2(1) 以降：Auto Update Server 証明書の確認がデフォルトでイネーブルになりました。新しい設定の場合、証明書の確認を明示的にディセーブルにする必要があります。証明書の確認をイネーブルにしていなかった場合に、以前のリリースからアップグレードしようとすると、証明書の確認はイネーブルではなく、次の警告が表示されます。

```
WARNING: The certificate provided by the auto-update servers will not be verified. In
order to verify this certificate please use the verify-certificate option.
```

設定を移行する場合は、次のように確認なしを明示的に設定します。

auto-update server no-verification

例

次に、Auto Update Server の URL を設定し、インターフェイスを outside として指定する例を示します。

```
ciscoasa(config)# auto-update server http://10.1.1.1:1741/ source outside
verify-certificate
```

関連コマンド

auto-update device-id	Auto Update Server で使用するための ASA デバイス ID を設定します。
auto-update poll-period	Auto Update Server からのアップデートを ASA が確認する頻度を設定します。
auto-update timeout	タイムアウト期間内に Auto Update Server に接続されない場合、ASA を通過するトラフィックを停止します。
clear configure auto-update	Auto Update Server コンフィギュレーションをクリアします。
management-access	ASA の内部管理インターフェイスへのアクセスをイネーブルにします。
show running-config auto-update	Auto Update Server コンフィギュレーションを表示します。

auto-update timeout

Auto Update Server へのアクセスのタイムアウト期間を設定するには、グローバル コンフィギュレーション モードで **auto-update timeout** コマンドを使用します。タイムアウトを削除するには、このコマンドの **no** 形式を使用します。

auto-update timeout [*period*]
no auto-update timeout [*period*]

構文の説明

period タイムアウト期間を分単位（1 ～ 35791）で指定します。デフォルトは 0 で、タイムアウトがないことを意味します。タイムアウトを 0 に設定することはできません。タイムアウトを 0 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。

コマンド デフォルト

デフォルトのタイムアウトは 0 で、ASA はタイムアウトしないよう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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
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

タイムアウト状態は、syslog メッセージ 201008 でレポートされます。

タイムアウト期間内に Auto Update Server へのアクセスが行われなかった場合、ASA はそれを通過するすべてのトラフィックを停止します。タイムアウトを設定すると、ASA に最新のイメージとコンフィギュレーションが保持されます。

例

次に、タイムアウトを 24 時間に設定する例を示します。

```
ciscoasa(config)# auto-update timeout 1440
```

関連コマンド

auto-update device-id	Auto Update Server で使用するための ASA デバイス ID を設定します。

auto-update poll-period	Auto Update Server からのアップデートを ASA が確認する頻度を設定します。
auto-update server	Auto Update Server を指定します。
clear configure auto-update	Auto Update Server コンフィギュレーションをクリアします。
show running-config auto-update	Auto Update Server コンフィギュレーションを表示します。

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