table-map through title

table-map

IP ルーティング テーブルが BGP で学習されたルートで更新された場合にメトリックおよびタグ値を変更するには、アドレス ファミリ コンフィギュレーション モードで **table-map** コマンドを使用します。この機能をディセーブルにするには、コマンドの **no** 形式を使用します。

table-map *map_name*

no table-map *map_name*

構文の説明

map_name	**route-map** コマンドのルート マップ名。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、**route-map** コマンドによって定義されたルート マップ名を IP ルーティング テーブルに追加します。このコマンドは、再配布を実装する目的でタグ名とルート メトリックを設定するために使用されます。

ルート マップの **match** 句を **table-map** コマンドで使用できます。IP アクセス リスト、自律システム パス、およびネクスト ホップの match 句がサポートされています。

例

次のアドレス ファミリ コンフィギュレーション モードの例では、ASA ソフトウェアは、BGP で学習されたルートのタグ値を自動的に計算し、IP ルーティング テーブルを更新するように設定されています。

```
ciscoasa(config)# route-map tag
ciscoasa(config-route-map)# match as path 10
ciscoasa(config-route-map)# set automatic-tag

ciscoasa(config)# router bgp 100
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# table-map tag
```

関連コマンド

コマンド	説明
address-family	アドレス ファミリ コンフィギュレーション モードを開始します。
ルート マップ	あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義します。

tcp-inspection

DNS over TCP インスペクションをイネーブルにするには、パラメータ コンフィギュレーション モードで **tcp-inspection** コマンドを使用します。プロトコルの強制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。

tcp-inspection

no tcp-inspection

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

DNS over TCP インスペクションはディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
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

このコマンドを DNS インスペクション ポリシー マップに追加して、DNS/TCP ポート 53 トラフィックをインスペクションに含めます。このコマンドを使用しなければ、UDP/53 DNS トラフィックのみが検査されます。DNS/TCP ポート 53 トラフィックが DNS インスペクションを適用するクラスに含まれていることを確認します。インスペクションのデフォルト クラスには、TCP/53 が含まれます。

例

次に、DNS インスペクション ポリシー マップで DNS over TCP インスペクションをイネーブルにする例を示します。

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# tcp-inspection
```

関連コマンド

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

tcp-map

一連の TCP 正規化アクションを定義するには、グローバル コンフィギュレーション モードで **tcp-map** コマンドを使用します。TCP 正規化機能によって、異常なパケットを識別する基準を指定できます。ASA は、異常なパケットが検出されるとそれらをドロップします。TCP マップを削除するには、このコマンドの **no** 形式を使用します。

tcp-map *map_name*

no tcp-map *map_name*

構文の説明

map_name	TCP マップ名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(4)/8.0(4)	**invalid-ack**、**seq-past-window**、および **synack-data** サブ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 モジュラ ポリシー フレームワーク を使用します。最初に、**tcp-map** コマンドを使用して実行する TCP 正規化アクションを定義します。**tcp-map** コマンドによって、tcp マップ コンフィギュレーション モードが開始されます。このモードで、1 つ以上のコマンドを入力して、TCP 正規化アクションを定義できます。その後、**class-map** コマンドを使用して、TCP マップを適用するトラフィックを定義します。**policy-map** コマンドを入力してポリシーを定義し、**class** コマンドを入力してクラス マップを参照します。クラス コンフィギュレーション モードで、**set connection advanced-options** コマンドを入力して TCP マップを参照します。最後に、**service-policy** コマンドを使用して、インターフェイスにポリシー マップを適用します。モジュラ ポリシー フレームワークの仕組みの詳細については、CLI 設定ガイドを参照してください。

次のコマンドは、tcp マップ コンフィギュレーション モードで使用可能です。

check-retransmission	再送信データのチェックをイネーブルまたはディセーブルにします。
checksum-verification	チェックサムの検証をイネーブルまたはディセーブルにします。
exceed-mss	ピアによって設定された MSS を超えるパケットを許可またはドロップします。
invalid-ack	無効な ACK を含むパケットに対するアクションを設定します。
queue-limit	TCP 接続のキューに入れることができる順序が不正なパケットの最大数を設定します。このコマンドは、ASA 5500 シリーズ ASA でのみ使用可能です。PIX 500 シリーズ ASA ではキュー制限は 3 で、この値は変更できません。
reserved-bits	ASA に予約済みフラグ ポリシーを設定します。
seq-past-window	パストウィンドウ シーケンス番号を含むパケットに対するアクションを設定します。つまり、受信した TCP パケットのシーケンス番号が、TCP 受信ウィンドウの右端より大きい場合です。
synack-data	データを含む TCP SYNACK パケットに対するアクションを設定します。
syn-data	データを持つ SYN パケットを許可またはドロップします。
tcp-options	TCP ヘッダーの TCP オプション フィールドの内容に基づいて、パケットのアクションを設定します。
ttl-evasion-protection	ASA によって提供された TTL 回避保護をイネーブルまたはディセーブルにします。
urgent-flag	ASA を通じて URG ポインタを許可またはクリアします。
window-variation	予期せずウィンドウ サイズが変更された接続をドロップします。

例

たとえば、既知の FTP データ ポートと Telnet ポートの間の TCP ポート範囲に送信されるすべてのトラフィックで緊急フラグと緊急オフセット パケットを許可するには、次のコマンドを入力します。

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# urgent-flag allow

ciscoasa(config-tcp-map)# class-map urg-class
ciscoasa(config-cmap)# match port tcp range ftp-data telnet

ciscoasa(config-cmap)# policy-map pmap
ciscoasa(config-pmap)# class urg-class
ciscoasa(config-pmap-c)# set connection advanced-options tmap

ciscoasa(config-pmap-c)# service-policy pmap global
```

関連コマンド

コマンド	説明
class（ポリシーマップ）	トラフィック分類に使用するクラス マップを指定します。
clear configure tcp-map	TCP マップのコンフィギュレーションをクリアします。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
show running-config tcp-map	TCP マップ コンフィギュレーションに関する情報を表示します。
tcp-options	selective-ack、timestamp、window-scale の各 TCP オプションを許可または消去します。

tcp-options

TCP ヘッダーの TCP オプションを許可またはクリアするには、TCP マップ コンフィギュレーション モードで **tcp-options** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

tcp-options {**md5** | **mss** | **selective-ack** | **timestamp** | **window-scale** | **range** *lower upper*} *action*

no tcp-options {**md5** | **mss** | **selective-ack** | **timestamp** | **window-scale** | **range** *lower upper*} *action*

構文の説明

アクション	オプションのために実行するアクションです。アクションは次のとおりです。 • **allow** [**multiple**]：オプションを含むパケットを許可します。9.6(2) 以降では、**allow** はこのタイプの単一のオプションを含むパケットを許可することを意味します。これは、すべての名前付きオプションのデフォルトです。オプションのインスタンスが複数含まれていてもパケットを許可する場合は、**multiple** キーワードを追加します。**multiple** キーワードは、**range** と一緒には使用できません。 • **maximum** *limit*：**mss** 専用。最大セグメント サイズを、示された制限（68 ～ 65535）に設定します。デフォルトの TCP MSS は、**sysopt connection tcpmss** コマンドで定義されます。 • **clear**：このタイプのオプションをヘッダーから削除して、パケットを許可します。これは、**range** キーワードで設定できるすべての番号付きオプションのデフォルトです。タイムスタンプ オプションを消去すると、PAWS と RTT がディセーブルになります。 • **drop**：このオプションを含むパケットをドロップします。このアクションは、**md5** および **range** だけで利用可能です。
md5	MD5 オプションのアクションを設定します。
mss	最大セグメント サイズ オプションのアクションを設定します。
range *lower upper*	範囲の下限および上限内の番号付きオプションのアクションで設定します。単一の番号付きオプションのアクションを設定するには、範囲の下限と上限に同じ数値を入力します。 （9.6(2) 以降）有効範囲は、6 ～ 7、9 ～ 18、および 20 ～ 255 以内です。 （9.6(1) 以降）有効範囲は、6 ～ 7 および 9 ～ 255 以内です。
selective-ack	選択的確認応答メカニズム（SACK）オプションのアクションを設定します。
timestamp	タイムスタンプ オプションのアクションを設定します。タイムスタンプ オプションをクリアすると、PAWS と RTT がディセーブルになります。
window-scale	ウィンドウ スケール メカニズム オプションのアクションを設定します。

デフォルト

(9.6(1) 以降)デフォルトでは、すべての名前付きオプションを許可し、オプション 6 ～ 7 および 9 ～ 255 をクリアします。

(9.6(2) 以降)デフォルトでは、名前付きオプションのそれぞれの 1 つのインスタンスを許可し、指定された名前付きオプションが複数あるパケットをドロップし、オプション 6 ～ 7、9 ～ 18、および 20 ～ 155 をクリアします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.6(2)	名前付きオプションのデフォルト処理は、指定されたタイプのオプションを 1 つ含む場合はパケットを許可し、そのタイプのオプションが複数ある場合はパケットをドロップするように変更されました。また、**md5**、**mss**、**allow multiple**、および **mss maximum** キーワードが追加されました。MD5 オプションのデフォルトは、クリアから許可に変更されました。

使用上のガイドライン

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

tcp-map コマンドを使用して、TCP マップ コンフィギュレーション モードを開始します。TCP マップ コンフィギュレーション モードで **tcp-options** コマンドを使用して、さまざまな TCP オプションを処理する方法を定義します。

例

次に、6 ～ 7 および 9 ～ 255 の範囲内の TCP オプションを持つすべてのパケットをドロップする例を示します。

```
ciscoasa(config)# access-list TCP extended permit tcp any any
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# tcp-options range 6 7 drop
ciscoasa(config-tcp-map)# tcp-options range 9 18 drop
ciscoasa(config-tcp-map)# tcp-options range 20 255 drop
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match access-list TCP
```

```
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
set connection	接続値を設定します。
tcp-map	TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。

telnet

インターフェイスへの Telnet アクセスを許可するには、グローバル コンフィギュレーション モードで **telnet** コマンドを使用します。Telnet アクセスを削除するには、このコマンドの **no** 形式を使用します。

telnet {*ipv4_address mask* | *ipv6_address/prefix*} *interface_name*

no telnet {*ipv4_address mask* | *ipv6_address/prefix*} *interface_name*

構文の説明

interface_name	Telnet を許可するインターフェイスの名前を指定します。VPN トンネル内で Telnet を使用する場合を除き、最も低いセキュリティ インターフェイスで Telnet をイネーブルにできません。物理または仮想インターフェイスを指定できます。
ipv4_address mask	ASA への Telnet が認可されているホストまたはネットワークの IPv4 アドレス、およびサブネット マスクを指定します。
ipv6_address/prefix	ASA への Telnet が認可されている IPv6 アドレスおよびプレフィックスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(2)、9.1(2)	デフォルト パスワードの「cisco」は削除されました。**password** コマンドを使用して能動的にログイン パスワードを設定する必要があります。
9.9.(2)	仮想インターフェイスが指定可能になりました。

使用上のガイドライン

telnet コマンドを使用すると、どのホストが Telnet を使用して ASA の CLI にアクセスできるかを指定できます。すべてのインターフェイスで ASA への Telnet をイネーブルにすることができます。ただし、VPN トンネル内で Telnet を使用する場合を除き、最も低いセキュリティ インターフェイスに対して Telnet は使用できません。また、BVI インターフェイスが指定されている場合、そのインターフェイスで **managenent-access** を設定する必要があります。

password コマンドを使用して、コンソールへの Telnet アクセスのパスワードを設定できます。**who** コマンドを使用して、現在、ASA コンソールにアクセス中の IP アドレスを表示できます。**kill** コマンドを使用すると、アクティブ Telnet コンソール セッションを終了できます。

aaa authentication telnet console コマンドを使用する場合は、Telnet コンソール アクセスを認証サーバで認証する必要があります。

例

次に、ホスト 192.168.1.3 と 192.168.1.4 に Telnet を介した ASA の CLI へのアクセスを許可する例を示します。さらに、192.168.2.0 ネットワーク上のすべてのホストにアクセス権が付与されています。

```
ciscoasa(config)# telnet 192.168.1.3 255.255.255.255 inside
ciscoasa(config)# telnet 192.168.1.4 255.255.255.255 inside
ciscoasa(config)# telnet 192.168.2.0 255.255.255.0 inside
ciscoasa(config)# show running-config telnet
192.168.1.3 255.255.255.255 inside
192.168.1.4 255.255.255.255 inside
192.168.2.0 255.255.255.0 inside
```

次に、Telnet コンソール ログイン セッションの例を示します（パスワードは、入力時に表示されません）。

```
ciscoasa# passwd: cisco

Welcome to the XXX
…
Type help or '?' for a list of available commands.
ciscoasa>
```

no telnet コマンドを使用して個々のエントリを、また、**clear configure telnet** コマンドを使用してすべての telnet コマンド ステートメントを削除できます。

```
ciscoasa(config)# no telnet 192.168.1.3 255.255.255.255 inside
ciscoasa(config)# show running-config telnet
192.168.1.4 255.255.255.255 inside
192.168.2.0 255.255.255.0 inside

ciscoasa(config)# clear configure telnet
```

関連コマンド

コマンド	説明
clear configure telnet	コンフィギュレーションから Telnet 接続を削除します。
kill	Telnet セッションを終了します。
show running-config telnet	ASA への Telnet 接続の使用を認可されている IP アドレスの現在のリストを表示します。
telnet timeout	Telnet タイムアウトを設定します。
who	ASA 上のアクティブ Telnet 管理セッションを表示します。

telnet timeout

Telnet のアイドル タイムアウトを設定するには、グローバル コンフィギュレーション モードで **telnet 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。

telnet timeout *minutes*

no telnet timeout *minutes*

構文の説明

分	Telnet セッションがアイドルになってから、ASA がセッションを閉じるまでの分数。有効な値は、1 ～ 1440 分です。デフォルトは 5 分です。

デフォルト

デフォルトでは、Telnet セッションは、アイドル状態のまま 5 分経過すると ASA によって閉じられます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

telnet timeout コマンドを使用して、コンソール Telnet セッションが、ASA によってログオフされるまでアイドル状態を継続できる最長時間を設定できます。

例

次に、セッションの最大アイドル時間を変更する例を示します。

```
ciscoasa(config)# telnet timeout 10
ciscoasa(config)# show running-config telnet timeout
telnet timeout 10 minutes
```

関連コマンド

コマンド	説明
clear configure telnet	コンフィギュレーションから Telnet 接続を削除します。
kill	Telnet セッションを終了します。
show running-config telnet	ASA への Telnet 接続の使用を認可されている IP アドレスの現在のリストを表示します。
Telnet	ASA への Telnet アクセスをイネーブルにします。
who	ASA 上のアクティブ Telnet 管理セッションを表示します。

terminal

現在の Telnet セッションで syslog メッセージの表示を許可するには、特権 EXEC モードで **terminal monitor** コマンドを使用します。syslog メッセージをディセーブルにするには、このコマンドの **no** 形式を使用します。

terminal {**monitor** | **no monitor**}

no terminal interactive

構文の説明

interactive	CLI に **?** と入力した場合にヘルプをイネーブルまたはディセーブルにします。
モニタ	現在の Telnet セッションでの syslog メッセージの表示をイネーブルにします。
no monitor	現在の Telnet セッションでの syslog メッセージの表示をディセーブルにします。

デフォルト

デフォルトでは、syslog メッセージはディセーブルです。このコマンドは、デフォルトではインタラクティブです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.4(1)	**interactive** オプションが追加されました。

使用上のガイドライン

通常、ASA CLI で ? を入力すると、コマンド ヘルプが表示されます。コマンド内にテキストとして ? を入力できるようにするには（たとえば、URL の一部として ? を含めるには）、**no terminal interactive** コマンドを使用してインタラクティブなヘルプをディセーブルにします。

例

次に、現在のセッションで syslog メッセージを表示する例およびディセーブルにする例を示します。

```
ciscoasa# terminal monitor
ciscoasa# terminal no monitor
```

次に、コンソールを非インタラクティブ モードにして、その後インタラクティブ モードにする例を示します。

```
ciscoasa# no terminal interactive
ciscoasa# terminal interactive
```

関連コマンド

コマンド	説明
clear configure terminal	端末の表示幅設定をクリアします。
pager	Telnet セッションで「---more---」プロンプトが表示されるまでの行数を設定します。このコマンドはコンフィギュレーションに保存されます。
show running-config terminal	現在の端末設定を表示します。
terminal pager	Telnet セッションで「---more---」プロンプトが表示されるまでの行数を設定します。このコマンドはコンフィギュレーションに保存されません。
terminal width	グローバル コンフィギュレーション モードでの端末の表示幅を設定します。

terminal pager

Telnet セッションで「---More---」プロンプトが表示されるまでの 1 ページあたりの行数を設定するには、特権 EXEC モードで **terminal pager** コマンドを使用します。

terminal pager [lines] *lines*

構文の説明

[**lines**] *lines*	「---More---」プロンプトが表示されるまでの 1 ページあたりの行数を設定します。デフォルトは 24 行です。0 は、ページの制限がないことを示します。指定できる範囲は 0 ～ 2147483647 行です。**lines** キーワードは任意であり、このキーワードの有無にかかわらずコマンドは同一です。

デフォルト

デフォルトは 24 行です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、現在の Telnet セッションのみを対象に、pager line 設定を変更します。ただし、ユーザ EXEC モードで **login** コマンドを入力するか、**enable** コマンドを入力して特権 EXEC モードを開始する場合にのみ、ASA は running-config から現在のセッションで pager 値を再開します。これは設計どおりです。

（注） ASA がユーザ プロンプトを再表示する前に、予期しない「--- More---」プロンプトが表示されます。これによって、**banner exec** コマンドの出力が抑制されることがあります。代わりに、**banner motd** コマンドまたは **banner login** コマンドを使用します。

新しいデフォルトの pager 設定をコンフィギュレーションに保存するには、次の手順を実行します。

1. **login** コマンドを入力してユーザ EXEC モードにアクセスするか、**enable** コマンドを入力して特権 EXEC モードにアクセスします。
2. **pager** コマンドを入力します。

管理コンテキストに Telnet 接続する場合、ある特定のコンテキスト内の **pager** コマンドに異なる設定があっても、他のコンテキストに移ったときには、pager line 設定はユーザのセッションに従います。現在の pager 設定を変更するには、新しい設定で **terminal pager** コマンドを入力するか、**pager** コマンドを現在のコンテキストで入力します。**pager** コマンドは、コンテキスト コンフィギュレーションに新しい pager 設定を保存する以外に、新しい設定を現在の Telnet セッションに適用します。

例

次に、表示される行数を 20 に変更する例を示します。

```
ciscoasa# terminal pager 20
```

関連コマンド

コマンド	説明
clear configure terminal	端末の表示幅設定をクリアします。
pager	Telnet セッションで「---More---」プロンプトが表示されるまでの行数を設定します。このコマンドはコンフィギュレーションに保存されます。
show running-config terminal	現在の端末設定を表示します。
terminal	Telnet セッションでの syslog メッセージの表示を許可します。
terminal width	グローバル コンフィギュレーション モードでの端末の表示幅を設定します。

terminal width

コンソール セッションで情報を表示する幅を設定するには、グローバル コンフィギュレーション モードで **terminal width** コマンドを使用します。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。

terminal width *columns*

no terminal width *columns*

構文の説明

columns	端末の幅をカラム数で指定します。デフォルトは 80 です。指定できる範囲は 40 ～ 511 です。

デフォルト

デフォルトの表示幅は 80 カラムです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、端末の表示幅を 100 カラムにする例を示します。

```
ciscoasa# terminal width 100
```

関連コマンド

コマンド	説明
clear configure terminal	端末の表示幅設定をクリアします。
show running-config terminal	現在の端末設定を表示します。
terminal	端末回線パラメータを特権 EXEC モードで設定します。

test aaa-server

ASA が特定の AAA サーバでユーザを認証または認可できるかどうかを確認するには、特権 EXEC モードで **test aaa-server** コマンドを使用します。ASA 上の不正なコンフィギュレーションが原因で AAA サーバに到達できない場合があります。また、限定されたネットワーク コンフィギュレーションやサーバのダウンタイムなどの他の理由で AAA サーバに到達できないこともあります。

test aaa-server {**authentication** *server_tag* [**host** *ip_address*] [**username** *username*] [**password** *password*] | **authorization** *server_tag* [**host** *ip_address*] [**username** *username*][**ad-agent**]}

構文の説明

ad-agent	AAA AD エージェント サーバへの接続をテストします。
認証	AAA サーバの認証機能をテストします。
許可	AAA サーバのレガシー VPN 認可機能をテストします。
host *ip_address*	サーバの IP アドレスを指定します。コマンドで IP アドレスを指定しないと、入力を求めるプロンプトが表示されます。
password *password*	ユーザ パスワードを指定します。コマンドでパスワードを指定しないと、入力を求めるプロンプトが表示されます。
server_tag	**aaa-server** コマンドで設定した AAA サーバ タグを指定します。
username *username*	AAA サーバの設定をテストするために使用するアカウントのユーザ名を指定します。ユーザ名が AAA サーバに存在することを確認してください。存在しないと、テストは失敗します。コマンドでユーザ名を指定しないと、入力を求めるプロンプトが表示されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが追加されました。
8.4(2)	**ad-agent** キーワードが追加されました。

使用上のガイドライン

test aaa-server コマンドでは、ASA が特定の AAA サーバを使用してユーザを認証できることと、ユーザを認可できる場合は、レガシー VPN 認可機能を確認できます。このコマンドを使用すると、認証または認可を試みる実際のユーザを持たない AAA サーバをテストできます。また、AAA 障害の原因が、AAA サーバ パラメータの設定ミス、AAA サーバへの接続問題、または ASA 上のその他のコンフィギュレーション エラーのいずれによるものかを特定するうえで役立ちます。

例

次に、ホスト 192.168.3.4 に srvgrp1 という RADIUS AAA サーバを設定し、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。AAA サーバ パラメータのセットアップの後の **test aaa-server** コマンドによって、認証テストがサーバに到達できなかったことが示されます。

```
ciscoasa(config)# aaa-server svrgrp1 protocol radius
ciscoasa(config-aaa-server-group)# aaa-server svrgrp1 host 192.168.3.4
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)# test aaa-server authentication svrgrp1
Server IP Address or name: 192.168.3.4
Username: bogus
Password: mypassword
INFO: Attempting Authentication test to IP address <192.168.3.4> (timeout: 10 seconds)
ERROR: Authentication Rejected: Unspecified
```

次に、正常な結果となった **test aaa-server** コマンドの出力例を示します。

```
ciscoasa# test aaa-server authentication svrgrp1 host 192.168.3.4 username bogus password
mypassword
INFO: Attempting Authentication test to IP address <10.77.152.85> (timeout: 12 seconds)
INFO: Authentication Successful
```

関連コマンド

コマンド	説明
aaa authentication console	管理トラフィックの認証を設定します。
aaa authentication match	通過するトラフィックの認証を設定します。
aaa-server	AAA サーバ グループを作成します。
aaa-server host	AAA サーバをサーバ グループに追加します。

test aaa-server ad-agent

設定後に Active Directory エージェントのコンフィギュレーションをテストするには、AAA サーバ グループ コンフィギュレーション モードで **test aaa-server ad-agent** コマンドを使用します。

test aaa-server ad-agent

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.4(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

アイデンティティ ファイアウォールに対して Active Directory エージェントを設定するには、**aaa-server** コマンドのサブモードである **ad-agent-mode** コマンドを入力します。**ad-agent-mode** コマンドを入力すると、AAA サーバ グループ コンフィギュレーション モードが開始します。

Active Directory エージェントの設定後、**test aaa-server ad-agent** コマンドを入力して、ASA に Active Directory エージェントへの機能接続があることを確認します。

AD エージェントは、定期的に、または要求に応じて、WMI を介して Active Directory サーバのセキュリティ イベント ログ ファイルをモニタし、ユーザのログインおよびログオフ イベントを調べます。AD エージェントは、ユーザ ID および IP アドレス マッピングのキャッシュを保持し、ASA に変更を通知します。

AD エージェント サーバ グループのプライマリ AD エージェントとセカンダリ AD エージェントを設定します。プライマリ AD エージェントが応答していないことを ASA が検出し、セカンダリ AD エージェントが指定されている場合、ASA はセカンダリ AD エージェントに切り替えます。AD エージェントの Active Directory サーバは、通信プロトコルとして RADIUS を使用します。そのため、ASA と AD エージェントとの共有秘密のキー属性を指定する必要があります。

例

次に、アイデンティティ ファイアウォールに対して Active Directory エージェントを設定する際に **ad-agent-mode** をイネーブルにし、接続をテストする例を示します。

```
hostname(config)# aaa-server adagent protocol radius
hostname(config)# ad-agent-mode
hostname(config-aaa-server-group)# aaa-server adagent (inside) host 192.168.1.101
hostname(config-aaa-server-host)# key mysecret
hostname(config-aaa-server-hostkey)# user-identity ad-agent aaa-server adagent
hostname(config-aaa-server-host)# test aaa-server ad-agent
```

関連コマンド

コマンド	説明
aaa-server	AAA サーバ グループを作成し、グループ固有の AAA サーバ 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 パラメータを設定します。
clear configure user-identity	アイデンティティ ファイアウォール機能のコンフィギュレーションをクリアします。

test dynamic-access-policy attributes

dap 属性モードを開始するには、特権 EXEC モードで、**test dynamic-access-policy attributes** コマンドを入力します。これにより、ユーザ属性とエンドポイント属性の値ペアを指定できます。

dynamic-access-policy attributes

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。

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

コマンド履歴

リリース	変更内容
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

通常、ASA は AAA サーバからユーザ認可属性を取得し、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。

この機能は、DAP レコードの作成を試みます。

例

次に、**attributes** コマンドの使用例を示します。

```
ciscoasa # test dynamic-access-policy attributes
ciscoasa(config-dap-test-attr)#
```

関連コマンド

コマンド	説明
dynamic-access-policy-record	DAP レコードを作成します。
属性	ユーザ属性値ペアを指定できる属性モードを開始します。
display	現在の属性リストを表示します。

test dynamic-access-policy execute

すでに設定されている DAP レコードをテストするには、特権 EXEC モードで test dynamic-access-policy execute を使用します。

test dynamic-access-policy execute

構文の説明

AAA attribute value	デバイスの DAP サブシステムは、各レコードの 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、これらの値を参照します。 – [AAA Attribute]: AAA 属性を特定します。 – [Operation Value]: 属性を指定された値に対して =/!= として指定します。
endpoint attribute value	エンドポイント属性を指定します。 – [Endpoint ID]: エンドポイント属性 ID を入力します。 – [Name/Operation/Value]:

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.4(4)	このコマンドが追加されました。

使用上のガイドライン

このコマンドでは、認可属性値のペアを指定することによって、デバイスで設定される DAP レコード セットが取得されるかどうかをテストできます。

test regex

正規表現をテストするには、特権 EXEC モードで **test regex** コマンドを使用します。

test regex *input_text regular_expression*

構文の説明

input_text	正規表現と一致させるテキストを指定します。
regular_expression	最大 100 文字の正規表現を指定します。正規表現で使用できるメタ文字のリストについては、**regex** コマンドを参照してください。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

test regex コマンドは、正規表現が一致すべきものと一致するかどうかをテストします。

正規表現が入力テキストと一致する場合は、次のメッセージが表示されます。

```
INFO: Regular expression match succeeded.
```

正規表現が入力テキストと一致しない場合は、次のメッセージが表示されます。

```
INFO: Regular expression match failed.
```

例

次に、正規表現に対して入力テキストをテストする例を示します。

```
ciscoasa# test regex farscape scape
INFO: Regular expression match succeeded.

ciscoasa# test regex farscape scaper

INFO: Regular expression match failed.
```

関連コマンド

コマンド	説明
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	トラフィック クラスを 1 つ以上のアクションと関連付けることによって、ポリシー マップを作成します。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
class-map type regex	正規表現クラス マップを作成します。
regex	正規表現を作成します。

test sso-server（廃止）

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

テスト用の認証要求で SSO サーバをテストするには、特権 EXEC モードで **test sso-server** コマンドを使用します。

test sso-server *server-name* **username** *user-name*

構文の説明

server-name	テストする SSO サーバの名前を指定します。
user-name	テストする SSO サーバのユーザの名前を指定します。

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。

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

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。
9.5(2)	SAML 2.0 がサポートされたため、このコマンドは廃止されました。

使用上のガイドライン

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザはユーザ名とパスワードを一度だけ入力すれば、別のサーバでさまざまなセキュアなサービスにアクセスできます。**test sso-server** コマンドは、SSO サーバが認識されるかどうか、さらに、認証要求に応答しているかどうかをテストします。

server-name 引数で指定された SSO サーバが見つからない場合は、次のエラーが表示されます。

```
ERROR: sso-server server-name does not exist
```

SSO サーバが見つかったが、*user-name* 引数で指定されたユーザが見つからない場合は、認証は拒否されます。

認証では、ASA は SSO サーバへの WebVPN ユーザのプロキシとして動作します。ASA は現在、SiteMinder SSO サーバ（以前の Netegrity SiteMinder）と SAML POST タイプの SSO サーバをサポートしています。このコマンドは SSO サーバの両タイプに適用されます。

例

次に、特権 EXEC モードを開始し、ユーザ名 Anyuser を使用して SSO サーバ my-sso-server をテストし、正常な結果を得た例を示します。

```
ciscoasa# test sso-server my-sso-server username Anyuser
INFO: Attempting authentication request to sso-server my-sso-server for user Anyuser
INFO: STATUS: Success
ciscoasa#
```

次に、同じサーバだが、ユーザ Anotheruser でテストし、認識されず、認証が失敗した例を示します。

```
ciscoasa# test sso-server my-sso-server username Anotheruser
INFO: Attempting authentication request to sso-server my-sso-server for user Anotheruser
INFO: STATUS: Failed
ciscoasa#
```

関連コマンド

コマンド	説明
max-retry-attempts	ASA が、失敗した SSO 認証を再試行する回数を設定します。
policy-server-secret	SiteMinder SSO サーバへの認証要求の暗号化に使用する秘密キーを作成します。
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 サーバの運用統計情報を表示します。
sso-server	シングル サインオン サーバを作成します。
web-agent-url	ASA が SiteMinder SSO 認証を要求する SSO サーバの URL を指定します。

text-color

ログイン ページ、ホームページ、およびファイル アクセス ページの WebVPN タイトルバーのテキストに色を設定するには、webvpn モードで **text-color** コマンドを使用します。テキストの色をコンフィギュレーションから削除して、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。

text-color [*black* | *white* | *auto*]

no text-color

構文の説明

auto	secondary-color コマンドの設定に基づいて黒または白を選択します。つまり、2 番めの色が黒の場合、この値は白となります。
black	タイトルバーのテキストのデフォルト色は白です。
white	色を黒に変更できます。

デフォルト

タイトルバーのテキストのデフォルト色は白です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、タイトルバーのテキストの色を黒に設定する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# text-color black
```

関連コマンド

コマンド	説明
secondary-text-color	WebVPN ログイン ページ、ホームページ、およびファイル アクセス ページのセカンダリ テキストの色を設定します。

tftp-server

configure net コマンドまたは **write net** コマンドで使用するデフォルトの TFTP サーバとパスおよびファイル名を指定するには、グローバル コンフィギュレーション モードで **tftp-server** コマンドを使用します。サーバ コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。このコマンドは IPv4 および IPv6 のアドレスをサポートします。

tftp-server *interface_name server filename*

no tftp-server [*interface_name server filename*]

構文の説明

filename	パスとファイル名を指定します。
interface_name	ゲートウェイ インターフェイス名を指定します。最高のセキュリティ インターフェイス以外のインターフェイスを指定した場合は、そのインターフェイスがセキュアではないことを示す警告メッセージが表示されます。
サーバ	TFTP サーバの IP アドレスまたは名前を設定します。IPv4 アドレスまたは IPv6 アドレスを入力できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	現在ではゲートウェイ インターフェイスが必要です。

使用上のガイドライン

tftp-server コマンドを使用すると、**configure net** コマンドと **write net** コマンドの入力が容易になります。**configure net** コマンドまたは **write net** コマンドを入力するときに、**tftp-server** コマンドで指定した TFTP サーバを継承するか、または独自の値を指定できます。また、**tftp-server** コマンドのパスをそのまま継承したり、**tftp-server** コマンド値の末尾にパスとファイル名を追加したり、**tftp-server** コマンド値を上書きすることもできます。

ASA がサポートする **tftp-server** コマンドは 1 つだけです。

例

次に、TFTP サーバを指定し、その後、/temp/config/test_config ディレクトリからコンフィギュレーションを読み込む例を示します。

```
ciscoasa(config)# tftp-server inside 10.1.1.42 /temp/config/test_config
ciscoasa(config)# configure net
```

関連コマンド

コマンド	説明
configure net	指定した TFTP サーバとパスからコンフィギュレーションをロードします。
show running-config tftp-server	デフォルトの TFTP サーバ アドレスとコンフィギュレーション ファイルのディレクトリを表示します。

tftp-server address（廃止）

クラスタ内の TFTP サーバを指定するには、電話プロキシ コンフィギュレーション モードで **tftp-server address** コマンドを使用します。電話プロキシ コンフィギュレーションから TFTP サーバを削除するには、このコマンドの **no** 形式を使用します。

tftp-server address *ip_address* [*port*] **interface** *interface*

no tftp-server address *ip_address* [*port*] **interface** *interface*

構文の説明

ip_address	TFTP サーバのアドレスを指定します。
interface *interface*	TFTP サーバが存在するインターフェイスを指定します。これは、TFTP サーバの実アドレスにする必要があります。
port	（任意）これは、TFTP サーバが TFTP 要求をリッスンするポートです。デフォルトの TFTP ポート 69 でない場合に、設定する必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。
9.4(1)	このコマンドは、すべての **phone-proxy** モード コマンドとともに廃止されました。

使用上のガイドライン

電話プロキシには、少なくとも 1 つの CUCM TFTP サーバを設定する必要があります。電話プロキシに対して TFTP サーバを 5 つまで設定できます。

TFTP サーバは、信頼ネットワーク上のファイアウォールの背後に存在すると想定されます。そのため、電話プロキシは IP 電話と TFTP サーバの間の要求を代行受信します。TFTP サーバは、CUCM と同じインターフェイス上に存在している必要があります。

内部 IP アドレスを使用して TFTP サーバを作成し、TFTP サーバが存在するインターフェイスを指定します。

IP 電話で、TFTP サーバの IP アドレスを次のように設定する必要があります。

- NAT が TFTP サーバ用に設定されている場合は、TFTP サーバのグローバル IP アドレスを使用します。
- NAT が TFTP サーバ用に設定されていない場合は、TFTP サーバの内部 IP アドレスを使用します。

サービス ポリシーがグローバルに適用されている場合は、TFTP サーバが存在するインターフェイスを除くすべての入力インターフェイスで、TFTP トラフィックを転送し TFTP サーバに到達させるための分類ルールが作成されます。サービス ポリシーが特定のインターフェイスに適用されている場合は、指定された電話プロキシ モジュールへのインターフェイスで、TFTP トラフィックを転送し TFTP サーバに到達させるための分類ルールが作成されます。

NAT ルールを TFTP サーバに設定する場合は、分類ルールのインストール時に TFTP サーバのグローバル アドレスが使用されるように、サービス ポリシーを適用する前に、NAT ルールを設定する必要があります。

例

次に、**tftp-server address** コマンドを使用して、電話プロキシに対応する 2 つの TFTP サーバを設定する例を示します。

```
ciscoasa(config)# phone-proxy asa_phone_proxy
ciscoasa(config-phone-proxy)# tftp-server address 192.168.1.2 in interface outside
ciscoasa(config-phone-proxy)# tftp-server address 192.168.1.3 in interface outside
ciscoasa(config-phone-proxy)# media-termination address 192.168.1.4 interface inside
ciscoasa(config-phone-proxy)# media-termination address 192.168.1.25 interface outside
ciscoasa(config-phone-proxy)# tls-proxy asa_tlsp
ciscoasa(config-phone-proxy)# ctl-file asactl
ciscoasa(config-phone-proxy)# cluster-mode nonsecure
```

関連コマンド

コマンド	説明
phone-proxy	Phone Proxy インスタンスを設定します。

threat-detection basic-threat

基本的な脅威の検出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 **threat-detection basic-threat** コマンドを使用します。基本的な脅威の検出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。

threat-detection basic-threat

no threat-detection basic-threat

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

基本脅威検出は、デフォルトでイネーブルになっています。次のデフォルトのレート制限が使用されます。

表 1-1　基本脅威検出のデフォルト設定

	トリガー設定	
パケット ドロップの理由	平均レート	バースト レート
• DoS 攻撃の検出 • 不正なパケット形式 • 接続制限の超過 • 疑わしい ICMP パケットの検出	直前の 600 秒間で 100 ドロップ/秒。	直近の 20 秒間で 400 ドロップ/秒。
	直前の 3600 秒間で 80 ドロップ/秒。	直近の 120 秒間で 320 ドロップ/秒。
スキャン攻撃の検出	直前の 600 秒間で 5 ドロップ/秒。	直近の 20 秒間で 10 ドロップ/秒。
	直前の 3600 秒間で 4 ドロップ/秒。	直近の 120 秒間で 8 ドロップ/秒。
不完全セッションの検出（TCP SYN 攻撃の検出や戻りデータなし UDP セッション攻撃の検出など）（複合）	直前の 600 秒間で 100 ドロップ/秒。	直近の 20 秒間で 200 ドロップ/秒。
	直前の 3600 秒間で 80 ドロップ/秒。	直近の 120 秒間で 160 ドロップ/秒。
アクセス リストによる拒否	直前の 600 秒間で 400 ドロップ/秒。	直近の 20 秒間で 800 ドロップ/秒。
	直前の 3600 秒間で 320 ドロップ/秒。	直近の 120 秒間で 640 ドロップ/秒。
• 基本ファイアウォール検査に不合格	直前の 600 秒間で 400 ドロップ/秒。	直近の 20 秒間で 1600 ドロップ/秒。
• アプリケーション インスペクションに不合格のパケット	直前の 3600 秒間で 320 ドロップ/秒。	直近の 120 秒間で 1280 ドロップ/秒。
インターフェイスの過負荷	直前の 600 秒間で 2000 ドロップ/秒。	直近の 20 秒間で 8000 ドロップ/秒。
	直前の 3600 秒間で 1600 ドロップ/秒。	直近の 120 秒間で 6400 ドロップ/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		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• Yes	• Yes	• Yes	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
8.2(1)	バースト レート間隔の平均レートが 60 分の 1 から 30 分の 1 に変更されました。

使用上のガイドライン

基本的な脅威の検出をイネーブルにすると、ASA は、次の理由によるドロップ パケットとセキュリティ イベントのレートをモニタします。

- アクセス リストによる拒否
- 不正なパケット形式（invalid-ip-header や invalid-tcp-hdr-length など）
- 接続制限の超過（システム全体のリソース制限とコンフィギュレーションで設定されている制限の両方）
- DoS 攻撃の検出（無効な SPI、ステートフル ファイアウォール検査の不合格など）
- 基本ファイアウォール検査の不合格（このオプションは、ここに列挙されているファイアウォール関連のパケット ドロップすべてを含む総合レートです。インターフェイスの過負荷、アプリケーション インスペクションで不合格のパケット、スキャン攻撃の検出など、ファイアウォールに関連しないパケット ドロップは含まれていません）
- 疑わしい ICMP パケットの検出
- アプリケーション インスペクションに不合格のパケット
- インターフェイスの過負荷
- 検出されたスキャン攻撃（このオプションでは、スキャン攻撃をモニタします。たとえば、最初の TCP パケットが SYN パケットでないことや、TCP 接続で 3 ウェイ ハンドシェイクに失敗することなどです。完全なスキャンによる脅威の検出（**threat-detection scanning-threat** コマンドを参照）では、このスキャン攻撃レート情報を使用し、ホストを攻撃者として分類してそれらのホストを自動的に回避するなどして対処します）。
- 不完全セッションの検出（TCP SYN 攻撃の検出や戻りデータなし UDP セッション攻撃の検出など）。

ASA は、脅威を検出するとすぐにシステム ログ メッセージ（733100）を送信し、ASDM に警告します。

基本脅威検出は、ドロップまたは潜在的な脅威が存在した場合にだけパフォーマンスに影響します。このようなシナリオでも、パフォーマンスへの影響はわずかです。

「デフォルト」の項の表 1-1 に、デフォルト設定を示します。すべてのデフォルト設定は、**show running-config all threat-detection** コマンドを使用して表示できます。**threat-detection rate** コマンドを使用して、各イベント タイプのデフォルト設定を上書きできます。

イベント レートが超過すると、ASA はシステム メッセージを送信します。ASA は、一定間隔における平均イベント レートと短期バースト間隔におけるバースト イベント レートの 2 種類のレートを追跡します。バースト イベント レートは、平均レート間隔の 1/30 または 10 秒のうち、どちらか大きいほうです。受信するイベントごとに、ASA は平均レート制限とバースト レート制限をチェックします。両方のレートが超過している場合、ASA はバースト期間あたりのレート タイプごとに最大 1 つのメッセージを生成して、2 つの異なるシステム メッセージを送信します。

例

次の例では、基本脅威検出をイネーブルにし、DoS 攻撃のトリガーを変更しています。

```
ciscoasa(config)# threat-detection basic-threat
ciscoasa(config)# threat-detection rate dos-drop rate-interval 600 average-rate 60
burst-rate 100
```

関連コマンド

コマンド	説明
clear threat-detection rate	基本脅威検出の統計情報をクリアします。
show running-config all threat-detection	脅威検出コンフィギュレーションを表示します。個別にレート設定をしていない場合はデフォルトのレート設定も表示されます。
show threat-detection rate	基本脅威検出の統計情報を表示します。
threat-detection rate	イベント タイプごとの脅威検出レート制限を設定します。
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。

threat-detection rate

threat-detection basic-threat コマンドを使用して基本的な脅威の検出をイネーブルにする場合は、グローバル コンフィギュレーション モードで **threat-detection rate** コマンドを使用して、各イベント タイプのデフォルトのレート制限を変更できます。**threat-detection scanning-threat** コマンドを使用してスキャンによる脅威の検出をイネーブルにする場合は、このコマンドに **scanning-threat** キーワードを指定して、ホストを攻撃者またはターゲットと見なすタイミングを設定できます。設定しない場合は、基本的な脅威の検出とスキャンによる脅威の検出の両方で、デフォルトの **scanning-threat** 値が使用されます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

threat-detection rate {**acl-drop** | **bad-packet-drop** | **conn-limit-drop** | **dos-drop** | **fw-drop** | **icmp-drop** | **inspect-drop** | **interface-drop** | **scanning-threat** | **syn-attack**} **rate-interval** *rate_interval* **average-rate** *av_rate* **burst-rate** *burst_rate*

no threat-detection rate {**acl-drop** | **bad-packet-drop** | **conn-limit-drop** | **dos-drop** | **fw-drop** | **icmp-drop** | **inspect-drop** | **interface-drop** | **scanning-threat** | **syn-attack**} **rate-interval** *rate_interval* **average-rate** *av_rate* **burst-rate** *burst_rate*

構文の説明

acl-drop	アクセス リストによる拒否のためにドロップされたパケットのレート制限を設定します。
average-rate *av_rate*	平均レート制限を 0 ～ 2147483647 ドロップ/秒の範囲で設定します。
bad-packet-drop	パケット形式に誤りがあって（invalid-ip-header や invalid-tcp-hdr-length など）拒否されたためにドロップされたパケットのレート制限を設定します。
burst-rate *burst_rate*	バースト レート制限を 0 ～ 2147483647 ドロップ/秒の範囲で設定します。バースト レートは、*N* 秒ごとの平均レートとして計算されます。*N* はバースト レート間隔です。バースト レート間隔は、**rate-interval** *rate_interval* 値の 1/30 または 10 秒のうち大きい方の値になります。
conn-limit-drop	接続制限（システム全体のリソース制限とコンフィギュレーションで設定される制限の両方）を超えたためにドロップされたパケットのレート制限を設定します。
dos-drop	DoS 攻撃（無効な SPI、ステートフル ファイアウォール チェック不合格など）を検出したためにドロップされたパケットのレート制限を設定します。
fw-drop	基本ファイアウォール チェックに不合格だったためにドロップされたパケットのレート制限を設定します。このオプションは、このコマンドのファイアウォールに関連したパケット ドロップをすべて含む複合レートです。**interface-drop**、**inspect-drop**、**scanning-threat** など、ファイアウォールに関連しないドロップ レートは含まれません。
icmp-drop	不審な ICMP パケットが検出されたためにドロップされたパケットのレート制限を設定します。
inspect-drop	パケットがアプリケーション インスペクションに失敗したためにドロップされたパケットのレート制限を設定します。
interface-drop	インターフェイスの過負荷が原因でドロップされたパケットのレート制限を設定します。

rate-interval *rate_interval*	平均レート間隔を 600 ～ 2592000 秒（30 日）の範囲で設定します。レート間隔は、ドロップ数の平均値を求める期間を決定するために使用されます。また、バーストしきい値レート間隔を決定します。
scanning-threat	スキャン攻撃が検出されたためにドロップされたパケットのレート制限を設定します。このオプションでは、たとえば最初の TCP パケットが SYN パケットでない、またはスリーウェイ ハンドシェイクで TCP 接続に失敗したなどのスキャン攻撃をモニタします。完全スキャン脅威検出（**threat-detection scanning-threat** コマンドを参照）では、このスキャン攻撃レートの情報を取得し、その情報をもとにして、たとえばホストを攻撃者として分類し自動的に遮断するなどの方法で対処します。
syn-attack	TCP SYN 攻撃や戻りデータなし UDP セッション攻撃など、不完全なセッションが原因でドロップされたパケットのレート制限を設定します。

デフォルト

threat-detection basic-threat コマンドを使用して基本的な脅威の検出をイネーブルにした場合は、次のデフォルトのレート制限が使用されます。

表 1-2　基本脅威検出のデフォルト設定

	トリガー設定	
パケット ドロップの理由	平均レート	バースト レート
• **dos-drop** • **bad-packet-drop** • **conn-limit-drop** • **icmp-drop**	直前の 600 秒間で 100 ドロップ/秒。	直近の 20 秒間で 400 ドロップ/秒。
	直前の 3600 秒間で 100 ドロップ/秒。	直近の 120 秒間で 400 ドロップ/秒。
scanning-threat	直前の 600 秒間で 5 ドロップ/秒。	直近の 20 秒間で 10 ドロップ/秒。
	直前の 3600 秒間で 5 ドロップ/秒。	直近の 120 秒間で 10 ドロップ/秒。
syn-attack	直前の 600 秒間で 100 ドロップ/秒。	直近の 20 秒間で 200 ドロップ/秒。
	直前の 3600 秒間で 100 ドロップ/秒。	直近の 120 秒間で 200 ドロップ/秒。
acl-drop	直前の 600 秒間で 400 ドロップ/秒。	直近の 20 秒間で 800 ドロップ/秒。
	直前の 3600 秒間で 400 ドロップ/秒。	直近の 120 秒間で 800 ドロップ/秒。
• **fw-drop** • **inspect-drop**	直前の 600 秒間で 400 ドロップ/秒。	直近の 20 秒間で 1600 ドロップ/秒。
	直前の 3600 秒間で 400 ドロップ/秒。	直近の 120 秒間で 1600 ドロップ/秒。
interface-drop	直前の 600 秒間で 2000 ドロップ/秒。	直近の 20 秒間で 8000 ドロップ/秒。
	直近の 3600 秒間で 2000 ドロップ/秒	直近の 120 秒間で 8000 ドロップ/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		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• Yes	• Yes	• Yes	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
8.2(1)	バースト レート間隔の平均レートが 60 分の 1 から 30 分の 1 に変更されました。

使用上のガイドライン

イベント タイプごとに、異なるレート間隔を 3 つまで設定できます。

基本的な脅威の検出をイネーブルにした場合、ASA は、「構文の説明」の表で説明したイベント タイプによるドロップ パケットとセキュリティ イベントのレートをモニタします。

ASA は、脅威を検出するとすぐにシステム ログ メッセージ(733100)を送信し、ASDM に警告します。

基本脅威検出は、ドロップまたは潜在的な脅威が存在した場合にだけパフォーマンスに影響します。このようなシナリオでも、パフォーマンスへの影響はわずかです。

「デフォルト」の項の表 1-1 に、デフォルト設定を示します。すべてのデフォルト設定は、**show running-config all threat-detection** コマンドを使用して表示できます。

イベント レートが超過すると、ASA はシステム メッセージを送信します。ASA は、一定間隔における平均イベント レートと短期バースト間隔におけるバースト イベント レートの 2 種類のレートを追跡します。受信するイベントごとに、ASA は平均レート制限とバースト レート制限をチェックします。両方のレートが超過している場合、ASA はバースト期間あたりのレート タイプごとに最大 1 つのメッセージを生成して、2 つの異なるシステム メッセージを送信します。

例

次の例では、基本脅威検出をイネーブルにし、DoS 攻撃のトリガーを変更しています。

```
ciscoasa(config)# threat-detection basic-threat
ciscoasa(config)# threat-detection rate dos-drop rate-interval 600 average-rate 60
burst-rate 100
```

関連コマンド

コマンド	説明
clear threat-detection rate	基本脅威検出の統計情報をクリアします。
show running-config all threat-detection	脅威検出コンフィギュレーションを表示します。個別にレート設定をしていない場合はデフォルトのレート設定も表示されます。
show threat-detection rate	基本脅威検出の統計情報を表示します。
threat-detection basic-threat	基本脅威検出をイネーブルにします。
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。

threat-detection scanning-threat

スキャンによる脅威の検出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 **threat-detection scanning-threat** コマンドを使用します。スキャンによる脅威の検出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。

threat-detection scanning-threat [**shun**
[**except** {**ip-address** *ip_address mask* | **object-group** *network_object_group_id*} | **duration** *seconds*]]

no threat-detection scanning-threat [**shun**
[**except** {**ip-address** *ip_address mask* | **object-group** *network_object_group_id*} | **duration** *seconds*]]

構文の説明

duration *seconds*	攻撃元ホストの回避期間を 10 ～ 2592000 秒の範囲で設定します。デフォルトの期間は 3600 秒（1 時間）です。
except	IP アドレスを回避対象から除外します。このコマンドを複数回入力し、複数の IP アドレスまたはネットワーク オブジェクト グループを特定して遮断対象から除外できます。
ip-address *ip_address mask*	回避対象から除外する IP アドレスを指定します。
object-group *network_object_group_id*	回避対象から除外するネットワーク オブジェクト グループを指定します。オブジェクト グループを作成するには、**object-group network** コマンドを参照してください。
shun	ASA がホストを攻撃者であると識別すると、syslog メッセージ 733101 を送信し、さらにホスト接続を自動的に終了します。

デフォルト

デフォルトの回避期間は 3600 秒（1 時間）です。

スキャン攻撃イベントでは、次のデフォルトのレート制限が使用されます。

表 1-3　スキャンによる脅威の検出のデフォルトのレート制限

平均レート	バースト レート
直前の 600 秒間で 5 ドロップ/秒。	直近の 20 秒間で 10 ドロップ/秒。
直前の 3600 秒間で 5 ドロップ/秒。	直近の 120 秒間で 10 ドロップ/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		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• Yes	• Yes	• Yes	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
8.0(4)	**duration** キーワードが追加されました。

使用上のガイドライン

典型的なスキャン攻撃では、あるホストがサブネット内の IP アドレスにアクセスできるかどうかを 1 つずつ試します（サブネット内の複数のホストすべてを順にスキャンするか、1 つのホストまたはサブネットの複数のポートすべてを順にスイープする）。スキャン脅威検出機能は、いつホストがスキャンを実行するかを判別します。トラフィック署名に基づく IPS スキャン検出とは異なり、ASA のスキャンによる脅威の検出機能では、広範なデータベースが保持され、これに含まれるホスト統計情報をスキャン アクティビティに関する分析に使用できます。

ホスト データベースは、不審なアクティビティを追跡します。このようなアクティビティには、戻りアクティビティのない接続、閉じているサービス ポートへのアクセス、脆弱な TCP 動作（非ランダム IPID など）、およびその他の多くの動作が含まれます。

注意 スキャンによる脅威の検出機能は、ホストおよびサブネットベースのデータ構造を作成し情報を収集する間、ASA のパフォーマンスとメモリに大きく影響することがあります。

攻撃者に関するシステム ログ メッセージを送信するように ASA を設定したり、自動的にホストを排除したりできます。デフォルトでは、ホストが攻撃者として識別されると、システム ログ メッセージ 730101 が生成されます。

ASA は、スキャンによる脅威イベント レートを超過した時点で、攻撃者とターゲットを識別します。ASA は、一定間隔における平均イベント レートと短期バースト間隔におけるバースト イベント レートの 2 種類のレートを追跡します。スキャン攻撃の一部と見なされるイベントが検出されるたびに、ASA は平均レート制限とバースト レート制限をチェックします。ホストから送信されるトラフィックがどちらかのレートを超えると、そのホストは攻撃者と見なされます。ホストが受信したトラフィックがどちらかのレートを超えると、そのホストはターゲットと見なされます。スキャンによる脅威イベントのレート制限は **threat-detection rate scanning-threat** コマンドを使用して変更できます。

攻撃者またはターゲットとして分類されたホストを表示するには、**show threat-detection scanning-threat** コマンドを使用します。

回避対象のホストを表示するには、**show threat-detection shun** コマンドを使用します。排除対象からホストを除外するには、**clear threat-detection shun** コマンドを使用します。

例

次に、スキャンによる脅威の検出をイネーブルにし、10.1.1.0 ネットワーク上のホストを除き、攻撃者として分類されたホストを自動的に回避する例を示します。スキャンによる脅威の検出のデフォルトのレート制限は変更することもできます。

```
ciscoasa(config)# threat-detection scanning-threat shun except ip-address 10.1.1.0
255.255.255.0
ciscoasa(config)# threat-detection rate scanning-threat rate-interval 1200 average-rate 10
burst-rate 20
ciscoasa(config)# threat-detection rate scanning-threat rate-interval 2400 average-rate 10
burst-rate 20
```

関連コマンド

コマンド	説明
clear threat-detection shun	ホストを回避対象から解除します。
show threat-detection scanning-threat	攻撃者およびターゲットとして分類されたホストを表示します。
show threat-detection shun	現在回避されているホストを表示します。
threat-detection basic-threat	基本脅威検出をイネーブルにします。
threat-detection rate	イベント タイプごとの脅威検出レート制限を設定します。

threat-detection statistics

高度なスキャン脅威検出の統計情報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 **threat-detection statistics** コマンドを使用します。高度なスキャン脅威検出の統計情報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。

注意 統計情報をイネーブルにすると、イネーブルにした統計情報のタイプに応じて、ASA のパフォーマンスに影響することがあります。**threat-detection statistics host** コマンドはパフォーマンスに大幅に影響を与えるため、トラフィックの負荷が高い場合は、このタイプの統計情報を一時的にイネーブルにすることを検討します。ただし、**threat-detection statistics port** コマンドは大きな影響を与えません。

threat-detection statistics [**access-list** | [**host** | **port** | **protocol** [**number-of-rate** {**1** | **2** | **3**}] | **tcp-intercept** [**rate-interval** *minutes*] [**burst-rate** *attacks_per_sec*] [**average-rate** *attacks_per_sec*]]

no threat-detection statistics [**access-list** | **host** | **port** | **protocol** | **tcp-intercept** [**rate-interval** *minutes*] [**burst-rate** *attacks_per_sec*] [**average-rate** *attacks_per_sec*]]

構文の説明

access-list	(任意)アクセス リストによる拒否の統計情報をイネーブルにします。アクセス リスト統計情報は、**show threat-detection top access-list** コマンドを使用した場合にだけ表示されます。
average-rate *attacks_per_sec*	(任意)TCP 代行受信について、syslog メッセージ生成の平均レートしきい値を 25 ～ 2147483647 の範囲で指定します。デフォルトは 1 秒間に 200 回です。平均レートがこれを超えると、syslog メッセージ 733105 が生成されます。
burst-rate *attacks_per_sec*	(任意)TCP 代行受信について、syslog メッセージ生成のしきい値を 25 ～ 2147483647 の範囲で指定します。デフォルトは 1 秒間に 400 です。バースト レートがこれを超えると、syslog メッセージ 733104 が生成されます。
ホスト	(任意)ホスト統計情報をイネーブルにします。ホストがアクティブで、スキャン脅威ホスト データベース内に存在する限り、ホスト統計情報は累積されます。ホストは、非アクティブになってから 10 分後にデータベースから削除されます(統計情報もクリアされます)。
number-of-rate {**1** | **2** | **3**}	(任意)ホスト、ポート、プロトコルの統計情報に対して維持されるレート間隔の数を設定します。デフォルトのレート間隔の数は **1** です。メモリの使用量を低く抑えます。より多くのレート間隔を表示するには、値を **2** または **3** に設定します。たとえば、値を **3** に設定すると、直前の 1 時間、8 時間、および 24 時間のデータが表示されます。このキーワードを **1** に設定した場合(デフォルト)、最も短いレート間隔統計情報だけが保持されます。値を **2** に設定すると、短い方から 2 つの間隔が保持されます。
port	(任意)ポート統計情報をイネーブルにします。
protocol	(任意)プロトコル統計情報をイネーブルにします。

rate-interval *minutes*	(任意)TCP 代行受信について、履歴モニタリング ウィンドウのサイズを、1 ～ 1440 分の範囲で設定します。デフォルトは 30 分です。この間隔の間に、ASA は攻撃の数を 30 回サンプリングします。
tcp-intercept	(任意)TCP 代行受信によって代行受信される攻撃の統計情報をイネーブルにします。TCP 代行受信をイネーブルにするには、**set connection embryonic-conn-max** コマンド、**nat** コマンド、または **static** コマンドを参照してください。

デフォルト

デフォルトでは、アクセス リスト統計情報はイネーブルです。このコマンドにオプションを指定しなかった場合は、すべてのオプションがイネーブルになります。

デフォルトの **tcp-intercept rate-interval** は 30 分です。デフォルトの **burst-rate** は 1 秒あたり 400 です。デフォルトの **average-rate** は 1 秒あたり 200 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
8.0(4)/8.1(2)	**tcp-intercept** キーワードが追加されました。
8.1(2)	**number-of-rates** キーワードがホスト統計情報用に追加され、レート数のデフォルト値が 3 から 1 に変更されました。
8.2(1)	バースト レート間隔の平均レートが 60 分の 1 から 30 分の 1 に変更されました。
8.3(1)	**number-of-rates** キーワードがポートとプロトコルの統計情報用に追加され、レート数のデフォルト値が 3 から 1 に変更されました。

使用上のガイドライン

このコマンドにオプションを指定しなかった場合は、すべての統計情報がイネーブルになります。特定の統計情報のみをイネーブルにするには、統計情報のタイプごとにこのコマンドを入力します。オプションを指定せずにコマンドを入力しないでください。**threat-detection statistics** を(何もオプションを指定しないで)入力した後、統計情報固有のオプション(たとえば **threat-detection statistics host number-of-rate 2**)を指定してコマンドを入力することで、特定の統計情報をカスタマイズできます。**threat-detection statistics** を(何もオプションを指定しないで)入力した後、特定の統計情報のコマンドを、統計情報固有のオプションを指定しないで入力した場合は、すでにイネーブルになっているので、そのコマンドによる効果は何もありません。

このコマンドの **no** 形式を入力すると、すべての **threat-detection statistics** コマンドが削除されます。これには、デフォルトでイネーブルになる **threat-detection statistics access-list** コマンドも含まれます。

統計情報を表示するには、**show threat-detection statistics** コマンドを使用します。

threat-detection scanning-threat コマンドを使用して、スキャンによる脅威の検出をイネーブルにする必要はありません。検出と統計情報は個別に設定できます。

例

次に、ホストを除くすべてのタイプのスキャンによる脅威の検出とスキャン脅威統計情報の例を示します。

```
ciscoasa(config)# threat-detection scanning-threat shun except ip-address 10.1.1.0
255.255.255.0
ciscoasa(config)# threat-detection statistics access-list
ciscoasa(config)# threat-detection statistics port
ciscoasa(config)# threat-detection statistics protocol
ciscoasa(config)# threat-detection statistics tcp-intercept
```

関連コマンド

コマンド	説明
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。
show threat-detection statistics host	ホストの統計情報を表示します。
show threat-detection memory	高度な脅威検出の統計情報のメモリ使用を表示します。
show threat-detection statistics port	ポートの統計情報を表示します。
show threat-detection statistics protocol	プロトコルの統計情報を表示します。
show threat-detection statistics top	上位 10 位までの統計情報を表示します。

threshold

SLA モニタリング動作のしきい値超過イベントのしきい値を設定するには、SLA モニタ コンフィギュレーション モードで **threshold** 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。

threshold *milliseconds*

no threshold

構文の説明

milliseconds	宣言する上昇しきい値をミリ秒で指定します。有効な値は、0 ～ 2147483647 です。この値は、タイムアウトに設定された値以下にする必要があります。

デフォルト

デフォルトのしきい値は 5000 ミリ秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
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

しきい値は、しきい値超過イベントを示すためにだけ使用されます。到達可能性には影響しませんが、**timeout** コマンドの適切な設定を評価するために使用できます。

例

次の例では、ID が 123 の SLA 動作を設定し、ID が 1 のトラッキング エントリを作成して、SLA の到達可能性を追跡しています。SLA 動作の頻度を 10 秒、しきい値を 2500 ミリ秒、タイムアウト値を 4000 ミリ秒に設定しています。

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
ciscoasa(config-sla-monitor-echo)# threshold 2500
ciscoasa(config-sla-monitor-echo)# timeout 4000
ciscoasa(config-sla-monitor-echo)# frequency 10
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
sla monitor	SLA モニタリング動作を定義します。
timeout	SLA 動作が応答を待機する期間を定義します。

throughput level

スマート ライセンス権限付与要求のスループット レベルを設定するには、ライセンス スマート コンフィギュレーション モードで **throughput level** コマンドを使用します。スループット レベルを削除し、デバイスのライセンスを登録解除するには、このコマンドの **no** 形式を使用します。

(注) この機能は、ASAv だけでサポートされています。

throughput level {100M | 1G | 2G}

no throughput level [100M | 1G | 2G]

構文の説明

100M	100 Mbps のスループット レベルを設定します。
1G	1 Gbps のスループット レベルを設定します。
2G	2 Gbps のスループット レベルを設定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.3(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

スループット レベルを要求または変更する場合、変更を反映させるには、ライセンス スマート コンフィギュレーション モードを終了する必要があります。

例

次に、機能階層を標準に設定し、スループット レベルを 2G に設定する例を示します。

```
ciscoasa# license smart
ciscoasa(config-smart-lic)# feature tier standard
ciscoasa(config-smart-lic)# throughput level 2G
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

関連コマンド

コマンド	説明
call-home	Smart Call Home を設定します。スマート ライセンスでは、Smart Call Home インフラストラクチャが使用されます。
clear configure license	スマート ライセンス設定をクリアします。
feature tier	スマート ライセンスの機能層を設定します。
http-proxy	スマート ライセンスおよび Smart Call Home の HTTP(S) プロキシを設定します。
license smart	スマート ライセンスのライセンス権限付与を要求できます。
license smart deregister	ライセンス認証局からデバイスを登録解除します。
license smart register	デバイスをライセンス認証局に登録します。
license smart renew	登録またはライセンス権限を更新します。
service call-home	Smart Call Home をイネーブルにします。
show license	スマート ライセンスのステータスを表示します。
show running-config license	スマート ライセンスの設定を表示します。

ticket（廃止）

Cisco Intercompany Media Engine プロキシ用にチケット エポックとパスワードを設定するには、UC-IME コンフィギュレーション モードで **ticket** コマンドを使用します。プロキシからコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

ticket epoch *n* **password** *password*

no ticket epoch *n* **password** *password*

構文の説明

n	パスワードの完全性チェックの時間間隔を設定します。1 ～ 255 の整数を入力します。
password	Cisco Intercompany Media Engine チケットのパスワードを設定します。US-ASCII 文字セットから印刷可能な文字を 10 文字以上 64 文字以下で、入力します。使用可能な文字は 0x21 ～ 0x73 であり、空白文字は除外されます。 パスワードは一度に 1 つしか設定できません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。
9.4(1)	このコマンドは、すべての **uc-ime** モード コマンドとともに廃止されました。

使用上のガイドライン

Cisco Intercompany Media Engine のチケットのエポックとパスワードを設定します。

このエポックには、パスワードが変更されるたびに更新される整数が保管されます。プロキシを初めて設定し、パスワードを初めて入力したとき、エポックの整数として 1 を入力します。このパスワードを変更するたびに、エポックを増やして新しいパスワードを示します。パスワードを変更するたびに、エポックの値を増やす必要があります。

通常、エポックは連続的に増やします。しかし、ASA では、エポックを更新するときに任意の値を選択できます。

エポック値を変更すると、現在のパスワードは無効になり、新しいパスワードを入力する必要があります。

20 文字以上のパスワードを推奨します。パスワードは一度に 1 つしか設定できません。

チケット パスワードはフラッシュ上に保存されます。**show running-config uc-ime** コマンドの出力には、パスワードの文字列ではなく、***** が表示されます。

(注) ASA 上で設定するエポックおよびパスワードは、Cisco Intercompany Media Engine サーバ上で設定されたエポックおよびパスワードと一致する必要があります。詳細については、Cisco Intercompany Media Engine サーバのマニュアルを参照してください。

例

次の例は、Cisco Intercompany Media Engine プロキシでチケットとエポックを設定する方法を示します。

```
ciscoasa(config)# uc-ime local_uc-ime_proxy
ciscoasa(config-uc-ime)# media-termination ime-media-term
ciscoasa(config-uc-ime)# ucm address 192.168.10.30 trunk-security-mode non-secure
ciscoasa(config-uc-ime)# ticket epoch 1 password password1234
hostname(config-uc-ime)# fallback monitoring timer 120
hostname(config-uc-ime)# fallback hold-down timer 30
```

関連コマンド

コマンド	説明
show running-config uc-ime	Cisco Intercompany Media Engine プロキシの実行コンフィギュレーションを表示します。
uc-ime	Cisco Intercompany Media Engine プロキシ インスタンスを ASA に作成します。

timeout（AAA サーバ ホスト）

AAA サーバとの接続確立を中断するまでに許容される、ホスト固有の最大応答時間を秒単位で設定するには、aaa サーバ ホスト モードで **timeout** コマンドを使用します。タイムアウト値を削除し、タイムアウトをデフォルト値の 10 秒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。

timeout *seconds*

no timeout

構文の説明

seconds	要求のタイムアウト間隔（1 ～ 60 秒）を指定します。この時間を超えると、ASA はプライマリ AAA サーバへの要求を断念します。スタンバイ AAA サーバが存在する場合、ASA は要求をそのバックアップ サーバに送信します。

デフォルト

デフォルトのタイムアウト値は 10 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドはすべての AAA サーバ プロトコル タイプで有効です。

ASA が AAA サーバへの接続を試行する時間の長さを指定するには、**timeout** コマンドを使用します。**retry-interval** コマンドを使用して、ASA が各接続試行の間で待機する時間を指定できます。

タイムアウトは、ASA がサーバとのトランザクションの完了を試みて費やす時間の合計です。再試行間隔は、タイムアウト期間中に通信を再試行する頻度を決定します。そのため、再試行間隔をタイムアウト値以上にすると、再試行は行われません。再試行が実行されるようにするには、再試行間隔をタイムアウト値より小さくする必要があります。

例

次に、ホスト 1.2.3.4 の RADIUS AAA サーバ「svrgrp1」が 30 秒のタイムアウト値と 10 秒の再試行間隔を使用するように設定する例を示します。ASA は、30 秒後に通信試行を中断するまでに 3 回試行を繰り返します。

```
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 30
ciscoasa(config-aaa-server-host)# retry-interval 10
ciscoasa(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードを開始して、ホスト固有の AAA サーバ パラメータを設定できるようにします。
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	現在の AAA コンフィギュレーションの値を表示します。

timeout（DNS サーバグループ）

次の DNS サーバを試行するまでの待機時間の合計を指定するには、DNS サーバグループ コンフィギュレーション モードで **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。

timeout *seconds*

no timeout [*seconds*]

構文の説明

seconds	タイムアウトを 1 ～ 30 の範囲で指定します（秒単位）。デフォルト値は 2 秒です。ASA がサーバのリストを再試行するたびに、このタイムアウトは倍増します。dns サーバ グループ コンフィギュレーション モードで **retries** コマンドを使用して、再試行回数を設定できます。

デフォルト

デフォルトのタイムアウトは 2 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

例

次に、DNS サーバ グループ「dnsgroup1」のタイムアウトを 1 秒に設定する例を示します。

```
ciscoasa(config)# dns server-group dnsgroup1
ciscoasa(config-dns-server-group)# dns timeout 1
```

関連コマンド

コマンド	説明
clear configure dns	ユーザが作成した DNS サーバ グループをすべて削除し、デフォルト サーバ グループの属性をデフォルト値にリセットします。
domain-name	デフォルトのドメイン名を設定します。
retries	ASA が応答を受信しないときに、DNS サーバのリストを再試行する回数を指定します。
show running-config dns server-group	現在の実行中の DNS サーバ グループ コンフィギュレーションを表示します。

timeout（グローバル）

さまざまな機能に対応するグローバルな最大アイドル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 **timeout** コマンドを使用します。すべてのタイムアウト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。単一の機能をデフォルトにリセットするには、**timeout** コマンドにデフォルト値を指定して再度入力します。

timeout {**conn** | **conn-holddown** | **floating-conn** | **h225** | **h323** | **half-closed** | **icmp** | **icmp-error** | **igp stale-route** | **mgcp** | **mgcp-pat** | **pat-xlate** | **sctp** | **sip** | **sip-disconnect** | **sip-invite** | **sip_media** | **sip-provisional-media** | **sunrpc** | **tcp-proxy-reassembly** | **udp** | **xlate**} *hh*:*mm*:*ss*

timeout uauth *hh*:*mm*:*ss* [**absolute** | **inactivity**]

no timeout

構文の説明

絶対	（**uauth** のオプション）uauth timeout が期限切れになった後、再認証を要求します。デフォルトでは、**absolute** キーワードはイネーブルです。非アクティブな状態が一定時間経過した後 uauth タイマーがタイムアウトするように設定するには、代わりに **inactivity** キーワードを入力します。
conn	接続を閉じるまでのアイドル時間を 0:5:0 ～ 1193:0:0 の範囲で指定します。デフォルトは 1 時間（1:0:0）です。接続がタイムアウトしないようにするには、**0** を使用します。
conn-holddown	接続に使用されるルートが存在しなくなったり非アクティブな場合に、接続を維持する必要がある時間。このホールドダウン時間内にルートがアクティブにならなければ、接続は解放されます。接続ホールドダウン タイマーの目的は、ルートが発生してすぐにダウンする可能性がある場合に、ルート フラッピングの影響を減らすことです。ルートの収束がもっと早く発生するようにホールドダウン タイマーを減らすことができます。デフォルトは 15 秒です。範囲は 00:00:00 ～ 00:00:15 です。
floating-conn	同じネットワークへの複数のルートが存在しており、それぞれメトリックが異なる場合、ASA は接続確立時点でメトリックが最良のルートを使用します。より適切なルートが使用可能になった場合は、このタイムアウトによって接続が閉じられるので、その適切なルートを使用して接続を再確立できます。デフォルトは 0 です（接続はタイムアウトしません）。より良いルートを使用できるようにするには、タイムアウト値を 0:0:30 ～ 1193:0:0 の間に設定します。
hh:*mm*:*ss*	タイムアウトを、時間、分、秒で指定します。接続をタイムアウトしない場合は、**0** を使用します（可能な場合）。
h225	H.225 シグナリング接続を閉じるまでのアイドル時間を 0:0:0 ～ 1193:0:0 の範囲で指定します。デフォルトは 1 時間（1:0:0）です。タイムアウト値を 0:0:1 に指定すると、タイマーはディセーブルになり、TCP 接続はすべてのコールがクリアされるとすぐに切断されます。
h323	H.245（TCP）および H.323（UDP）メディア接続を閉じるまでのアイドル時間を 0:0:0 ～ 1193:0:0 の範囲で指定します。デフォルトは 5 分（0:5:0）です。H.245 と H.323 のいずれのメディア接続にも同じ接続フラグが設定されているため、H.245（TCP）接続は H.323（RTP および RTCP）メディア接続とアイドル タイムアウトを共有します。

half-closed	TCP half-closed 接続が解放されるまでのアイドル時間を 0:5:0（9.1(1) 以前の場合）または 0:0:30（9.1(2) 以降の場合）～ 1193:0:0 の範囲で指定します。デフォルトは 10 分（0:10:0）です。接続がタイムアウトしないようにするには、**0** を使用します。
icmp	ICMP のアイドル時間を 0:0:2 ～ 1193:0:0 の範囲で指定します。デフォルトは 2 秒（0:0:2）です。
icmp-error	ASA が ICMP エコー応答パケットを受信してから ICMP 接続を削除するまでのアイドル時間に、0:0:0 ～ 0:1:0 の値、または **timeout icmp** 値のいずれか低い方を指定します。デフォルトは **0**（ディセーブル）です。このタイムアウトが無効で、ICMP インスペクションを有効にすると、ASA では、エコー応答が受信されるとすぐに ICMP 接続を削除します。したがってその（すでに閉じられた）接続用に生成されたすべての ICMP エラーは破棄されます。このタイムアウトは ICMP 接続の削除を遅らせるので、重要な ICMP エラーを受信することが可能になります。
igp stale-route	古いルートをルータの情報ベースから削除する前に保持するアイドル時間を指定します。これらのルートは OSPF などの内部ゲートウェイ プロトコル用です。デフォルトは 70 秒（00:01:10）です。指定できる範囲は 00:00:10 ～ 00:01:40 です。
inactivity	（**uauth** のオプション）非アクティブ タイムアウトが期限切れになった後、uauth 再認証を要求します。
mgcp	MGCP メディア接続を削除するまでのアイドル時間を 0:0:0 ～ 1193:0:0 の範囲で設定します。デフォルトは、5 分（0:5:0）です。
mgcp-pat	MGCP PAT 変換を削除するまでの絶対間隔を 0:0:0 ～ 1193:0:0 の範囲で設定します。デフォルトは 5 分（0:5:0）です。
pat-xlate	PAT 変換スロットが解放されるまでのアイドル時間を 0:0:30 ～ 0:5:0 の範囲で指定します。デフォルトは 30 秒です。前の接続がアップストリーム デバイスで引き続き開いている可能性があるため、開放された PAT ポートを使用する新しい接続をアップストリーム ルータが拒否する場合、このタイムアウトを増やすことができます。
sctp	Stream Control Transmission Protocol（SCTP）の接続が閉じるまでのアイドル時間を 0:1:0 ～ 1193:0:0 の間で指定します。デフォルトは 2 分（0:2:0）です。
sip	SIP 制御接続を閉じるまでのアイドル時間を 0:5:0 ～ 1193:0:0 の範囲で指定します。デフォルトは、30 分（0:30:0）です。接続がタイムアウトしないようにするには、**0** を使用します。
sip-disconnect	CANCEL メッセージまたは BYE メッセージで 200 OK を受信しなかった場合に、SIP セッションを削除するまでのアイドル時間を 0:0:1 ～ 00:10:0 の範囲で指定します。デフォルトは 2 分（0:2:0）です。
sip-invite	（任意）暫定応答のピンホールとメディア xlate を閉じるまでのアイドル時間を 0:1:0 ～ 1193:0:0 の範囲で指定します。デフォルトは、3 分（0:3:0）です。
sip_media	SIP メディア接続を閉じるまでのアイドル時間を 0:1:0 ～ 1193:0:0 の範囲で指定します。デフォルトは 2 分（0:2:0）です。接続がタイムアウトしないようにするには、**0** を使用します。 SIP メディア タイマーは、SIP UDP メディア パケットを使用する SIP RTP/RTCP で、UDP 非アクティブ タイムアウトの代わりに使用されます。
sip-provisional-media	SIP プロビジョナル メディア接続のタイムアウト値を 0:1:0 ～ 1193:0:0 の範囲で指定します。デフォルトは 2 分（0:2:0）です。

sunrpc	SUNRPC スロットを閉じるまでのアイドル時間を 0:1:0 ～ 1193:0:0 の範囲で指定します。デフォルトは 10 分（0:10:0）です。接続がタイムアウトしないようにするには、**0** を使用します。
tcp-proxy-reassembly	再構築のためバッファ内で待機しているパケットをドロップするまでのアイドル タイムアウトを 0:0:10 ～ 1193:0:0 の範囲で設定します。デフォルトは、1 分（0:1:0）です。
uauth	認証および認可キャッシュがタイムアウトし、ユーザが次回接続時に再認証が必要となるまでの継続時間を 0:0:0 ～ 1193:0:0 の範囲で指定します。デフォルトは 5 分（0:5:0）です。デフォルトのタイマーは **absolute** です。**inactivity** キーワードを入力すると、非アクティブになってから一定の期間後にタイムアウトが発生するように設定できます。**uauth** 継続時間は、**xlate** 継続時間より短く設定する必要があります。キャッシュをディセーブルにするには、**0** に設定します。接続に受動 FTP を使用している場合、または Web 認証に **virtual http** コマンドを使用している場合は、**0** を使用しないでください。
udp	UDP スロットが解放されるまでのアイドル時間を指定します。有効な値は 0:1:0 ～ 1193:0:0 です。デフォルトは 2 分（0:2:0）です。接続がタイムアウトしないようにするには、**0** を使用します。
xlate	変換スロットが解放されるまでのアイドル時間を指定します。有効な値は 0:1:0 ～ 1193:0:0 です。デフォルトは 3 時間（3:0:0）です。

デフォルト

デフォルトの設定は次のとおりです。

- **conn** は 1 時間（**1:0:0**）です。
- **conn-holddown** は 15 秒（**0:0:15**）です。
- **floating-conn** はタイムアウトになりません（**0**）。
- **h225** は 1 時間（**1:0:0**）です。
- **h323** は 5 分（**0:5:0**）です。
- **half-closed** は 10 分（**0:10:0**）です。
- **icmp** は 2 秒（**0:0:2**）です。
- **icmp-error** はタイムアウトになりません（**0**）。
- **igp stale-route** は 70 秒（**00:01:10**）です。
- **mgcp** は 5 分（**0:5:0**）です。
- **mgcp-pat** は 5 分（**0:5:0**）です。
- **rpc** は 5 分（**0:5:0**）です。
- **sctp** は 2 分（**0:2:0**）です。
- **sip** は 30 分（**0:30:0**）です。
- **sip-disconnect** は 2 分（**0:2:0**）です。
- **sip-invite** は 3 分（**0:3:0**）です。
- **sip_media** は 2 分（**0:2:0**）です。
- **sip-provisional-media** は 2 分（**0:2:0**）です。
- **sunrpc** は 10 分（**0:10:0**）です。
- **tcp-proxy-reassembly** は 1 分（**0:1:0**）です。

- **uauth** は 5 分（**0:5:0**）**絶対時間**です。
- **udp** は 2 分（**0:02:0**）です。
- **xlate** は 3 時間（**3:0:0**）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	**mgcp-pat**、**sip-disconnect**、および **sip-invite** キーワードが追加されました。
7.2(4)/8.0(4)	**sip-provisional-media** キーワードが追加されました。
7.2(5)/8.0(5)/8.1(2)/8.2(1)	**tcp-proxy-reassembly** キーワードが追加されました。
8.2(5)/8.4(2)	**floating-conn** キーワードが追加されました。
8.4(3)	**pat-xlate** キーワードが追加されました。
9.1(2)	最小 **half-closed** 値が 30 秒（0:0:30）に引き下げられました。
9.4(3)/9.6(2)	**conn-holddown** キーワードが追加されました。
9.5(2)	**sctp** キーワードが追加されました。
9.7(1)	**igp stale-route** キーワードが追加されました。
9.8(1)	**icmp-error** キーワードが追加されました。

使用上のガイドライン

timeout コマンドを使用すると、グローバルにタイムアウトを設定できます。一部の機能では、コマンドで指定されたトラフィックに対し、**set connection timeout** コマンドが優先されます。

timeout コマンドの後に、キーワードと値を複数入力できます。

接続タイマー（**conn**）は変換タイマー（**xlate**）より優先されます。変換タイマーは、すべての接続がタイムアウトになった後にのみ動作します。

例

次に、最大アイドル時間を設定する例を示します。

```
ciscoasa(config)# timeout uauth 0:5:0 absolute uauth 0:4:0 inactivity
ciscoasa(config)# show running-config timeout
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00
sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute uauth 0:04:00 inactivity
```

関連コマンド

コマンド	説明
clear configure timeout	タイムアウト コンフィギュレーションをクリアし、デフォルトにリセットします。
set connection timeout	Modular Policy Framework を使用して接続タイムアウトを設定します。
show running-config timeout	指定されたプロトコルのタイムアウト値を表示します。

timeout（policy-map type inspect gtp > パラメータ）

GTP セッションの非アクティブ状態タイマーを変更するには、パラメータ コンフィギュレーション モードで **timeout** コマンドを使用します。パラメータ コンフィギュレーション モードにアクセスするには、まず **policy-map type inspect gtp** コマンドを入力します。これらの間隔にデフォルト値を設定するには、このコマンドの **no** 形式を使用します。

timeout {**endpoint** | **gsn** | **pdp-context** | **request** | **signaling** | **t3-response** | **tunnel**} *hh*:*mm*:*ss*

no timeout {**endpoint** | **gsn** | **pdp-context** | **request** | **signaling** | **t3-response** | **tunnel**} *hh*:*mm*:*ss*

構文の説明

hh:*mm*:*ss*	指定したサービスのアイドル タイムアウト（時間:分:秒の形式）。タイムアウトを設定しない場合は、番号に 0 を指定します。
エンドポイント	GTP エンドポイントが削除されるまでの非アクティブ時間の最大値。
gsn	GSN が削除されるまでの非アクティブ時間の最大値。 9.5(1) 以降、このキーワードは削除され、**endpoint** キーワードに置き換えられました。
pdp-context	GTP セッションの PDP コンテキストを削除するまでの非アクティブ時間の最大値。GTPv2 では、これはベアラー コンテキストです。
request	要求キューから要求が削除されるまでの非アクティブ時間の最大値。廃棄された要求に対する後続の応答もすべて廃棄されます。
signaling	GTP シグナリングが削除されるまでの非アクティブ時間の最大値。
t3-response	接続を除去する前に応答を待機する最大時間。
tunnel	GTP トンネルが切断されるまでの非アクティブ時間の最大値。

デフォルト

endpoint、**gsn**、**pdp-context**、および **signaling** のデフォルトは 30 分です。

request のデフォルトは 1 分です。

tunnel のデフォルトは 1 時間です（PDP コンテキスト削除要求を受信しない場合）。

t3-response のデフォルトは、20 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.5(1)	**gsn** キーワードは **endpoint** に置き換えられました。

使用上のガイドライン

GTP インスペクションで使用されるデフォルト タイムアウトを変更するには、このコマンドを使用します。

例

次に、要求キューのタイムアウト値を 2 分に設定する例を示します。

```
ciscoasa(config)# policy-map type inspect gtp gtp-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# timeout request 00:02:00
```

関連コマンド

コマンド	説明
clear service-policy inspect gtp	グローバルな GTP 統計情報をクリアします。
inspect gtp	アプリケーション インスペクションに使用する特定の GTP マップを適用します。
show service-policy inspect gtp	GTP コンフィギュレーションを表示します。

timeout（policy-map type inspect m3ua > パラメータ）

M3UA セッションの非アクティブ状態タイマーを変更するには、パラメータ コンフィギュレーション モードで **timeout** コマンドを使用します。パラメータ コンフィギュレーション モードにアクセスするには、まず **policy-map type inspect m3ua** コマンドを入力します。これらの間隔にデフォルト値を設定するには、このコマンドの **no** 形式を使用します。

timeout {**endpoint** | **session**} *hh*:*mm*:*ss*

no timeout {**endpoint** | **session**} *hh*:*mm*:*ss*

構文の説明

hh:*mm*:*ss*	指定したサービスのアイドル タイムアウト（時間:分:秒の形式）。タイムアウトを設定しない場合は、番号に 0 を指定します。
エンドポイント	M3UA エンドポイントの統計情報が削除されるまでの非アクティブ時間の最大値。デフォルトは 30 分です。
session	厳密な ASP 状態の確認を有効にしている場合の、M3UA セッションを削除するためのアイドル タイムアウト（hh:mm:ss の形式）。デフォルトは 30 分（0:30:00）です。このタイムアウトを無効にすると、失効したセッションの削除を防止できます。

デフォルト

endpoint および **session** のデフォルトは 30 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。

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

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。
9.7(1)	**session** キーワードが追加されました。

使用上のガイドライン

M3UA インスペクションで使用されるデフォルト タイムアウトを変更するには、このコマンドを使用します。

例

次の例では、45 分のエンドポイントのタイムアウトを設定します。

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# timeout endpoint 00:45:00
```

関連コマンド

コマンド	説明
inspect m3ua	M3UA インスペクションをイネーブルにします。
policy-map type inspect	インスペクション ポリシー マップを作成します。
show service-policy inspect m3ua	M3UA 統計情報を表示します。
strict-asp-state	厳密な M3UA ASP 状態の確認をイネーブルにします。

timeout（policy-map type inspect radius-accounting > パラメータ）

RADIUS アカウンティング ユーザの非アクティブ状態タイマーを変更するには、パラメータ コンフィギュレーション モードで **timeout** コマンドを使用します。パラメータ コンフィギュレーション モードにアクセスするには、まず **policy-map type inspect radius-accounting** コマンドを入力します。これらの間隔にデフォルト値を設定するには、このコマンドの **no** 形式を使用します。

timeout users *hh*:*mm*:*ss*

no timeout users *hh*:*mm*:*ss*

構文の説明

hh:*mm*:*ss*	これはタイムアウトで、*hh* は時間、*mm* は分、*ss* は秒を示し、これら 3 つの要素はコロン(:)で分けられます。値 0 は、すぐには絶対に終了しないことを意味します。デフォルトは 1 時間です。
users	ユーザのタイムアウトを指定します。

デフォルト

ユーザのデフォルトのタイムアウトは 1 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。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、ユーザのタイムアウト値を 10 分に設定する例を示します。

```
hostname(config)# policy-map type inspect radius-accounting ra
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# timeout user 00:10:00
```

関連コマンド

コマンド	説明
inspect radius-accounting	RADIUS アカウンティングのインスペクションを設定します。
パラメータ	インスペクション ポリシー マップのパラメータを設定します。

timeout（type echo）

SLA 動作が要求パケットへの応答を待機する時間を設定するには、type echo コンフィギュレーション モードで **timeout** コマンドを使用します。type echo コンフィギュレーション モードにアクセスするには、まず **sla monitor** コマンドを入力します。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。

timeout *milliseconds*

no timeout

構文の説明

milliseconds	0 ～ 604800000

デフォルト

デフォルトのタイムアウト値は 5000 ミリ秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
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

frequency コマンドを使用して、SLA 動作が要求パケットを送信する頻度を設定し、**timeout** コマンドを使用して、SLA 動作がそれらの要求への応答の受信を待機する時間を設定できます。**timeout** コマンドには、**frequency** コマンドに指定する値より大きい値は指定できません。

例

次の例では、ID が 123 の SLA 動作を設定し、ID が 1 のトラッキング エントリを作成して、SLA の到達可能性を追跡しています。SLA 動作の頻度を 10 秒、しきい値を 2500 ミリ秒、タイムアウト値を 4000 ミリ秒に設定しています。

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
ciscoasa(config-sla-monitor-echo)# threshold 2500
ciscoasa(config-sla-monitor-echo)# timeout 4000
ciscoasa(config-sla-monitor-echo)# frequency 10
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
frequency	SLA 動作を繰り返す頻度を指定します。
sla monitor	SLA モニタリング動作を定義します。

timeout assertion

SAML タイムアウトを設定するには、webvpn コンフィギュレーション モードで **timeout assertion** コマンドを使用します。

timeout assertion *number of seconds*

構文の説明

number of seconds	SAML IdP タイムアウト(秒)。

デフォルト

デフォルトは、なしです。アサーションの NotBefore と NotOnOrAfter によって有効期間が決定されることを意味します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.5.2	このコマンドが追加されました。

使用上のガイドライン

指定すると、NotBefore とタイムアウト(秒単位)の合計が NotOnOrAfter よりも前になる場合、この設定が NotOnOrAfter よりも優先されます。指定しない場合、アサーションの NotBefore と NotOnOrAfter が妥当性を判断するために使用されます。config-webvpn-saml-idp でタイムアウト値を入力する場合、アサーションと秒数の両方が必要です。

例

次に、クライアントレス VPN ベースの URL、SAML 要求署名、および SAML アサーション タイムアウトの設定例を示します。

```
ciscoasa(config-webvpn-saml-idp)# base url https://172.23.34.222
ciscoasa(config-webvpn-saml-idp)# signature
ciscoasa(config-webvpn-saml-idp)# timeout assertion 7200
```

timeout pinhole

DCERPC ピンホールのタイムアウトを設定し、2 分のグローバル システム ピンホール タイムアウトを上書きするには、パラメータ コンフィギュレーション モードで **timeout pinhole** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

timeout pinhole *hh:mm:ss*

no timeout pinhole

構文の説明

hh:mm:ss	ピンホール接続のタイムアウト。指定できる値は 0:0:1 ～ 1193:0:0 です。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、DCERPC インスペクション ポリシー マップでピンホール接続のピンホール タイムアウトを設定する例を示します。

```
ciscoasa(config)# policy-map type inspect dcerpc dcerpc_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# timeout pinhole 0:10:00
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

timeout secure-phones（廃止）

電話プロキシ データベースからセキュア フォン エントリを削除するまでのアイドル タイムアウトを設定するには、電話プロキシ コンフィギュレーション モードで **timeout secure-phones** コマンドを使用します。タイムアウト値をデフォルトの 5 分に戻すには、このコマンドの **no** 形式を使用します。

timeout secure-phones *hh:mm:ss*

no timeout secure-phones *hh:mm:ss*

構文の説明

hh:mm:ss	オブジェクトを削除するまでのアイドル タイムアウトを指定します。デフォルトは 5 分です。

デフォルト

セキュア フォン タイムアウトのデフォルト値は 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。

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

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。
9.4(1)	このコマンドは、すべての **phone-proxy** モード コマンドとともに廃止されました。

使用上のガイドライン

セキュア フォンによって起動時に必ず CTL ファイルが要求されるため、電話プロキシは、電話をセキュアとしてマークするデータベースを作成します。セキュア フォン データベースのエントリは、設定された指定タイムアウト後に（**timeout secure-phones** コマンドを介して）削除されます。エントリのタイムスタンプは、電話プロキシが SIP 電話の登録更新および SCCP 電話のキープアライブを受信するたびに更新されます。

timeout secure-phones コマンドのデフォルト値は 5 分です。SCCP キープアライブおよび SIP レジスタ更新の最大タイムアウト値より大きい値を指定します。たとえば、SCCP キープアライブが 1 分間隔に指定され、SIP レジスタ更新が 3 分に設定されている場合は、このタイムアウト値には 3 分より大きい値を設定します。

例

次に、**timeout secure-phones** コマンドを使用して、電話プロキシが 3 分後にセキュア フォン データベースのエントリをタイムアウトにするように設定する例を示します。

```
ciscoasa(config)# phone-proxy asa_phone_proxy
ciscoasa(config-phone-proxy)# tftp-server address 192.168.1.2 in interface outside
ciscoasa(config-phone-proxy)# tftp-server address 192.168.1.3 in interface outside
ciscoasa(config-phone-proxy)# media-termination address 192.168.1.4
ciscoasa(config-phone-proxy)# tls-proxy asa_tlsp
ciscoasa(config-phone-proxy)# ctl-file asactl
ciscoasa(config-phone-proxy)# timeout secure-phones 00:03:00
```

関連コマンド

コマンド	説明
phone-proxy	Phone Proxy インスタンスを設定します。

time-range

時間範囲コンフィギュレーション モードを開始し、トラフィック ルールにアタッチできる時間範囲、またはアクションを定義するには、グローバル コンフィギュレーション モードで **time-range** コマンドを使用します。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。

time-range *name*

no time-range *name*

構文の説明

name　時間範囲の名前。名前は 64 文字以下にする必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

時間範囲を作成してもデバイスへのアクセスは制限されません。**time-range** コマンドは時間範囲のみを定義します。時間範囲を定義した後、それをトラフィック ルールまたはアクションにアタッチできます。

時間ベース ACL を実装するには、**time-range** コマンドを使用して、週および 1 日の中の特定の時刻を定義します。次に、**access-list extended time-range** コマンドとともに使用して、時間範囲を ACL にバインドします。

時間範囲は ASA のシステム クロックに依存しています。ただし、この機能は、NTP 同期化により最適に動作します。

例

次に、時間範囲「New_York_Minute」を作成し、時間範囲コンフィギュレーション モードを開始する例を示します。

```
ciscoasa(config)# time-range New_York_Minute
ciscoasa(config-time-range)#
```

時間範囲を作成し、時間範囲コンフィギュレーション モードを開始した後、**absolute** コマンドと **periodic** コマンドを使用して時間範囲パラメータを定義できます。**time-range** コマンドの **absolute** キーワードと **periodic** キーワードをデフォルト設定に戻すには、時間範囲コンフィギュレーション モードで **default** コマンドを使用します。

時間ベース ACL を実装するには、**time-range** コマンドを使用して、週および 1 日の中の特定の時刻を定義します。その後、**access-list extended** コマンドを使用して、時間範囲を ACL にバインドします。次に、ACL「Sales」を時間範囲「New_York_Minute」にバインドする例を示します。

```
ciscoasa(config)# access-list Sales line 1 extended deny tcp host 209.165.200.225 host
209.165.201.1 time-range New_York_Minute
ciscoasa(config)#
```

ACL の詳細については、**access-list extended** コマンドを参照してください。

関連コマンド

コマンド	説明
絶対	時間範囲が有効になる絶対時間を定義します。
access-list extended	ASA 経由の IP トラフィックを許可または拒否するためのポリシーを設定します。
デフォルト	**time-range** コマンドの **absolute** キーワードと **periodic** キーワードをデフォルト設定に戻します。
定期	時間範囲機能をサポートする機能に対して、定期的な（週単位の）時間範囲を指定します。

timers bgp

BGP ネットワーク タイマーを調整するには、ルータ BGP コンフィギュレーション モードで **timers bgp** コマンドを使用します。BGP のタイミング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。

timers bgp *keepalive holdtime* [*min-holdtime*]

no timers bgp *keepalive holdtime* [*min-holdtime*]

構文の説明

Keepalive（キープアライブ）	Cisco IOS ソフトウェアがピアにキープアライブ メッセージを送信する頻度（秒単位）。デフォルトは 60 秒です。範囲は 0 ～ 65535 です。
holdtime	キープアライブ メッセージを受信できない状態が継続して、ピアがデッドであるとソフトウェアが宣言するまでの時間（秒単位）。デフォルトは 180 秒です。範囲は 0 ～ 65535 です。
min-holdtime	（オプション）BGP ネイバーからの最小許容ホールド タイムを指定する間隔（秒単位）。最小許容ホールド タイムは、*holdtime* 引数で指定された間隔以下にする必要があります。範囲は 0 ～ 65535 です。

デフォルト

keepalive：60 秒
holdtime：180 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。

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

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

holdtime 引数を 20 秒未満の値の値に設定すると、次の警告が表示されます。「A hold time of less than 20 seconds increases the chances of peer flapping」

最小許容ホールド タイム間隔が、指定されたホールド タイムを超過する場合は、「Minimum acceptable hold time should be less than or equal to the configured hold time」という通知が表示されます。

(注) BGP ルータに最小許容ホールド タイムが設定されている場合、リモート BGP ピア セッションは、リモート ピアが最小許容ホールド タイム間隔以上のホールド タイムをアドバタイズする場合にのみ確立されます。最小許容ホールド タイム間隔が、設定されたホールド タイムを超過する場合、次回のリモート セッション確立の試行は失敗し、ローカル ルータは「unacceptable hold time」という示す通知を送信します。

例

次に、キープアライブ タイマーを 70 秒、ホールド タイム タイマーを 130 秒、最小許容ホールド タイム間隔を 100 秒に変更する例を示します。

```
ciscoasa(config)# router bgp 45000
ciscoasa(config-router)# timers bgp 70 130 100
```

timers lsa arrival

ASA が OSPFv3 ネイバーから同じ LSA を受信する最小間隔を設定するには、IPv6 ルータ コンフィギュレーション モードで **timers lsa arrival** 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。

timers lsa arrival *milliseconds*

no timers lsa arrival *milliseconds*

構文の説明

milliseconds	ネイバー間で着信する同じ LSA を受信する間に経過する必要がある最小遅延を指定します（ミリ秒単位）。有効値の範囲は 0 ～ 600,000 ミリ秒です。

デフォルト

デフォルトは 1000 ミリ秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
IPv6 ルータ コンフィギュレーション	• Yes	—	• Yes	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用して、ネイバーから着信する同じ LSA を受信する間に経過する必要がある最小間隔を指定します。

例

次に、同じ LSA を受信する最小間隔を 2000 ミリ秒に設定する例を示します。

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-rtr)# log-adjacency-changes
ciscoasa(config-rtr)# timers lsa arrival 2000
```

関連コマンド

コマンド	説明
ipv6 router ospf	OSPFv3 のルータ コンフィギュレーション モードを開始します。
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。
timers pacing flood	OSPFv3 ルーティング プロセスの LSA フラッド パケット ペーシングを設定します。

timers lsa-group-pacing

OSPF リンク ステート アドバタイズメント（LSA）を 1 つのグループに収集し、更新、チェックサム、または期限切れにする間隔を指定するには、ルータ コンフィギュレーション モードで **timers lsa-group-pacing** 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。

timers lsa-group-pacing *seconds*

no timers lsa-group-pacing [*seconds*]

構文の説明

seconds	OSPF リンク ステート アドバタイズメント（LSA）を 1 つのグループに収集し、更新、チェックサム、または期限切れにする間隔。有効な値は、10 ～ 1800 秒です。

デフォルト

デフォルトの間隔は 240 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
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

OSPF リンク ステート アドバタイズメント（LSA）を 1 つのグループに収集し、更新、チェックサム、または期限切れにする間隔を変更するには **timers lsa-group-pacing** *seconds* コマンドを使用します。デフォルトのタイマー値に戻すには、**no timers lsa-group-pacing** コマンドを使用します。

例

次に、LSA のグループ処理間隔を 500 秒に設定する例を示します。

```
ciscoasa(config-rtr)# timers lsa-group-pacing 500
ciscoasa(config-rtr)#
```

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。
timers spf	最短パス優先（SPF）計算遅延とホールド タイムを指定します。

timers pacing flood

LSA フラッド パケット ペーシングを設定するには、IPv6 ルータ コンフィギュレーション モードで **timers pacing flood** コマンドを使用します。デフォルトのフラッド パケット ペーシング値に戻すには、このコマンドの **no** 形式を使用します。

timers pacing flood *milliseconds*

no timers pacing flood *milliseconds*

構文の説明

milliseconds	フラッディング キュー内の LSA がアップデート間にペーシング処理される時間を指定します（ミリ秒単位）。設定できる範囲は 5 ～ 100 ミリ秒です。

デフォルト

デフォルトは 33 ミリ秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
IPv6 ルータ コンフィギュレーション	• Yes	—	• Yes	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用して、LSA フラッド パケット ペーシングを設定します。

例

次の例は、OSPFv3 に対して LSA フラッド パケット ペーシング更新が 20 ミリ秒間隔で発生する設定を示しています。

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-rtr)# timers pacing flood 20
```

関連コマンド

コマンド	説明
ipv6 router ospf	IPv6 のルータ コンフィギュレーション モードを開始します。
timers pacing lsa-group	OSPFv3 LSA を収集してグループ化し、更新、チェックサム、または期限切れにする間隔を指定します。

timers pacing lsa-group

OSPFv3 LSA を 1 つのグループに収集し、更新、チェックサム、または期限切れにする間隔を指定するには、IPv6 ルータ コンフィギュレーション モードで **timers pacing lsa-group** 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。

timers pacing lsa-group *seconds*

no timers pacing lsa-group [*seconds*]

構文の説明

seconds	LSA を 1 つのグループに収集し、更新、チェックサム、または期限切れにする間隔を指定します（秒単位）。有効な値は、10 ～ 1800 秒です。

デフォルト

デフォルトの間隔は 240 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
IPv6 ルータ コンフィギュレーション	• Yes	—	• Yes	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用して、OSPFv3 LSA を 1 つのグループに収集し、更新、チェックサム、または期限切れにする間隔を指定します。

例

次に、OSPFv3 ルーティング プロセス 1 に対して、LSA グループ間の OSPFv3 グループ パケット ペーシング更新が 300 秒間隔で発生するように設定する例を示します。

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-rtr)# timers pacing lsa-group 300
```

関連コマンド

コマンド	説明
ipv6 router ospf	IPv6 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。
timers pacing flood	OSPFv3 ルーティング プロセスの LSA フラッド パケット ペーシングを設定します。
timers pacing retransmission	LSA 再送信パケット ペーシングを設定します。

timers pacing retransmission

リンクステート アドバタイズメント（LSA）の再送信パケット ペーシングを設定するには、ルータ コンフィギュレーション モードで **timers pacing retransmission** コマンドを使用します。デフォルトの再送信パケット ペーシング値に戻すには、このコマンドの **no** 形式を使用します。

timers pacing retransmission *milliseconds*

no timers pacing retransmission

構文の説明

milliseconds	再送信キュー内の LSA がペーシング処理される間隔を指定します（ミリ秒単位）。有効な値は、5 ～ 200 ミリ秒です。

デフォルト

デフォルトの間隔は 66 ミリ秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
IPv6 ルータ コンフィギュレーション	• Yes	—	• Yes	—	—

コマンド履歴

リリース	変更内容
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

Open Shortest Path First（OSPF）再送信ペーシング タイマーを設定すると、OSPF 伝送キュー内の連続リンクステート アップデート パケット間のパケット間スペースを制御できます。このコマンドを使用すると、LSA 更新が発生するレートを制御できます。したがって、エリアが非常に多くの数の LSA で満たされた場合に発生する可能性のある、CPU またはバッファの高い使用率を低減させることができます。OSPF パケット再送信ペーシング タイマーのデフォルト設定は、大半の OSPF 配備に適しています。

（注） OSPF パケット フラッディングの要件を満たす他のオプションをすべて使用した場合に限り、パケット再送信ペーシング タイマーを変更してください。特に、ネットワーク オペレータは、デフォルトのフラッディング タイマーを変更する前に、集約、スタブ エリアの使用方法、キューの調整、およびバッファの調整を優先して行う必要があります。

さらに、タイマー値を変更するガイドラインはなく、各 OSPF 配備は一意であり、ケースバイケースで考慮する必要があります。ネットワーク オペレータは、デフォルトのパケット再送信ペーシング タイマー値を変更することで生じるリスクを念頭に置く必要があります。

例

次に、OSPF ルーティング プロセス 1 に対して、LSA フラッド ペーシング更新が 55 ミリ秒間隔で発生するように設定する例を示します。

```
hostname(config)# router ospf 1
hostname(config-router)# timers pacing retransmission 55
```

関連コマンド

コマンド	説明
ipv6 router ospf	IPv6 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。
timers pacing flood	OSPFv3 ルーティング プロセスの LSA フラッド パケット ペーシングを設定します。

timers spf

最短パス優先(SPF)計算遅延とホールド タイムを指定するには、ルータ コンフィギュレーション モードで **timers spf** 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。

timers spf *delay holdtime*

no timers spf [*delay holdtime*]

構文の説明

delay	OSPF がトポロジ変更を受信してから最短パス優先(SPF)計算を開始するまでの遅延時間を 1 ～ 65535 の範囲(秒単位)で指定します。
holdtime	2 つの連続する SPF 計算の間のホールド タイム(秒単位)。有効な値は、1 ～ 65535 です。

デフォルト

デフォルトの設定は次のとおりです。

- *delay* は 5 秒です。
- *holdtime* は 10 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

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

使用上のガイドライン

OSPF プロトコルがトポロジ変更を受信してから計算を開始するまでの遅延時間と、2 つの連続する SPF 計算の間のホールド タイムを設定するには、**timers spf** コマンドを使用します。デフォルトのタイマー値に戻すには、**no timers spf** コマンドを使用します。

例

次に、SPF 計算遅延を 10 秒に設定し、SPF 計算ホールド タイムを 20 秒に設定する例を示します。

```
ciscoasa(config-router)# timers spf 10 20
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 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。
timers lsa-group-pacing	OSPF リンク ステート アドバタイズメント（LSA）を収集し、更新、チェックサム、または期限切れにする間隔を指定します。

timers throttle

Open Shortest Path First（OSPF）のリンクステート アドバタイズメント（LSA）の生成または SPF の生成に関するレート制限値を設定するには、ルータ OSPF または IPv6 ルータ OSPF コンフィギュレーション モードで **timers throttle** 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。

timers throttle {**lsa** | **spf**} *start-interval hold-interval max-interval*

no timers throttle {**lsa** | **spf**}

構文の説明

lsa	LSA スロットリングを設定します。
start-interval	LSA の最初のオカレンスを生成する遅延を指定します（ミリ秒単位）。SPF 計算への変更を受信する遅延を指定します（ミリ秒単位）。 LSA の最初のオカレンスを生成する最小遅延を指定します（ミリ秒単位）。 （注） LSA の最初のインスタンスは、ローカル OSPF トポロジの変更直後に生成されます。次の LSA は、*start-interval* の後にのみ生成されます。 有効な値は、0 ～ 600,000 ミリ秒です。デフォルト値は 0 ミリ秒です。LSA は即座に送信されます。
hold-interval	同じ LSA を発信する最大遅延を指定します（ミリ秒単位）。1 番目と 2 番目の SPF 計算間の遅延を指定します（ミリ秒単位）。 LSA を生成する最小遅延を再度指定します（ミリ秒単位）。この値は、LSA 生成の後続のレート制限時間の計算に使用されます。有効な値は、1 ～ 600,000 ミリ秒です。デフォルト値は 5000 ミリ秒です。
max-interval	同じ LSA を発信する最小遅延を指定します（ミリ秒単位）。SPF 計算を待機する最大時間を指定します（ミリ秒単位）。 LSA を生成する最大遅延を再度指定します（ミリ秒単位）。有効な値は、1 ～ 600,000 ミリ秒です。デフォルト値は 5000 ミリ秒です。
spf	SPF スロットリングを設定します。

デフォルト

LSA スロットリング:

- *start-interval* の場合、デフォルト値は 0 ミリ秒です。
- *hold-interval* の場合、デフォルト値は 5000 ミリ秒です。
- *max-interval* の場合、デフォルト値は 5000 ミリ秒です。

SPF スロットリング:

- *start-interval* の場合、デフォルト値は 5000 ミリ秒です。
- *hold-interval* の場合、デフォルト値は 10000 ミリ秒です。
- *max-interval* の場合、デフォルト値は 10000 ミリ秒です。

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		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
IPv6 ルータ OSPF コンフィギュレーション	• **Yes**	—	• **Yes**	• **Yes**	—
ルータ OSPF コンフィギュレーション	• **Yes**	—	• **Yes**	• **Yes**	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。
9.2(1)	IPv6 のサポートが追加されました。

使用上のガイドライン

LSA および SPF スロットリングは、ネットワークが不安定になっている間に OSPF の LSA 更新速度を低下し、ミリ秒単位の LSA レート制限を提供することにより、より高速な OSPF コンバージェンスを許可するダイナミック メカニズムを提供します。

LSA スロットリングでは、最小時間または最大時間が最初のオカレンスの値よりも小さい場合、OSPF が自動的に最初のオカレンス値に修正します。同様に、指定された最大遅延が最小遅延よりも小さい場合、OSPF が自動的に最小遅延値に修正します。

SPF スロットリングでは、*hold-interval* または *max-interval* が *start-interval* よりも小さい場合、OSPF が自動的に *start-interval* の値に修正します。同様に、*max-interval* が *hold-interval* よりも小さい場合、OSPF が自動的に *hold-interval* の値に修正します。

例

次に、OSPFv3 LSA スロットリングをミリ秒単位で設定する例を示します。

```
ciscoasa(config)# ipv6 router ospf 10
ciscoasa(config-rtr)# timers throttle lsa 100 4000 5000
```

次に、LSA スロットリングで、指定された最大遅延値が最小遅延値を下回る場合に発生する自動修正の例を示します。

```
ciscoasa(config)# ipv6 router ospf 10
ciscoasa(config-rtr)# timers throttle lsa 100 50 50
% OSPFv3: Throttle timers corrected to: 100 100 100
ciscoasa(config-rtr)# show running-config ipv6
ipv6 router ospf 10
 timers throttle lsa 100 100 100
```

次に、OSPFv3 SPF スロットリングをミリ秒単位で設定する例を示します。

```
ciscoasa(config)# ipv6 router ospf 10
ciscoasa(config-rtr)# timers throttle spf 6000 12000 14000
```

次に、SPF スロットリングで、指定された最大遅延値が最小遅延値を下回る場合に発生する自動修正の例を示します。

```
ciscoasa(config)# ipv6 router ospf 10
ciscoasa(config-rtr)# timers throttle spf 100 50 50
% OSPFv3: Throttle timers corrected to: 100 100 100
ciscoasa(config-rtr)# show running-config ipv6
ipv6 router ospf 10
 timers throttle spf 100 100 100
```

関連コマンド

コマンド	説明
ipv6 router ospf	IPv6 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。
timers lsa-group-pacing	OSPFv3 LSA を収集し、更新、チェックサム、または期限切れにする間隔を指定します。

timestamp

IP オプション インスペクションにおいて、パケット ヘッダー内にタイム スタンプ（TS）オプションが存在する場合のアクションを定義するには、パラメータ コンフィギュレーション モードで **timestamp** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

timestamp action {allow | clear}

no timestamp action {allow | clear}

構文の説明

allow	タイム スタンプ IP オプションを含むパケットを許可します。
clear	パケット ヘッダーからタイム スタンプ オプションを削除してから、パケットを許可します。

デフォルト

デフォルトでは、IP オプション インスペクションは、タイム スタンプ オプションを含むパケットをドロップします。

IP オプション インスペクション ポリシー マップで **default** コマンドを使用するとデフォルト値を変更できます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.5(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、IP オプション インスペクション ポリシー マップで設定できます。

IP オプション インスペクションを設定して、どの IP パケットが所定の IP オプションを持ち、ASA を通過できるかを制御できます。変更せずにパケットを通過させたり、指定されている IP オプションをクリアしてからパケットを通過させたりできます。

例

次に、IP オプション インスペクションのアクションをポリシー マップで設定する例を示します。

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# timestamp action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

title

WebVPN ユーザがセキュリティ アプライアンスに接続したときに表示する WebVPN ページのタイトルをカスタマイズするには、webvpn カスタマイゼーション モードで **title** コマンドを使用します。

title {**text** | **style**} *value*

[**no**] **title** {**text** | **style**} *value*

コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

構文の説明

text	テキストを変更することを指定します。
style	スタイルを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

デフォルトのタイトル テキストは「WebVPN Service」です。

デフォルトのタイトル スタイルは、次のとおりです。

background-color:white;color:maroon;border-bottom:5px groove #669999;font-size:larger; vertical-align:middle;text-align:left;font-weight:bold

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
WebVPN カスタマイゼーション	• Yes	—	• Yes	—	—

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

タイトルを付けない場合は、*value* 引数を指定せずに **title text** コマンドを使用します。

style オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注） WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次の例では、タイトルがテキスト「Cisco WebVPN Service」でカスタマイズされています。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# title text Cisco WebVPN Service
```

関連コマンド

コマンド	説明
logo	WebVPN ページのロゴをカスタマイズします。
page style	カスケーディング スタイル シート（CSS）パラメータを使用して WebVPN ページをカスタマイズします。