C のコマンド

cache-time

CRL を期限切れと見なす前にキャッシュに残す時間を分単位で指定するには、**cache-time** コマンドを ca-crl コンフィギュレーション モードで使用します。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。

cache-time *refresh-time*

no cache-time

シンタックスの説明

refresh-time	CRL をキャッシュに残す時間（分）を指定します。範囲は 1 ～ 1,440 分です。CRL に NextUpdate フィールドがない場合、CRL はキャッシュされません。

デフォルト

デフォルト設定は 60 分です。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CRL コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

例

次の例では、ca-crl コンフィギュレーション モードに入り、トラストポイント central に 10 分のキャッシュ時間のリフレッシュ値を指定します。

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# cache-time 10
hostname(ca-crl)#
```

関連コマンド

コマンド	説明
crl configure	crl コンフィギュレーション モードに入ります。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。
enforcenextupdate	証明書で NextUpdate CRL フィールドを処理する方法を指定します。

call-agent

コール エージェントのグループを指定するには、**mgcp-map** コマンドを使用してアクセスできる **call-agent** コマンドを MGCP マップ コンフィギュレーション モードで使用します。この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。

call-agent *ip_address group_id*

no call-agent *ip_address group_id*

シンタックスの説明

ip_address	ゲートウェイの IP アドレス。
group_id	コール エージェント グループの ID （0 ～ 2147483647）。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

call-agent コマンドは、1 つまたは複数のゲートウェイを管理できるコール エージェントのグループを指定するために使用します。コール エージェントのグループ情報は、どのコール エージェントも応答を送信できるように、グループ内の（ゲートウェイがコマンドを送信する先以外の）コール エージェントに接続を開くために使用されます。*group_id* が同じコール エージェントは、同じグループに所属します。1 つのコール エージェントは複数のグループに所属できます。*group_id* オプションは 0 ～ 4294967295 の数字です。*ip_address* オプションでは、コール エージェントの IP アドレスを指定します。

例

次の例では、コール エージェント 10.10.11.5 と 10.10.11.6 がゲートウェイ 10.10.10.115 を制御できるようにし、コール エージェント 10.10.11.7 と 10.10.11.8 がゲートウェイ 10.10.10.116 と 10.10.10.117 の両方を制御できるようにしています。

```
hostname(config)# mgcp-map mgcp_inbound
hostname(config-mgcp-map)# call-agent 10.10.11.5 101
hostname(config-mgcp-map)# call-agent 10.10.11.6 101
hostname(config-mgcp-map)# call-agent 10.10.11.7 102
hostname(config-mgcp-map)# call-agent 10.10.11.8 102
hostname(config-mgcp-map)# gateway 10.10.10.115 101
hostname(config-mgcp-map)# gateway 10.10.10.116 102
hostname(config-mgcp-map)# gateway 10.10.10.117 102
```

関連コマンド

コマンド	説明
debug mgcp	MGCP に関するデバッグ情報の表示をイネーブルにします。
mgcp-map	MGCP マップを定義し、MGCP マップ コンフィギュレーション モードをイネーブルにします。
show mgcp	MGCP のコンフィギュレーションおよびセッション情報を表示します。

capture

パケット キャプチャ機能をイネーブルにして、パケットのスニッフィングやネットワーク障害を検出できるようにするには、**capture** コマンドを使用します。パケット キャプチャ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（このコマンドの **no** 形式の詳細については、「使用上のガイドライン」の項を参照してください）。

capture *capture_name* [**access-list** *access_list_name*] [**buffer** *buf_size*] [**ethernet-type** *type*] [**interface** *interface_name*] [**packet-length** *bytes*] [**circular-buffer**]

capture *capture_name* ***type asp-drop*** [*drop-code*] [**buffer** *buf_size*] [**circular-buffer**] [**packet-length** *bytes*]

capture *capture_name* ***type isakmp*** [**access-list** *access_list_name*] [**buffer** *buf_size*] [**circular-buffer**] [**interface** *interface_name*] [**packet-length** *bytes*]

capture *capture_name* ***type raw-data*** [**access-list** *access_list_name*] [**buffer** *buf_size*] [**circular-buffer**] [**ethernet-type** *type*] [**interface** *interface_name*] [**packet-length** *bytes*]

capture *capture_name* ***type webvpn*** **user** *webvpn-user* [**url** *url*]

no capture *capture_name*

シンタックスの説明

access-list *access_list_name*	（オプション）IP フィールドまたはより高位のフィールドに基づいて、特定のアクセスリスト ID のパケットを選択します。
buffer *buf_size*	（オプション）パケットの保存に使用するバッファのサイズをバイト単位で定義します。
capture_name	パケット キャプチャの名前を指定します。
circular-buffer	（オプション）バッファがいっぱいになったときに、先頭部分からバッファを上書きしていきます。
ethernet-type *type*	（オプション）キャプチャするイーサネット タイプを選択します。
interface *interface_name*	（オプション）パケット キャプチャに使用するインターフェイスを指定します。*interface_name* は、**nameif** コマンドによってインターフェイスに割り当てられた名前です。
packet-length *bytes*	（オプション）キャプチャ バッファに保存する各パケットの最大サイズ（バイト数）を設定します。
type asp-drop *drop-code*	（オプション）何らかの原因でドロップされたパケットをキャプチャします。*drop-code* 引数を使用して、特定の理由を指定できます。*drop-code* 引数の有効値は、次の「使用上のガイドライン」に一覧表示されています。
type isakamp	（オプション）暗号化および暗号解除された ISAKMP ペイロードをキャプチャします。
type raw-data	（オプション）着信パケットと発信パケットを 1 つまたは複数のインターフェイス上でキャプチャします。これがデフォルト値です。
type webvpn	（オプション）特定の WebVPN 接続の WebVPN データをキャプチャします。
url ***url***	（オプション）WebVPN 接続キャプチャの URL を指定します。
user ***webvpn-user***	（オプション）WebVPN キャプチャのユーザ名を指定します。

デフォルト

デフォルトは次のとおりです。

- キャプチャ タイプは raw data です。
- **buffer** *size* は 512 KB です。
- すべてのイーサネット タイプが選択されます。
- すべての IP パケットが一致します。
- **packet-length** は 68 バイトです。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権モード	•	•	•	•	•

コマンド履歴

リリース	変更
6.2	セキュリティ アプライアンスでこのコマンドがサポートされるようになりました。
7.0	このコマンドは複数の新しいキーワード、特に ***type asp-drop***、***type isakmp***、***type raw-data***、および ***type webvpn*** キーワードを含めるように修正されました。

使用上のガイドライン

パケットのキャプチャは、接続上の問題のトラブルシューティングや疑わしいアクティビティのモニタリングを行う場合に役立ちます。セキュリティ アプライアンスは、管理トラフィックや検査エンジンを含む、通過するトラフィックのパケット情報を追跡できます。装置を通過するすべてのトラフィックのパケット情報がキャプチャされます。

ISAKMP では、ISAKMP サブシステムは上位レイヤ プロトコルにアクセスできません。キャプチャは、PCAP パーサーを満たすために物理層、IP 層、および UDP 層が組み合された擬似キャプチャです。ピア アドレスは SA 交換から取得され、IP 層に保存されます。

含めるイーサネット タイプをキャプチャから選択する場合、802.1Q タイプまたは VLAN タイプでは例外が発生します。802.1Q タグは自動的にスキップされ、条件に一致しているかどうかの判定には内部イーサネット タイプが使用されます。デフォルトでは、すべてのイーサネット タイプが選択されます。

バッファがいっぱいになると、パケットのキャプチャが停止します。

パケット キャプチャをイネーブルにするには、オプションの引数 *interface* を使用してキャプチャをインターフェイスに関連付けます。複数の **capture** コマンド文を使用すると、キャプチャが複数のインターフェイスに関連付けられます。

バッファの内容を TFTP サーバに ASCII 形式でコピーする場合は、パケットの詳細や 16 進ダンプは表示されず、ヘッダーだけが表示されます。詳細や 16 進ダンプを表示するには、バッファを PCAP 形式で伝送し、TCPDUMP または Ethereal を使用して読み取る必要があります。

ethernet-type オプション キーワードと **access-list** オプション キーワードを使用すると、バッファに保存するパケットを選択できます。イーサネット フィルタとアクセスリスト フィルタの両方を通過したパケットだけがキャプチャ バッファに保存されます。

circular-buffer キーワードを使用すると、キャプチャ バッファがいっぱいになったときに、キャプチャ バッファを先頭部分から上書きできます。

キャプチャが消去されないようにする場合は、**no capture** に **access-list** オプション キーワードまたは **interface** オプション キーワードのいずれかを付加して入力します。オプション キーワードを付加せずに **no capture** を入力すると、キャプチャが削除されます。**access-list** オプション キーワードを指定した場合は、キャプチャからアクセスリストが削除され、キャプチャは残されます。**interface** オプション キーワードを指定した場合は、指定したインターフェイスからキャプチャが分離され、キャプチャは残されます。

（注）　**capture** コマンドはコンフィギュレーションには保存されず、フェールオーバー中にスタンバイ モジュールにコピーされることもありません。

キャプチャ情報をリモートの TFTP サーバにコピーするには、
copy capture: *capture_name* **tftp://server/***path* **[pcap]** コマンドを使用します。

パケット キャプチャ情報を Web ブラウザで表示するには、
https://*securityappliance-ip-address***/capture/***capture_name***[/pcap]** コマンドを使用します。

pcap オプション キーワードを指定すると、libpcap 形式のファイルが Web ブラウザにダウンロードされるので、Web ブラウザを使用してファイルを保存できます。libcap ファイルは、TCPDUMP または Ethereal で表示できます。

WebVPN キャプチャをイネーブルにすると、セキュリティ アプライアンスは一致するファイルのペア（*capture name*_ORIGINAL.000 と *capture name*_MANGLED.000）を作成します。セキュリティ アプライアンスは後続のキャプチャごとに一致するファイルのペアをさらに生成し、ファイル拡張子を増分します。*url* は、データ キャプチャに一致する URL プレフィックスです。サーバへの HTTP トラフィックをキャプチャするには、URL http://*server*/*path* を使用します。サーバへの HTTPS トラフィックをキャプチャするには、https://*server*/*path* を使用します。

（注）　WebVPN キャプチャをイネーブルにすると、セキュリティ アプライアンスのパフォーマンスに影響します。トラブルシューティングに必要なキャプチャ ファイルを生成した後は、キャプチャをディセーブルにしてください。

type asp-drop の drop-code

次の表に、***type asp-drop*** キーワードの後に指定できるオプションの *drop-code* 引数の有効値を示します。

drop-code	説明
acl-drop	アクセス規則によってフローが拒否されます。
all	すべてのパケット ドロップ理由。
bad-crypto	不良暗号がパケットで戻ります。
bad-ipsec-natt	不良 IPSEC NATT パケット。
bad-ipsec-prot	AH または ESP ではない IPSEC。
bad-ipsec-udp	不良 IPSEC UDP パケット。
bad-tcp-cksum	不良 TCP チェックサム。
bad-tcp-flags	不良 TCP フラグ。

drop-code	説明
buffer	キャプチャ バッファのサイズを設定します。デフォルトは 512 KB です。
circular-buffer	バッファがいっぱいになったときに先頭部分から上書きします。デフォルトは non-circular です。
conn-limit	接続制限値に到達しました。
ctm-error	CTM がエラーを返しました。
dns-guard-id-not-matched	DNS Guard id が一致しません。
dns-guard-out-of-app-id	app id 以外の DNS Guard。
dst-l2_lookup-fail	Dst MAC L2 検索が失敗しました。
flow-expired	期限切れのフロー。
fo-standby	スタンバイ装置によってドロップされました。
host-move-pkt	FP ホスト移動パケット。
ifc-classify	仮想ファイアウォール分類が失敗しました。
inspect-dns-id-not-matched	DNS Inspect id が一致しません。
inspect-dns-invalid-domain-label	DNS Inspect 無効ドメイン ラベル。
inspect-dns-invalid-pak	DNS Inspect 無効パケット。
inspect-dns-out-of-app-id	app id 以外の DNS Inspect。
inspect-dns-pak-too-long	DNS Inspect パケットが長すぎます。
inspect-icmp-error-different-embedded-conn	ICMP Error Inspect の組み込み接続が異なります。
inspect-icmp-error-no-existing-conn	ICMP Error Inspect に既存の接続がありません。
inspect-icmp-out-of-app-id	app id 以外の ICMP Inspect。
inspect-icmp-seq-num-not-matched	ICMP Inspect シーケンス番号が一致しません。
inspect-icmpv6-error-invalid-pak	ICMPv6 Error Inspect 無効パケット。
inspect-icmpv6-error-no-existing-conn	ICMPv6 Error Inspect に既存の接続がありません。
intercept-unexpected	予期しないパケットを代行受信します。
interface-down	インターフェイスがダウンしています。
invalid-app-length	無効な app 長。
invalid-encap	無効なカプセル化。
invalid-ethertype	無効な ethertype。
invalid-ip-addr	無効な IP アドレス。
invalid-ip-header	無効な IP ヘッダー。
invalid-ip-length	無効な IP 長。
invalid-ip-option	設定された IP オプションはドロップされます。
invalid-tcp-hdr-length	無効な tcp 長。
invalid-tcp-pak	無効な TCP パケット。
invalid-udp-length	無効な udp 長。
ip-fragment	IP フラグメント（サポート対象外）。
ips-fail-close	IPS カードがダウンしています。
ips-request	要求された IPS モジュールはドロップされます。
ipsec-clearpkt-notun	トンネルなしの IPSEC Clear Pkt。
ipsec-ipv6	IPV6 経由の IPSEC。
ipsec-need-sa	IPSEC SA がまだネゴシエートされていません。

drop-code	説明
ipsec-spoof	IPSEC Spoof が検出されました。
ipsec-tun-down	IPSEC トンネルがダウンしています。
ipsecudp-keepalive	IPSEC/UDP キープアライブ メッセージ。
ipv6_fp-security-failed	IPv6 高速パス セキュリティ チェックが失敗しました。
ipv6_sp-security-failed	IPv6 低速パス セキュリティ チェックが失敗しました。
l2_acl	FP L2 規則がドロップされます。
l2_same-lan-port	L2 Src/Dst が同じ LAN ポートです。
large-buf-alloc-fail	FP fp 大容量バッファ割り当てが失敗しました。
loopback-buffer-full	ループバック バッファがいっぱいです。
lu-invalid-pkt	無効な LU パケット。
natt-keepalive	NAT-T キープアライブ メッセージ。
no-adjacency	有効な隣接情報がありません。
no-mcast-entry	FP に mcast エントリがありません。
no-mcast-intrf	FP に mcast 出力インターフェイスがありません。
no-punt-cb	登録されたパント cb がありません。
no-route	ホストへのルートがありません。
non-ip-pkt-in-routed-mode	非 IP パケットがルーテッド モードで受信されました。
np-sp-invalid-spi	無効な SPI。
packet-length	各パケットから保存する最大長を設定します。デフォルトは 68 バイトです。
punt-rate-limit	パントのレート制限を越えました。
queue-removed	キューに入っているパケットがドロップされました。
rate-exceeded	QoS レートを超えました。
rpf-violated	逆パス確認が失敗しました。
security-failed	早期セキュリティ チェックが失敗しました。
send-ctm-error	CTM への送信がエラーを返しました。
sp-security-failed	低速パス セキュリティ チェックが失敗しました。
tcp-3whs-failed	TCP が 3 ウェイ ハンドシェイクに失敗しました。
tcp-ack-syn-diff	SYNACK 内の TCP ACK が無効です。
tcp-acked	TCP DUP が確認されました。
tcp-bad-option-len	TCP 内のオプション長が不良です。
tcp-bad-option-list	TCP オプション リストが無効です。
tcp-bad-sack-allow	TCP SACK ALLOW オプションが不良です。
tcp-bad-winscale	TCP ウィンドウ スケール値が不良です。
tcp-buffer-full	TCP パケット バッファがいっぱいです。
tcp-conn-limit	TCP 接続制限値に到達しました。
tcp-data-past-fin	FIN 後に TCP データが送信されました。
tcp-discarded-ooo	順序が異なる TCP パケット。
tcp-dual-open	TCP デュアル オープンが拒否されました。
tcp-fo-drop	TCP の複製されたフロー pak がドロップされました。

drop-code	説明
tcp-invalid-ack	TCP の無効な ACK。
tcp-mss-exceeded	TCP MSS が大きすぎました。
tcp-mss-no-syn	TCP MSS オプションが非 SYN 上にあります。
tcp-not-syn	最初の TCP パケットが SYN ではありません。
tcp-paws-fail	TCP パケットが PAWS テストに失敗しました。
tcp-reserved-set	TCP の予約済みフラグが設定されました。
tcp-rst-syn-in-win	TCP RST/SYN がウィンドウ内にあります。
tcp-rstfin-ooo	順序が異なる TCP RST/FIN。
tcp-seq-past-win	TCP パケット SEQ の過去のウィンドウ。
tcp-seq-syn-diff	TCP SEQ が SYN/SYNACK 内にあります。
tcp-syn-data	TCP SYN にデータがあります。
tcp-syn-ooo	TCP SYN が確立された接続上にあります。
tcp-synack-data	TCP SYNACK にデータがあります。
tcp-synack-ooo	TCP SYNACK が確立された接続上にあります。
tcp-tsopt-notallowed	TCP タイムスタンプが許可されませんでした。
tcp-winscale-no-syn	TCP ウィンドウ スケールが非 SYN 上にあります。
tcp_xmit_partial	TCP 再送信が不完全です。
tfw-no-mgmt-ip-config	TFW に管理 IP アドレスが設定されていません。
unable-to-add-flow	フロー ハッシュがいっぱいです。
unable-to-create-flow	フロー キャッシュ メモリ不足です。
unimplemented	低速パスが実装されていません。
unsupport-ipv6-hdr	サポートされていない IPV6。
unsupported-ip-version	サポートされていない IP バージョン。

例

パケット キャプチャをイネーブルにするには、次のように入力します。

```
hostname(config)# capture captest interface inside
hostname(config)# capture captest interface outside
```

「mycapture」という名前のキャプチャの内容を Web ブラウザで表示するには、次のアドレスを入力します。

```
https://171.69.38.95/capture/mycapture/pcap
```

Internet Explorer や Netscape Navigator などの Web ブラウザで使用される libcap ファイルをローカル マシンにダウンロードするには、次のアドレスを入力します。

```
https://171.69.38.95/capture/http/pcap
```

次の例では、外部ホスト 171.71.69.234 からキャプチャしたトラフィックが内部 HTTP サーバに伝送されます。

```
hostname(config)# access-list http permit tcp host 10.120.56.15 eq http host
171.71.69.234
hostname(config)# access-list http permit tcp host 171.71.69.234 host 10.120.56.15 eq
http
hostname(config)# capture http access-list http packet-length 74 interface inside
```

次の例では、ARP パケットをキャプチャする方法を示します。

```
hostname(config)# capture arp ethernet-type arp interface outside
```

次の例では、*hr* に指定された WebVPN キャプチャが作成されます。このキャプチャは、Web サイト wwwin.abcd.com/hr/people にアクセスする user2 の HTTP トラフィックをキャプチャするように設定されています。

```
hostname# capture hr type webvpn user user2 url http://wwwin.abcd.com/hr/people
WebVPN capture started.
   capture name   hr
   user name      user2
   url            /http/0/wwwin.abcd.com/hr/people
hostname#
```

関連コマンド

コマンド	説明
clear capture	キャプチャ バッファをクリアします。
copy capture	キャプチャ ファイルをサーバにコピーします。
show capture	オプションが何も指定されていない場合は、キャプチャのコンフィギュレーションを表示します。

cd

現在の作業ディレクトリから指定したディレクトリに移動するには、***cd*** コマンドを特権 EXEC モードで使用します。

cd [**disk0: | disk1: | flash:**] [*path*]

シンタックスの説明

disk0:	後ろにコロンを付けて内部フラッシュ メモリを指定します。
disk1:	取り外し可能な外部フラッシュ メモリ カードを指定し、続けてコロン（:）を入力します。
flash:	後ろにコロンを付けて内部フラッシュ メモリを指定します。ASA 5500 シリーズでは、***flash*** キーワードは ***disk0*** のエイリアスです。
path	（オプション）移動先ディレクトリの絶対パスです。

デフォルト

ディレクトリを指定しない場合、ルート ディレクトリに移動します。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、「config」ディレクトリに移動する方法を示します。

```
hostname# cd flash:/config/
```

関連コマンド

コマンド	説明
pwd	現在の作業ディレクトリを表示します。

certificate

指定した証明書を追加するには、**certificate** コマンドを暗号 CA 証明書チェーン モードで使用します。このコマンドを使用する場合、セキュリティ アプライアンスは、コマンドに含まれているデータを 16 進形式の証明書として解釈します。**quit** 文字列は証明書の終わりを示します。

証明書を削除するには、このコマンドの **no** 形式を使用します。

certificate [***ca*** | ***ra-encrypt*** | ***ra-sign*** | ***ra-general***] *certificate-serial-number*

no certificate *certificate-serial-number*

シンタックスの説明

certificate-serial-number	quit で終わる 16 進形式の証明書のシリアル番号を指定します。
ca	証明書が certificate authority（CA; 認証局）発行の証明書であることを示します。
ra-encrypt	証明書が SCEP で使用される registration authority（RA; 登録局）の鍵暗号化証明書であることを示します。
ra-general	証明書が SCEP メッセージのデジタル署名および鍵暗号化に使用される登録局（RA）の証明書であることを示します。
ra-sign	証明書が SCEP メッセージで使用される登録局（RA）のデジタル署名証明書であることを示します。

デフォルト

このコマンドにデフォルト値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
証明書チェーン コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

認証局（CA）は、ネットワークにおいてセキュリティ クレデンシャルおよびメッセージ暗号化用の公開キーを発行、管理する組織です。公開キー インフラストラクチャの一部として、CA では登録局（RA）とともに、デジタル証明書の要求者から提供された情報を確認するためにチェックを行います。RA で要求者の情報が確認されると、CA は証明書を発行します。

例

次の例では、central という名前のトラストポイントの CA トラストポイント モードに入り、次に central の 暗号 CA 証明書チェーン モードに入り、シリアル番号 29573D5FF010FE25B45 の CA を追加します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crypto ca certificate chain central
hostname(ca-cert-chain)# certificate ca 29573D5FF010FE25B45
  30820345 308202EF A0030201 02021029 572A3FF2 96EF854F D0D6732F E25B4530
  0D06092A 864886F7 0D010105 05003081 8F311630 1406092A 864886F7 0D010901
  16076140 622E636F 6D310B30 09060355 04061302 55533116 30140603 55040813
  0D6D6173 73616368 75736574 74733111 300F0603 55040713 08667261 6E6B6C69
  6E310E30 0C060355 040A1305 63697363 6F310F30 0D060355 040B1306 726F6F74
  6F75311C 301A0603 55040313 136D732D 726F6F74 2D736861 2D30362D 32303031
  301E170D 30313036 32363134 31313430 5A170D32 32303630 34313430 3133305A
  30818F31 16301406 092A8648 86F70D01 09011607 6140622E 636F6D31 0B300906
  03550406 13025553 31163014 06035504 08130D6D 61737361 63687573 65747473
  3111300F 06035504 07130866 72616E6B 6C696E31 0E300C06 0355040A 13056369
  73636F31 0F300D06 0355040B 1306726F 6F746F75 311C301A 06035504 0313136D
  732D726F 6F742D73 68612D30 362D3230 3031305C 300D0609 2A864886 F70D0101
  01050003 4B003048 024100AA 3EB9859B 8670A6FB 5E7D2223 5C11BCFE 48E6D3A8
  181643ED CF7E75EE E77D83DF 26E51876 97D8281E 9F58E4B0 353FDA41 29FC791B
  1E14219C 847D19F4 A51B7B02 03010001 A3820123 3082011F 300B0603 551D0F04
  04030201 C6300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604
  14E0D412 3ACC96C2 FBF651F3 3F66C0CE A62AB63B 323081CD 0603551D 1F0481C5
  3081C230 3EA03CA0 3A86386C 6461703A 2F2F7732 6B616476 616E6365 64737276
  2F436572 74456E72 6F6C6C2F 6D732D72 6F6F742D 7368612D 30362D32 3030312E
  63726C30 3EA03CA0 3A863868 7474703A 2F2F7732 6B616476 616E6365 64737276
  2F436572 74456E72 6F6C6C2F 6D732D72 6F6F742D 7368612D 30362D32 3030312E
  63726C30 40A03EA0 3C863A66 696C653A 2F2F5C5C 77326B61 6476616E 63656473
  72765C43 65727445 6E726F6C 6C5C6D73 2D726F6F 742D7368 612D3036 2D323030
  312E6372 6C301006 092B0601 04018237 15010403 02010130 0D06092A 864886F7
  0D010105 05000341 0056221E 03F377B9 E6900BF7 BCB3568E ADBA146F 3B8A71F3
  DF9EB96C BB1873B2 B6268B7C 0229D8D0 FFB40433 C8B3CB41 0E4D212B 2AEECD77
  BEA3C1FE 5EE2AB6D 91
  quit
```

関連コマンド

コマンド	説明
clear configure crypto map	すべての暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。
crypto ca certificate chain	証明書暗号 CA 証明書チェーン モードに入ります。
crypto ca trustpoint	CA トラストポイント モードに入ります。
show running-config crypto map	すべての暗号マップのすべてのコンフィギュレーションを表示します。

chain

証明書チェーンの送信をイネーブルにするには、**chain** コマンドをトンネルグループ ipsec アトリビュート コンフィギュレーション モードで使用します。この操作には、ルート証明書および伝送のすべての下位 CA 証明書が含まれます。このコマンド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。

chain

no chain

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトでは、このコマンドの設定はディセーブルになっています。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネルグループ ipsec アトリビュート コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

すべてのトンネルグループ タイプにこのアトリビュートを適用できます。

例

次の例では、config-ipsec コンフィギュレーション モードに入り、ルート証明書およびすべての下位 CA 証明書を含む IP アドレス 209.165.200.225 の IPSec LAN-to-LAN トンネルグループのチェーンの送信をイネーブルにします。

```
hostname(config)# tunnel-group 209.165.200.225 type IPSec_L2L
hostname(config)# tunnel-group 209.165.200.225 ipsec-attributes
hostname(config-ipsec)# chain
hostname(config-ipsec)#
```

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消去します。
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** コマンドで作成された証明書マップ エントリをトンネルグループに関連付けます。

changeto

セキュリティ コンテキストとシステムの間で切り替えを行うには、**changeto** コマンドを特権 EXEC モードで使用します。

changeto {**system** | **context** *name*}

シンタックスの説明

***context** name*	指定した名前を持つコンテキストに変更します。
system	システム実行スペースに変更します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	•	•

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

システム実行スペースまたは管理コンテキストにログインする場合は、各コンテキスト内でコンテキスト、実行コンフィギュレーション、モニタリング タスクを切り替えることができます。コンフィギュレーション モードで編集、あるいは **copy** または **write** コマンドで使用される「実行」コンフィギュレーションは、どの実行スペースにいるかによって異なります。システム実行スペースにいる場合、実行コンフィギュレーションはシステム コンフィギュレーションだけで構成されます。コンテキスト実行スペースにいる場合、実行コンフィギュレーションはそのコンテキストだけで構成されます。たとえば、**show running-config** コマンドを入力することで、実行コンフィギュレーションをすべて（システムとすべてのコンテキスト）表示することはできません。現在のコンフィギュレーションだけが表示されます。

例

次の例では、特権 EXEC モードでコンテキストとシステム間の切り替えを行います。

```
hostname/admin# changeto system
hostname# changeto context customerA
hostname/customerA#
```

次の例では、インターフェイス コンフィギュレーション モードでシステムと管理コンテキスト間の切り替えを行います。実行スペース間で切り替えを行い、コンフィギュレーション サブモードにいる場合、モードは新しい実行スペースでグローバル コンフィギュレーション モードに変わります。

```
hostname(config-if)# changeto context admin
hostname/admin(config)#
```

関連コマンド

コマンド	説明
admin-context	コンテキストを管理コンテキストに設定します。
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードに入ります。
show context	コンテキストのリスト（システム実行スペース）または現在のコンテキストに関する情報を表示します。

checkheaps

チェックヒープ確認の間隔を設定するには、**checkheaps** コマンドをグローバル コンフィギュレーション モードで使用します。値をデフォルトに設定するには、このコマンドの **no** 形式を使用します。チェックヒープは、ピープ メモリ バッファ（ダイナミック メモリはシステム ヒープ メモリ領域から割り当てられる）の健全性およびコード領域の完全性を確認する定期的なプロセスです。

checkheaps {check-interval | validate-checksum} *seconds*

no checkheaps {check-interval | validate-checksum} [*seconds*]

シンタックスの説明

check-interval	バッファ確認の間隔を設定します。バッファ確認のプロセスはヒープ（割り当てられ、解放されたメモリ バッファ）の健全性を確認します。プロセスをそれぞれ呼び出している間､セキュリティ アプライアンスは各メモリ バッファを確認し、ヒープ全体をチェックします。不一致がある場合、セキュリティ アプライアンスは「allocated buffer error」または「free buffer error」を発行します。エラーがある場合、セキュリティ アプライアンスは可能であればトレースバック情報をダンプし、リロードします。
validate-checksum	コード スペース チェックサム確認の間隔を設定します。セキュリティ アプライアンスは、最初の起動時にコード全体のハッシュを計算します。その後、定期チェックの間に、セキュリティ アプライアンスは新しいハッシュを生成し、最初のハッシュと比較します。ミスマッチがある場合、セキュリティ アプライアンスは「text checksum checkheaps error」を発行します。エラーがある場合、セキュリティ アプライアンスは可能であればトレースバック情報をダンプし、リロードします。
seconds	1 ～ 2,147,483 の間隔を秒単位で指定します。

デフォルト

デフォルトの間隔はそれぞれ 60 秒です。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、バッファ割り当ての間隔を 200 秒に設定し、コード スペース チェックサムの間隔を 500 秒に設定します。

```
hostname(config)# checkheaps check-interval 200
hostname(config)# checkheaps validate-checksum 500
```

関連コマンド

コマンド	説明
show checkheaps	チェックヒープ統計情報を表示します。

check-retransmission

TCP 再送信スタイルの攻撃を防止するには、**check-retransmission** コマンドを tcp マップ コンフィギュレーション モードで使用します。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。

check-retransmission

no check-retransmission

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトはディセーブルです。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

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ともに使用します。**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 検査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 検査を有効にします。

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 モードに入ります。矛盾する再送信のエンド システムの解釈によって発生する TCP 再送信スタイルの攻撃を防止するには、**check-retransmission** コマンドを tcp マップ コンフィギュレーション モードで使用します。

セキュリティ アプライアンスは、再送信内のデータが元のデータと同じであるかどうかを確認しようとします。データが一致しない場合、接続はセキュリティ アプライアンスによってドロップされます。この機能がイネーブルの場合、TCP 接続上のパケットは、順番に許可されます。詳細については、**queue-limit** コマンドを参照してください。

例

次の例では、すべての TCP フロー上で、TCP check-retransmission 機能をイネーブルにします。

```
hostname(config)# access-list TCP extended permit tcp any any
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# check-retransmission
hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(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。
help	**policy-map**、**class**、および **description** コマンドのシンタックス ヘルプを表示します。
policy-map	ポリシー（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
set connection	接続値を設定します。
tcp-map	TCP マップを作成し、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。

checksum-verification

TCP チェックサムの確認をイネーブルまたはディセーブルにするには、**checksum-verification** コマンドを tcp マップ コンフィギュレーション モードで使用します。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。

checksum-verification

no checksum-verification

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　チェックサムの確認は、デフォルトではディセーブルになっています。

コマンドのモード　次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

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ともに使用します。**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 検査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 検査を有効にします。

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 モードに入ります。**checksum-verification** コマンドを tcp マップ コンフィギュレーション モードで使用して、TCP チェックサムの確認をイネーブルにします。チェックが失敗した場合、パケットはドロップされます。

例

次の例では、10.0.0.0 ～ 20.0.0.0 の TCP 接続上で TPC チェックサムの確認をイネーブルにします。

```
hostname(config)# access-list TCP1 extended permit tcp 10.0.0.0 255.0.0.0 20.0.0.0
255.0.0.0
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# checksum-verification

hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP1

hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap

hostname(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。
help	**policy-map**、**class**、および **description** コマンドのシンタックス ヘルプを表示します。
policy-map	ポリシー（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
set connection	接続値を設定します。
tcp-map	TCP マップを作成し、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。

class (policy-map)

トラフィック分類のポリシーにクラスマップを割り当てるには、**class** コマンドをポリシーマップ モードで使用します。ポリシーマップに対するクラスマップ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。

class *classmap-name*

no class *classmap-name*

シンタックスの説明

classmap-name	クラスマップの名前。名前には、最大 40 文字を使用できます。

デフォルト

デフォルトでは、「class class-default」が常にポリシーマップの最後にあります。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ポリシーマップ	•	•	•	•	—

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

class-default を含む、最大 63 のクラス コマンドをポリシーマップに設定できます。

「class-default」という名前は、デフォルト クラスに予約されている名前であり、常に存在します。つまり、この名前をコンフィギュレーションに含めることはできますが、CLI を使用して再設定や削除を行うことはできません。詳細については、**class-map** コマンドの説明を参照してください。

class コマンドを使用してクラス モードに入り、次のコマンドを入力できます。

set connection

inspect

ips

priority

police

詳細については、個々のコマンドの説明を参照してください。

例

次に、ポリシーマップ モードのクラス コマンドの例を示します。プロンプトの変化に注意してください。

```
hostname(config)# class-map localclass1
hostname(config-cmap)# match any
hostname(config-cmap)# exit
hostname(config)# policy-map localpolicy1
hostname(config-pmap)# class localclass1
hostname(config-pmap-c)# priority
hostname(config-pmap-c)# exit
```

次に、最大 256 の HTTP サーバに接続を制限する接続ポリシー用の **policy-map** コマンドとその **class** コマンドの例を示します。

```
hostname(config)# access-list myhttp permit tcp any host 10.1.1.1
hostname(config)# class-map myhttp

hostname(config-cmap)# match access-list myhttp
hostname(config-cmap)# exit

hostname(config)# policy-map global-policy
hostname(config-pmap)# description This policy map defines a policy concerning
connection to http server.
hostname(config-pmap)# class myhttp
hostname(config-pmap-c)# set connection conn-max 256
```

次に、**service-policy** コマンドで定義された外部インターフェイス用の **policy-map** コマンドとその **class** コマンドの例を示します。**class-map** コマンドは、宛先 IP アドレスが 192.168.10.10 のトラフィックのクラスを指定します。

```
hostname(config)# class-map outside-voip
hostname(config-cmap)# match dscp af11
hostname(config-cmap)# exit

hostname(config)# policy-map outside-policy
hostname(config-pmap)# description This policy map defines policies for the outside
interface.
hostname(config-pmap)# class outside-voip
hostname(config-pmap-c)# priority
hostname(config-pmap-c)# exit
hostname(config-pmap)# exit
hostname(config)# service-policy outside-policy interface outside
```

関連コマンド

コマンド	説明
clear configure policy-map	service-policy コマンドで使用されているポリシーマップを除く、すべてのポリシーマップ コンフィギュレーションを削除します。
policy-map	ポリシー（それぞれ 1 つまたは複数のアクションがある 1 つまたは複数のトラフィック クラスのアソシエーション）を設定します。
show running-config policy-map	現在のすべてのポリシーマップ コンフィギュレーションを表示します。

class-map

モジュラ ポリシー フレームワークを使用してセキュリティ機能を設定する場合にインターフェイスのトラフィックを分類するには、**class-map** コマンドをグローバル コンフィギュレーション モードで使用します。クラス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。

class-map *class_map_name*

no class-map *class_map_name*

シンタックスの説明

class_map_name	クラスマップ名のテキスト。最大 40 文字まで指定できます。クラスマップの名前のスペースは、セキュリティ コンテキストに対してローカルです。このため、複数のセキュリティ コンテキストで同じ名前を使用できる場合があります。セキュリティ コンテキストあたりのクラスマップの最大数は 255 です。

デフォルト

デフォルト クラスの class-default は常に存在し、CLI を使用して設定または削除することはできません。デフォルト クラスは、ポリシーマップで使用する場合、「他のすべてのトラフィック」を意味します。class-default の定義は次のとおりです。

```
class-map class-default
    match any
```

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

class-map コマンドを使用すると、モジュラ ポリシー フレームワークを使用してセキュリティ機能を設定する場合にトラフィック クラスを定義できます。モジュラ ポリシー フレームワークは、セキュリティ アプライアンスの機能を Cisco IOS ソフトウェア QoS CLI と同様の方法で設定する一貫性のある柔軟な方法です。モジュラ ポリシー フレームワークを使用してセキュリティ機能を設定するには、**class-map**、**policy-map**、および **service-policy** グローバル コンフィギュレーション コマンドを使用します。

class-map グローバル コンフィギュレーション コマンドを使用してトラフィック クラスを定義します。次に、**policy-map** グローバル コンフィギュレーション コマンドを使用して、トラフィック クラスを 1 つまたは複数のアクションに関連付けてポリシーマップを作成します。最後に、**service-policy** コマンドを使用して、ポリシーマップを 1 つまたは複数のインターフェイスに関連付けてセキュリティ ポリシーを作成します。

1 つのトラフィック クラスマップには、最大 1 つの **match** コマンドが含まれます（**match tunnel-group** および **match default-inspection-traffic** コマンドを除く）。**match** コマンドでは、トラフィック クラスに含まれるトラフィックを指定します。パケットをクラスマップと照合した場合、照合の結果は match または no match のいずれかとなります。

class-map コマンドを使用して、クラスマップ コンフィギュレーション モードに入ります。クラスマップ コンフィギュレーション モードから、**match** コマンドを使用して、クラスに含めるトラフィックを定義できます。次のコマンドをクラスマップ コンフィギュレーション モードで使用できます。

description	クラスマップの説明を指定します。
match access-list	一致条件として使用するアクセスリストの名前を指定します。パケットがアクセスリスト内のエントリと一致しない場合、照合の結果は no-match となります。パケットがアクセスリスト内のエントリと一致する場合、およびパケットが permit エントリの場合、照合の結果は match となります。または、拒否アクセスリスト エントリと一致する場合、照合の結果は no-match となります。
match port	TCP/UDP 宛先ポートを使用して、トラフィックに一致するように指定します。
match precedence	IP ヘッダーに TOS バイトで示される優先順位値に一致するように指定します。
match dscp	IP ヘッダーの IETF 定義の DSCP 値に一致するように指定します。
match rtp	RTP ポートに一致するように指定します。
match tunnel-group	セキュリティ関連のトンネルグループに一致するように指定します。
match flow ip destination-address	IP 宛先アドレスに一致するように指定します。
match default-inspection-traffic	**inspect** コマンドのデフォルト トラフィックに一致するように指定します。

例

次の例では、クラスマップを使用して、すべての TCP トラフィックのトラフィック クラスをポート 21 に定義する方法を示します。

```
hostname(config)# class-map ftp-port
hostname(config-cmap)# match port tcp eq 21
```

関連コマンド

コマンド	説明
clear configure class-map	すべてのトラフィック マップ定義を削除します。
policy-map	トラフィック クラスを 1 つまたは複数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。
service-policy	ポリシーマップを 1 つまたは複数のインターフェイスと関連付けることによって、セキュリティ ポリシーを作成します。
show running-config class-map	クラスマップ コンフィギュレーションに関する情報を表示します。

clear aaa local user fail-attempts

ユーザのロックアウト ステータスを変更せずに、失敗したユーザ認証試行の数を 0 にリセットするには、**clear aaa local user fail-attempts** コマンドを特権 EXEC モードで使用します。

clear aaa local user authentication fail-attempts {**username** *name* | **all**}

シンタックスの説明

all	すべてのユーザの失敗試行カウンタを 0 にリセットします。
name	失敗試行カウンタが 0 にリセットされる特定のユーザ名を指定します。
username	後続のパラメータが、失敗試行カウンタが 0 にリセットされるユーザ名であることを示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ユーザが数回認証に失敗した場合は、このコマンドを使用します。ただし、たとえば、コンフィギュレーションが最近変更された場合などは、カウンタを 0 にリセットします。

認証試行の失敗が設定された回数を超えると、ユーザはシステムからロックアウトされ、システム管理者がユーザ名をアンロックするか、システムをリブートするまで正常にログインできません。

ユーザが正常に認証されるか、セキュリティ アプライアンスがリブートされると、失敗した試行の回数は 0 にリセットされ、ロックアウト ステータスは No にリセットされます。

ユーザ名のロックまたはアンロックにより、syslog メッセージが生成されます。

特権レベル 15 のシステム管理者は、ロックアウトされません。

例

次の例では、**clear aaa local user authentication fail-attempts** コマンドを使用して、ユーザ名 anyuser の失敗試行カウンタを 0 にリセットする方法を示します。

```
hostname(config)# clear aaa local user authentication fail-attempts username anyuser
hostname(config)#
```

次の例では、**clear aaa local user authentication fail-attempts** コマンドを使用して、すべてのユーザの失敗試行カウンタを 0 にリセットする方法を示します。

```
hostname(config)# clear aaa local user authentication fail-attempts all
hostname(config)#
```

関連コマンド

コマンド	説明
aaa local authentication attempts max-fail	ユーザ認証試行の失敗が許可される回数の制限を設定します。
clear aaa local user lockout	ユーザのロックアウト ステータスを変更せずに、失敗したユーザ認証試行の数を 0 にリセットします。
show aaa local user [locked]	現在ロックされているユーザ名のリストを表示します。

clear aaa local user lockout

指定したユーザのロックアウト ステータスを消去し、失敗試行カウンタを 0 にリセットするには、**clear aaa local user lockout** コマンドを特権 EXEC モードで使用します。

clear aaa local user lockout {**username** *name* | **all**}

シンタックスの説明

all	すべてのユーザの失敗試行カウンタを 0 にリセットします。
name	失敗試行カウンタが 0 にリセットされる特定のユーザ名を指定します。
username	後続のパラメータが、失敗試行カウンタが 0 にリセットされるユーザ名であることを示します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

username オプションを使用して単一のユーザを指定することも、***all*** オプションを使用してすべてのユーザを指定することもできます。

このコマンドは、ロックアウトされているユーザのステータスだけに影響を及ぼします。

管理者は、デバイスからロックアウトされません。

ユーザ名のロックまたはアンロックにより、syslog メッセージが生成されます。

例

次の例では、**clear aaa local user lockout** コマンドを使用してロックアウト状態をクリアし、ユーザ名 anyuser の失敗試行カウンタを 0 にリセットする方法を示します。

```
hostname(config)# clear aaa local user lockout username anyuser
hostname(config)#
```

関連コマンド

コマンド	説明
aaa local authentication attempts max-fail	ユーザ認証試行の失敗が許可される回数の制限を設定します。
clear aaa local user fail-attempts	ユーザのロックアウト ステータスを変更せずに、失敗したユーザ認証試行の数を 0 にリセットします。
show aaa local user [locked]	現在ロックされているユーザ名のリストを表示します。

clear aaa-server statistics

AAA サーバの統計情報をリセットするには、**clear aaa-server statistics** コマンドを特権 EXEC モードで使用します。

clear aaa-server statistics [**LOCAL** | *groupname* [**host** *hostname*] | **protocol** *protocol*]

シンタックスの説明

LOCAL	（オプション）LOCAL ユーザ データベースの統計情報を消去します。
groupname	（オプション）グループ内のサーバの統計情報を消去します。
host *hostname*	（オプション）グループ内の特定のサーバの統計情報を消去します。
protocol *protocol*	（オプション）次の特定のプロトコルのサーバの統計情報を消去します。 • **kerberos** • **ldap** • **nt** • **radius** • **sdi** • **tacacs+**

デフォルト

すべてのグループのすべての AAA サーバ統計情報を削除します。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更
7.0(1)	CLI ガイドラインに沿うように、このコマンドが変更されました。プロトコル値においては、***nt*** が以前の ***nt-domain*** に置き換えられ、***sdi*** が以前の ***rsa-ace*** に置き換えられます。

例

次のコマンドは、グループ内の特定のサーバの AAA 統計情報をリセットする方法を示しています。

```
hostname(config)# clear aaa-server statistics svrgrp1 host 1.2.3.4
```

次のコマンドは、1 つのサーバ グループ全体の AAA 統計情報をリセットする方法を示しています。

```
hostname(config)# clear aaa-server statistics svrgrp1
```

次のコマンドは、すべてのサーバ グループの AAA 統計情報をリセットする方法を示しています。

```
hostname(config)# clear aaa-server statistics
```

次のコマンドは、特定のプロトコル（この場合は TACACS+）の AAA 統計情報をリセットする方法を示しています。

```
hostname(config)# clear aaa-server statistics protocol tacacs+
```

関連コマンド

コマンド	説明
aaa-server protocol	AAA サーバ接続データのグループ化を指定および管理します。
clear configure aaa-server	デフォルト以外のすべての aaa サーバ グループを削除、または指定したグループを消去します。
show aaa-server	AAA サーバの統計情報を表示します。
show running-config aaa-server	現在の AAA サーバのコンフィギュレーション値を表示します。

clear access-group

すべての インターフェイスからアクセス グループを削除するには、**clear access-group** コマンドを使用します。

clear access-group

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　このコマンドにデフォルト設定はありません。

コマンドのモード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン　このコマンドに使用上のガイドラインはありません。

例　次の例では、すべてのアクセス グループを削除する方法を示します。

```
hostname(config)# clear access-group
```

関連コマンド

コマンド	説明
access-group	アクセスリストをインターフェイスにバインドします。
show access-group	コンテキスト グループのメンバーを表示します。

clear access-list

アクセスリスト カウンタをクリアするには、**clear access-list** コマンドをグローバル コンフィギュレーション モードで使用します。

clear access-list [*id*] **counters**

シンタックスの説明

counters	アクセスリスト カウンタをクリアします。
id	（オプション）アクセスリストの名前または番号。

デフォルト

すべてのアクセスリスト カウンタがクリアされます。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

clear access-list コマンドを入力する場合、*id* を指定しなければ、すべてのアクセスリスト カウンタがクリアされます。

例

次の例では、特定のアクセスリスト カウンタをクリアする方法を示します。

```
hostname# clear access-list inbound counters
```

関連コマンド

コマンド	説明
access-list extended	アクセスリストをコンフィギュレーションに追加し、ファイアウォールを通過する IP トラフィック用のポリシーを設定します。
access-list standard	アクセスリストを追加して、OSPF 再配布のルートマップに使用できる、OSPF ルートの宛先 IP アドレスを指定します。
clear configure access-list	実行コンフィギュレーションからアクセスリストを消去します。
show access-list	アクセスリストのエントリを番号別に表示します。
show running-config access-list	セキュリティ アプライアンスで実行されているアクセスリスト コンフィギュレーションを表示します。

clear arp statistics

ARP 統計情報を消去するには、**clear arp statistics** コマンドを特権 EXEC モードで使用します。

clear arp statistics

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

例

次の例では、ARP 統計情報をすべて消去します。

```
hostname# clear arp statistics
```

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	透過 ファイアウォール モードで、ARP パケットを調べて ARP スプーフィングを防止します。
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。

clear asp drop

アクセラレーション セキュリティ パスのドロップ統計情報を消去するには、**clear asp drop** コマンドを特権 EXEC モードで使用します。

clear asp drop [**flow** *type* | **frame** *type*]

シンタックスの説明

flow	（オプション）ドロップされたフロー統計情報を消去します。
frame	（オプション）ドロップされたパケット統計情報を消去します。
type	（オプション）特定のプロセスのドロップされたフローまたはパケットの統計情報を消去します。タイプのリストについては、「使用上のガイドライン」を参照してください。

デフォルト

デフォルトでは、このコマンドはすべてのドロップ統計情報を消去します。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン　プロセス タイプには、次のものがあります。

```
acl-drop
audit-failure
closed-by-inspection
conn-limit-exceeded
fin-timeout
flow-reclaimed
fo-primary-closed
fo-standby
fo_rep_err
host-removed
inspect-fail
ips-fail-close
ips-request
ipsec-spoof-detect
loopback
mcast-entry-removed
mcast-intrf-removed
mgmt-lockdown
nat-failed
nat-rpf-failed
need-ike
no-ipv6-ipsec
non_tcp_syn
out-of-memory
parent-closed
pinhole-timeout
recurse
reinject-punt
reset-by-ips
reset-in
reset-oout
shunned
syn-timeout
tcp-fins
tcp-intecept-no-response
tcp-intercept-kill
tcp-intercept-unexpected
tcpnorm-invalid-syn
tcpnorm-rexmit-bad
tcpnorm-win-variation
timeout
tunnel-pending
tunnel-torn-down
xlate-removed
```

例　次の例では、ドロップ統計情報をすべて消去します。

```
hostname# clear asp drop
```

関連コマンド

コマンド	説明
show asp drop	ドロップされたパケットのアクセラレーション セキュリティ パス カウンタを表示します。

clear blocks

最低水準点や履歴情報などのパケット バッファ カウンタをリセットするには、**clear blocks** コマンドを特権 EXEC モードで使用します。

clear blocks

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

最低水準点カウンタを各プール内で現在使用可能なブロックにリセットします。また、前回のバッファ割り当ての失敗時に保存された履歴情報も消去します。

例

次の例では、ブロックを消去します。

```
hostname# clear blocks
```

関連コマンド

コマンド	説明
blocks	ブロック診断に割り当てられているメモリを増やします。
show blocks	システム バッファの使用状況を表示します。

clear capture

キャプチャ バッファを消去するには、**clear capture** *capture_name* コマンドを使用します。

clear capture *capture_name*

シンタックスの説明

capture_name	パケット キャプチャの名前。

デフォルト

このコマンドにデフォルト設定はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権モード	•	•	•	•	•

コマンド履歴

リリース	変更
2.2(1)	セキュリティ アプライアンスでこのコマンドがサポートされるようになりました。

使用上のガイドライン

誤ってパケット キャプチャを全消去することを防ぐため、**clear capture** の短縮形（**cl cap** や **clear cap** など）はサポートされていません。

例

次の例では、キャプチャ バッファ「trudy」のキャプチャ バッファを消去する方法を示します。

```
hostname(config)# clear capture trudy
```

関連コマンド

コマンド	説明
capture	パケット キャプチャ機能を有効にして、パケットのスニッフィングやネットワーク障害を検出できるようにします。
show capture	オプションが何も指定されていない場合は、キャプチャのコンフィギュレーションを表示します。

clear configure

実行コンフィギュレーションを消去するには、**clear configure** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure {***primary*** | ***secondary*** | ***all*** | *command*}

シンタックスの説明

command	指定したコマンドのコンフィギュレーションを消去します。詳細については、このマニュアルの各 **clear configure** *command* コマンドの個々のエントリを参照してください。
primary	次のコマンドを含む、接続性に関連するコマンドを消去します。 • **tftp-server** • **shun** • **route** • **ip address** • **mtu** • **failover** • **monitor-interface** • **boot**
secondary	（***primary*** キーワードを使用して消去される）接続に関連するコマンド以外のコマンドを消去します。
all	実行コンフィギュレーション全体を消去します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

このコマンドをセキュリティ コンテキストで入力する場合は、コンテキスト コンフィギュレーションだけが消去されます。このコマンドをシステム実行スペースで入力する場合は、すべてのコンテキスト実行コンフィギュレーションに加えてシステム実行コンフィギュレーションも消去されます。システム コンフィギュレーション内のすべてのコンテキスト エントリが消去されるため（**context** コマンドを参照）、コンテキストは実行されず、コンテキスト実行スペースに移動できなくなります。

コンフィギュレーションを消去する前に、（スタートアップ コンフィギュレーションの場所を指定する）**boot config** コマンドへのすべての変更をスタートアップ コンフィギュレーションに保存します。スタートアップ コンフィギュレーションの場所を実行コンフィギュレーション内だけで変更した場合は、再起動時にコンフィギュレーションはデフォルト位置からロードされます。

例

次の例では、実行コンフィギュレーション全体を消去します。

```
hostname(config)# clear configure all
```

関連コマンド

コマンド	説明
configure http	指定した HTTP(S) URL からのコンフィギュレーション ファイルを実行コンフィギュレーションとマージします。
configure memory	スタートアップ コンフィギュレーションを実行コンフィギュレーションとマージします。
configure net	指定した TFTP URL からのコンフィギュレーション ファイルを実行コンフィギュレーションとマージします。
configure factory-default	CLI で入力するコマンドを実行コンフィギュレーションに追加します。
show running-config	実行コンフィギュレーションを表示します。

clear configure aaa

aaa コンフィギュレーションを消去するには、**clear configure aaa** コマンドをグローバル コンフィギュレーション モードで使用します。**clear configure aaa** コマンドは、コンフィギュレーションから AAA コマンド文を削除します。

clear configure aaa

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	CLI 内の一貫性のために、このコマンドが修正されました。

使用上のガイドライン

また、このコマンドは、AAA パラメータが存在する場合リセットしてデフォルト値にします。

元に戻すことはできません。

例

```
hostname(config)# clear configure aaa
```

関連コマンド

コマンド	説明
aaa accounting	ユーザがアクセスしたネットワーク サービスのレコードの保持をイネーブル化、ディセーブル化、または表示します。
aaa authentication	**aaa-server** コマンドで指定されたサーバ上での、LOCAL、TACACS+、または RADIUS のユーザ認証、または ASDM ユーザ認証をイネーブル化または表示します。
aaa authorization	**aaa-server** コマンドで指定された LOCAL または TACACS+ サーバのユーザ認可、あるいは ASDM ユーザ認証のユーザ認可をイネーブルまたはディセーブルにします。
show running-config aaa	AAA コンフィギュレーションを表示します。

clear configure aaa-server

すべての AAA サーバ グループを削除、または指定したグループを消去するには、**clear configure aaa-server** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure aaa-server [*server-tag*]

clear configure aaa-server [*server-tag*] **host** *server-ip*

シンタックスの説明

server-ip	AAA サーバの IP アドレス。
server-tag	（オプション）消去するサーバ グループの識別名。

デフォルト

すべての AAA サーバ グループを削除します。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

特定の AAA サーバ グループ、またはデフォルトで、すべての AAA サーバ グループを指定できます。

サーバ グループ内の特定のサーバを指定するには、***host*** キーワードを使用します。

また、このコマンドは、AAA サーバ パラメータが存在する場合リセットしてデフォルト値にします。

例

```
hostname(config)# aaa-server svrgrp1 protocol sdi
hostname(config)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server)# timeout 9
hostname(config-aaa-server)# retry 7
hostname(config-aaa-server)# sdi-version sdi-5
hostname(config-aaa-server)# exit
```

上記のコンフィギュレーションで、次のコマンドは、グループから特定のサーバを削除する方法を示しています。

```
hostname(config)# clear config aaa-server svrgrp1 host 1.2.3.4
```

次のコマンドは、1 つのサーバ グループを削除する方法を示しています。

```
hostname(config)# clear config aaa-server svrgrp1
```

次のコマンドは、すべてのサーバ グループを削除する方法を示しています。

```
hostname(config)# clear config aaa-server
```

関連コマンド

コマンド	説明
aaa-server host	ホスト固有の AAA サーバ接続データを指定および管理します。
aaa-server protocol	すべてのホストに共通する、グループ固有の AAA サーバ パラメータを設定できます。
show running-config aaa	他の AAA コンフィギュレーション値とともに、ユーザ 1 人あたりに許可する同時プロキシ接続の現在の最大数を表示します。

clear configure access-group

すべての インターフェイスからアクセス グループを削除するには、**clear configure access-group** コマンドを使用します。

clear configure access-group

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトの動作や値はありません。

コマンドのモード　次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	キーワード ***configure*** が追加されました。

例　次の例では、すべてのアクセス グループを削除する方法を示します。

```
hostname(config)# clear configure access-group
```

関連コマンド

コマンド	説明
access-group	アクセスリストをインターフェイスにバインドします。
show running-config access-group	現在のアクセス グループ コンフィギュレーションを表示します。

clear configure access-list

実行コンフィギュレーションからアクセスリストを消去するには、**clear configure access-list** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure access-list [*id*]

シンタックスの説明

id	（オプション）アクセスリストの名前または番号。

デフォルト

実行コンフィギュレーションからすべてのアクセスリストが消去されます。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

clear configure access-list コマンドを実行すると、**crypto map** コマンドまたはインターフェイスからアクセスリストが自動的にアンバインドされます。**crypto map** コマンドからアクセスリストをアンバインドすると、パケットがすべて廃棄される状態になる可能性があります。これは、アクセスリストを参照している **crypto map** コマンドが不完全なものになるためです。この状態を解消するには、別の **access-list** コマンドを定義して **crypto map** コマンドを完全なものにするか、**access-list** コマンドに関係する **crypto map** コマンドを削除します。詳細については、**crypto map client** コマンドの項を参照してください。

例

次の例では、実行コンフィギュレーションからアクセスリストを消去する方法を示します。

```
hostname(config)# clear configure access-list
```

関連コマンド

コマンド	説明
access-list extended	アクセスリストをコンフィギュレーションに追加し、ファイアウォールを通過する IP トラフィック用のポリシーを設定します。
access-list standard	アクセスリストを追加して、OSPF 再配布のルートマップに使用できる、OSPF ルートの宛先 IP アドレスを指定します。
clear access-list	アクセスリスト カウンタをクリアします。
show access-list	アクセスリストのカウンタを表示します。
show running-config access-list	セキュリティ アプライアンスで実行されているアクセスリスト コンフィギュレーションを表示します。

clear configure alias

コンフィギュレーションからすべての **alias** コマンドを削除するには、**clear configure alias** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure alias

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

例

次の例では、コンフィギュレーションからすべての **alias** コマンドを削除する方法を示します。

```
hostname(config)# clear configure alias
```

関連コマンド

コマンド	説明
alias	1 つのアドレスを別のアドレスに変換します。
show running-config alias	コンフィギュレーション内の、デュアル NAT コマンドで使用する重複アドレスを表示します。

clear configure arp-inspection

ARP 検査のコンフィギュレーションを消去するには、**clear configure arp-inspection** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure arp-inspection

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、ARP 検査のコンフィギュレーションを消去します。

```
hostname# clear configure arp-inspection
```

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	透過 ファイアウォール モードで、ARP パケットを調べて ARP スプーフィングを防止します。
firewall transparent	ファイアウォール モードを透過に設定します。
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。

clear configure asdm

実行コンフィギュレーションからすべての **asdm** コマンドを削除するには、**clear configure asdm** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure asdm [*location* | *group* | *image*]

シンタックスの説明

group	（オプション）実行コンフィギュレーションから **asdm group** コマンドだけを消去します。
image	（オプション）実行コンフィギュレーションから **asdm image** コマンドだけを消去します。
location	（オプション）実行コンフィギュレーションから **asdm location** コマンドだけを消去します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更
7.0(1)	このコマンドが、**clear pdm** コマンドから **clear configure asdm** コマンドに変更されました。

使用上のガイドライン

実行コンフィギュレーション内の **asdm** コマンドを表示するには、**show running-config asdm** コマンドを使用します。

コンフィギュレーションから **asdm image** コマンドを消去すると、ASDM アクセスがディセーブルになります。コンフィギュレーションから **asdm location** コマンドおよび **asdm group** コマンドを消去すると、次にアクセスされたときに ASDM によってこれらのコマンドが再生成されますが、アクティブな ASDM セッションが妨げられることがあります。

（注）　マルチ コンテキスト モードで実行されているセキュリティ アプライアンスでは、**clear configure asdm image** コマンドはシステム実行スペースでのみ使用できます。一方、**clear configure asdm group** コマンドおよび **clear configure asdm location** コマンドは、ユーザ コンテキストでのみ使用できます。

例

次の例では、実行コンフィギュレーションから **asdm group** コマンドを消去します。

```
hostname(config)# clear configure asdm group
hostname(config)#
```

関連コマンド

コマンド	説明
asdm group	オブジェクト グループ名をインターフェイスに関連付けるために ASDM によって使用されます。
asdm image	ASDM イメージ ファイルを指定します。
asdm location	IP アドレスをインターフェイス アソシエーションに記録するために ASDM によって使用されます。
show running-config asdm	実行コンフィギュレーション内の **asdm** コマンドを表示します。

clear configure auth-prompt

指定済みの認証プロンプト チャレンジ テキストを削除し、デフォルト値に戻すには（存在する場合）、**clear configure auth-prompt** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure auth-prompt

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	CLI 規格に適合するように、このコマンドが修正されました。

使用上のガイドライン

認証プロンプトを消去した後、ユーザのログイン時に表示されるプロンプトは、使用するプロトコルによって次のように異なります。

- HTTP を使用してログインするユーザの場合、`HTTP Authentication` が表示されます。
- FTP を使用してログインするユーザの場合、`FTP Authentication` が表示されます。
- Telnet を使用してログインするユーザの場合、プロンプトは表示されません。

例

次の例では、認証プロンプトを消去する方法を示します。

```
hostname(config)# clear configure auth-prompt
```

関連コマンド

auth-prompt	ユーザ認可プロンプトを設定します。
show running-config auth-prompt	ユーザ認可プロンプトを表示します。

clear configure banner

すべてのバナーを削除するには、**clear configure banner** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure banner

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更
2.2(1)	このコマンドが導入されました。

例

次の例では、バナーを消去する方法を示します。

```
hostname(config)# clear configure banner
```

関連コマンド

コマンド	説明
banner	セッション バナー、ログイン バナー、および「今日のお知らせ」バナーを設定します。
show running-config banner	すべてのバナーを表示します。

clear configure ca certificate map

証明書マップ エントリをすべて削除、または指定した証明書マップ エントリを削除するには、**clear configure ca configurate map** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure ca certificate map [*sequence-number*]

シンタックスの説明

sequence-number	（オプション）削除する証明書マップ規則の番号を指定します。範囲は 1 ～ 65535 です。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、すべての証明書マップ エントリを削除します。

```
hostname(config)# clear configure ca certificate map
hostname(config)#
```

関連コマンド+

コマンド	説明
crypto ca certificate map	CA 証明書マップ モードに入ります。

clear configure class-map

すべてのクラスマップを削除するには、**clear configure class-map** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure class-map

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	キーワード ***configure*** が追加されました。

使用上のガイドライン

特定のクラスマップ名のクラスマップを消去するには、**class-map** コマンドの **no** 形式を使用します。

例

次の例では、設定済みのクラスマップをすべて消去する方法を示します。

```
hostname(config)# clear configure class-map
```

関連コマンド

コマンド	説明
class-map	トラフィック クラスをインターフェイスに適用します。
show running-config class-map	クラスマップ コンフィギュレーションに関する情報を表示します。

clear configure clock

クロック コンフィギュレーションを消去するには、**clear configure clock** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure clock

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが、**clear clock** から変更されました。

使用上のガイドライン

このコマンドは、すべての **clock** コンフィギュレーション コマンドを消去します。**clock set** コマンドはコンフィギュレーション コマンドではないため、このコマンドではクロックはリセットされません。クロックをリセットするには、**clock set** コマンドに新しい時間を設定する必要があります。

例

次の例では、すべてのクロック コマンドを消去します。

```
hostname# clear configure clock
```

関連コマンド

コマンド	説明
clock set	時間を手動で設定します。
clock summer-time	夏時間を表示する日付範囲を設定します。
clock timezone	時間帯を設定します。

clear configure command-alias

デフォルト以外のコマンド エイリアスをすべて削除するには、***clear configure command-alias*** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure command-alias

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドに使用上のガイドラインはありません。

例

次の例では、デフォルト以外のコマンド エイリアスをすべて削除する方法を示します。

```
hostname(config)# clear configure command-alias
```

関連コマンド

コマンド	説明
command-alias	コマンド エイリアスを作成します。
show running-config command-alias	デフォルト以外のコマンド エイリアスをすべて表示します。

clear configure console

コンソール接続の設定をデフォルトにリセットするには、**clear configure console** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure console

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、コンソール接続の設定をデフォルトにリセットする方法を示します。

```
hostname(config)# clear configure console
```

関連コマンド

コマンド	説明
console timeout	セキュリティ アプライアンスへのコンソール接続のアイドル タイムアウトを設定します。
show running-config console timeout	セキュリティ アプライアンスへのコンソール接続のアイドル タイムアウトを表示します。

clear configure context

システム コンフィギュレーションのすべてのコンテキスト コンフィギュレーションを消去するには、**clear configure context** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure context [*noconfirm*]

シンタックスの説明

noconfirm	（オプション）確認を求めるプロンプトを表示せずにすべてのコンテキストを削除します。このオプションは、自動スクリプトに役立ちます。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、管理コンテキストを含むすべてのコンテキストを削除できます。管理コンテキストは **no context** コマンドを使用して削除することはできませんが、**clear configure context** コマンドを使用して削除できます。

例

次の例では、システム コンフィギュレーションからすべてのコンテキストを削除し、削除を確認しません。

```
hostname(config)# clear configure context noconfirm
```

関連コマンド

コマンド	説明
admin-context	管理コンテキストを設定します。
changeto	コンテキスト間またはコンテキストとシステム実行スペースの間で切り替えを行います。
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードに入ります。
mode	コンテキスト モードをシングルまたはマルチに設定します。
show context	コンテキストのリスト（システム実行スペース）または現在のコンテキストに関する情報を表示します。

clear configure crypto

IPSec、暗号マップ、ダイナミック暗号マップ、CA トラストポイント、すべての証明書、証明書マップ コンフィギュレーション、ISAKMP など、暗号コンフィギュレーション全体を削除するには、**clear configure crypto** コマンドをグローバル コンフィギュレーション モードで使用します。特定のコンフィギュレーションを削除するには、シンタックスに示されているように、このコマンドをキーワードとともに使用します。このコマンドは、慎重に使用してください。

clear configure crypto [**ca** | **dynamic-map** | **ipsec** | **iskmp** | **map**]

シンタックスの説明

ca	認証局のポリシーを削除します。
dynamic-map	ダイナミック暗号マップ コンフィギュレーションを削除します。
ipsec	IPSec コンフィギュレーションを削除します。
isakmp	ISAKMP コンフィギュレーションを削除します。
map	暗号マップ コンフィギュレーションを削除します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで発行した次の例では、セキュリティ アプライアンスからすべての暗号コンフィギュレーションを削除します。

```
hostname(config)# clear configure crypto
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	すべてのまたは指定したダイナミック暗号マップをコンフィギュレーションから消去します。
clear configure crypto map	すべてのまたは指定した暗号マップをコンフィギュレーションから消去します。
clear configure isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
show running-config crypto	IPSec、暗号マップ、ダイナミック暗号マップ、ISAKMP など、暗号コンフィギュレーション全体を表示します。

clear configure crypto ca trustpoint

コンフィギュレーションからすべてのトラストポイントを削除するには、**clear configure crypto ca trustpoint** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure crypto ca trustpoint

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで入力した次の例では、コンフィギュレーションからすべてのトラストポイントを削除します。

```
hostname(config)# clear configure crypto ca trustpoint
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	指定したトラストポイントのトラストポイント サブコンフィギュレーション レベルに入ります。

clear configure crypto dynamic-map

コンフィギュレーションからすべてのまたは指定したダイナミック暗号マップを削除するには、**clear configure crypto dynamic-map** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure crypto dynamic-map *dynamic-map-name dynamic-seq-num*

シンタックスの説明

dynamic-map-name	特定のダイナミック暗号マップの名前を指定します。
dynamic-seq-num	ダイナミック暗号マップのシーケンス番号を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで入力した次の例では、コンフィギュレーションからシーケンス番号 3 のダイナミック暗号マップ mymaps を削除します。

```
hostname(config)# clear configure crypto dynamic-map mymaps 3
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべてのまたは指定した暗号マップのコンフィギュレーションを消去します。
	すべてのダイナミック暗号マップのすべてのアクティブなコンフィギュレーションを表示します。
show running-config crypto map	すべての暗号マップのすべてのアクティブなコンフィギュレーションを表示します。

clear configure crypto map

コンフィギュレーションからすべてのまたは指定した暗号マップを削除するには、**clear configure crypto map** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure crypto map *map-name seq-num*

シンタックスの説明

map-name	特定の暗号マップの名前を指定します。
seq-num	暗号マップのシーケンス番号を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで入力した次の例では、コンフィギュレーションからシーケンス番号 3 の暗号マップ mymaps を削除します。

```
hostname(config)# clear configure crypto map mymaps 3
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	すべてのまたは指定したダイナミック暗号マップのコンフィギュレーションを消去します。
crypto map interface	暗号マップをインターフェイスに適用します。
show running-config crypto map	すべての暗号マップのアクティブなコンフィギュレーションを表示します。
	すべてのダイナミック暗号マップのアクティブなコンフィギュレーションを表示します。

clear configure dhcpd

DHCP サーバ コマンド、バインディング、および統計情報をすべて消去するには、**clear configure dhcpd** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure *dhcpd*

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが、**clear dhcpd** から **clear configure dhcpd** に変更されました。

使用上のガイドライン

clear configure dhcpd コマンドは、**dhcpd** コマンド、バインディング、および統計情報をすべて消去します。統計情報カウンタまたはバインディング情報だけを消去するには、**clear dhcpd** コマンドを使用します。

例

次の例では、すべての **dhcpd** コマンドを消去する方法を示します。

```
hostname(config)# clear configure dhcpd
```

関連コマンド

コマンド	説明
clear dhcpd	DHCP サーバのバインディングおよび統計情報カウンタをクリアします。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

clear configure dhcprelay

すべての DHCP リレー コンフィギュレーションを消去するには、**clear configure dhcprelay** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure *dhcprelay*

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが、**clear dhcprelay** から **clear configure dhcprelay** に変更されました。

使用上のガイドライン

clear configure dhcprelay コマンドは、DHCP リレー統計情報およびコンフィギュレーションを消去します。DHCP 統計情報カウンタだけを消去するには、**clear dhcprelay statistics** コマンドを使用します。

例

次の例では、DHCP リレー コンフィギュレーションを消去する方法を示します。

```
hostname(config)# clear configure dhcprelay
```

関連コマンド

コマンド	説明
clear dhcprelay statistics	DHCP リレー エージェント統計情報カウンタをクリアします。
debug dhcprelay	DHCP リレー エージェントに関するデバッグ情報を表示します。
show dhcprelay statistics	DHCP リレー エージェントの統計情報を表示します。
show running-config dhcprelay	現在の DHCP リレー エージェント コンフィギュレーションを表示します。

clear configure dns

すべての DNS コマンドを消去するには、**clear configure dns** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure dns

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトの動作や値はありません。

コマンドのモード　次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例　次の例では、すべての DNS コマンドを消去します。

```
hostname(config)# clear configure dns
```

関連コマンド

コマンド	説明
dns domain-lookup	セキュリティ アプライアンスがネーム ルックアップを実行できるようにします。
dns name-server	DNS サーバのアドレスを設定します。
dns retries	セキュリティ アプライアンスが応答を受け取らなかった場合に、DNS サーバのリストを再試行する回数を指定します。
dns timeout	次の DNS サーバを試すまでに待つ時間を指定します。
show dns-hosts	DNS キャッシュを表示します。

clear configure established

確立されたコマンドをすべて削除するには、**clear configure established** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure established

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更
7.0(1)	キーワード ***configure*** が追加されました。

使用上のガイドライン

established コマンドで作成した確立されている接続を削除するには、***clear xlate*** コマンドを入力します。

例

次の例では、確立されたコマンドを削除する方法を示します。

```
hostname(config)# clear configure established
```

関連コマンド

コマンド	説明
established	確立されている接続に基づくポート上のリターン接続を許可します。
show running-config established	確立されている接続に基づく、許可済みの着信接続を表示します。
clear xlate	現在の変換スロット情報および接続スロット情報を消去します。

clear configure failover

コンフィギュレーションから **failover** コマンドを削除してデフォルトに戻すには、**clear configure failover** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure failover

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更
7.0(1)	このコマンドが **clear failover** から **clear configure failover** に変更されました。

使用上のガイドライン

このコマンドは、すべての **failover** コマンドを実行コンフィギュレーションから消去し、デフォルトに戻します。***all*** キーワードを **show running-config failover** コマンドとともに使用すると、デフォルトのフェールオーバー コンフィギュレーションが表示されます。

clear configure failover コマンドは、マルチ コンフィギュレーション モードのセキュリティ コンテキストでは使用できません。このコマンドはシステム実行スペースで入力する必要があります。

例

次の例では、コンフィギュレーションからすべてのフェールオーバー コマンドを消去します。

```
hostname(config)# clear configure failover
hostname(config)# show running-configuration failover
no failover
```

関連コマンド

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

clear configure filter

URL、FTP、および HTTPS フィルタリング コンフィギュレーションを消去するには、**clear configure filter** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure filter

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure filter コマンドは、URL、FTP、および HTTPS フィルタリング コンフィギュレーションを消去します。

例

次の例では、URL、FTP、および HTTPS フィルタリング コンフィギュレーションを消去します。

```
hostname# clear configure filter
```

関連コマンド

コマンド	説明
filter ftp	URL フィルタリング サーバによってフィルタリングされる FTP トラフィックを指定します。
filter https	Websense サーバによってフィルタリングされる HTTPS トラフィックを指定します。
filter url	トラフィックを URL フィルタリング サーバに誘導します。
show running-config filter	フィルタリング コンフィギュレーションを表示します。
url-server	**filter** コマンド用の N2H2 サーバまたは Websense サーバを指定します。

clear configure fips

NVRAM に格納されているシステムまたはモジュールの FIPS コンフィギュレーション情報を消去するには、**clear configure fips** コマンドを使用します。

clear configure fips

シンタックスの説明

fips	FIPS-2 準拠情報

デフォルト

このコマンドにデフォルト設定はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(4)	このコマンドが導入されました。

例

```
sw8-ASA(config)# clear configure fips
```

関連コマンド

コマンド	説明
crashinfo console disable	フラッシュに対するクラッシュ書き込み情報の読み取り、書き込み、および設定をディセーブルにします。
fips enable	システムまたはモジュールに対して FIPS 準拠を強制するためのポリシーチェックをイネーブルまたはディセーブルにします。
fips self-test poweron	パワーオン セルフテストを実行します。
show crashinfo console	フラッシュに対するクラッシュ書き込みの読み取り、書き込み、および設定を行います。
show running-config fips	セキュリティ アプライアンス上で実行されている FIPS コンフィギュレーションを表示します。

clear configure firewall

ファイアウォール モードをデフォルトのルーテッド モードに設定するには、**clear configure firewall** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure firewall

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、ファイアウォール モードをデフォルトに設定します。

```
hostname(config)# clear configure firewall
```

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。
firewall transparent	ファイアウォール モードを透過に設定します。
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。

clear configure fixup

フィックスアップ コンフィギュレーションを消去するには、**clear configure fixup** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure fixup

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

clear configure fixup コマンドは、フィックスアップ コンフィギュレーションを削除します。

例

次の例では、フィックスアップ コンフィギュレーションを消去します。

```
hostname# clear configure fixup
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
policy-map	クラスマップを特定のセキュリティ アクションに関連付けます。

clear configure fragment

すべての IP フラグメント再構成コンフィギュレーションをデフォルトにリセットするには、**clear configure fragment** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure fragment [*interface*]

シンタックスの説明

interface	（オプション）セキュリティ アプライアンスのインターフェイスを指定します。

デフォルト

interface が指定されていない場合、このコマンドはすべてのインターフェイスに適用されます。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	***configure*** キーワードおよびオプションの *interface* 引数が追加されました。また、このコマンドは、運用データの消去とコンフィギュレーション データの消去を区別するため、***clear fragment*** と ***clear configure fragment*** の 2 つのコマンドに分けられました。

使用上のガイドライン

clear configure fragment コマンドは、すべての IP フラグメント再構成コンフィギュレーションをデフォルトにリセットします。また、**chain**、**size**、および **timeout** キーワードが次のデフォルト値にリセットされます。

- ***chain*** は 24 パケット
- ***size*** は 200
- ***timeout*** は 5 秒

例

次の例では、すべての IP フラグメント再構成コンフィギュレーションをデフォルトにリセットする方法を示します。

```
hostname(config)# clear configure fragment
```

関連コマンド

コマンド	説明
clear fragment	IP フラグメント再構成モジュールの運用データを消去します。
fragment	特別なパケット フラグメント化の管理を提供して、NFS との互換性を改善します。
show fragment	IP フラグメント再構成モジュールの運用データを表示します。
show running-config fragment	IP フラグメント再構成コンフィギュレーションを表示します。

clear configure ftp

FTP コンフィギュレーションを消去するには、**clear configure ftp** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure ftp

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure ftp コマンドは、FTP コンフィギュレーションを消去します。

例

次の例では、FTP コンフィギュレーションを消去します。

```
hostname# clear configure filter
```

関連コマンド

コマンド	説明
filter ftp	URL フィルタリング サーバによってフィルタリングされる FTP トラフィックを指定します。
filter https	Websense サーバによってフィルタリングされる HTTPS トラフィックを指定します。
filter url	トラフィックを URL フィルタリング サーバに誘導します。
show running-config filter	フィルタリング コンフィギュレーションを表示します。
url-server	**filter** コマンド用の N2H2 サーバまたは Websense サーバを指定します。

clear configure ftp-map

FTP マップ コンフィギュレーションを消去するには、**clear configure ftp-map** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure ftp-map

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure ftp-map コマンドは、FTP マップ コンフィギュレーションを削除します。

例

次の例では、FTP マップ コンフィギュレーションを消去します。

```
hostname# clear configure ftp-map
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
ftp-map	FTP マップを定義し、FTP マップ コンフィギュレーション モードをイネーブルにします。
inspect ftp	アプリケーション検査用に特定の FTP マップを適用します。
request-command deny	禁止する FTP コマンドを指定します。

clear configure global

コンフィギュレーションから **global** コマンドを削除するには、**clear configure global** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure global

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	キーワード ***configure*** が追加されました。

例

次の例では、コンフィギュレーションから **global** コマンドを削除する方法を示します。

```
hostname(config)# clear configure global
```

関連コマンド

コマンド	説明
global	グローバル アドレス プールに対してエントリを作成します。
show running-config global	コンフィギュレーション内の **global** コマンドを表示します。

clear configure group-policy

特定のグループポリシーのコンフィギュレーションを削除するには、**clear configure group-policy** コマンドをグローバル コンフィギュレーション モードで使用し、グループポリシーの名前を付加します。デフォルトのグループポリシー以外のすべての group-policy コマンドをコンフィギュレーションから削除するには、このコマンドを引数なしで使用します。

clear configure group-policy [*name*]

シンタックスの説明

name	グループポリシーの名前を指定します。

デフォルト

デフォルトのグループポリシー以外のすべての group-policy コマンドをコンフィギュレーションから削除します。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、FirstGroup という名前のグループポリシーのコンフィギュレーションを消去する方法を示します。

```
hostname(config)# clear configure group-policy FirstGroup
```

関連コマンド

コマンド	説明
group-policy	グループポリシーを作成、編集、または削除します。
group-policy attributes	指定したグループポリシーの AVP を設定できるグループポリシー アトリビュート モードに入ります。
show running-config group-policy	特定のグループポリシーまたはすべてのグループポリシーの実行コンフィギュレーションを表示します。

clear configure gtp-map

GTP マップ コンフィギュレーションを消去するには、**clear configure gtp-map** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure gtp-map

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure gtp -map コマンドは、GTP マップ コンフィギュレーションを削除します。

例

次の例では、GTP マップ コンフィギュレーションを消去します。

```
hostname# clear configure gtp-map
```

関連コマンド

コマンド	説明
clear service-policy inspect gtp	グローバル GTP 統計情報を消去します。
debug gtp	GTP 検査に関する詳細情報を表示します。
gtp-map	GTP マップを定義し、GTP マップ コンフィギュレーション モードをイネーブルにします。
inspect gtp	アプリケーション検査用に特定の 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。

clear configure http

HTTP サーバをディセーブルにし、HTTP サーバにアクセスできる設定済みホストを削除するには、**clear configure http** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure http

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、HTTP コンフィギュレーションを消去する方法を示します。

```
hostname(config)# clear configure http
```

関連コマンド

コマンド	説明
http	IP アドレスとサブネット マスクによって、HTTP サーバにアクセスできるホストを指定します。ホストが HTTP サーバにアクセスするときに通過するセキュリティ アプライアンス インターフェイスを指定します。
http authentication-certificate	セキュリティ アプライアンスへの HTTPS 接続を確立するユーザに証明書による認証を要求します。
http redirect	セキュリティ アプライアンスが HTTP 接続を HTTPS にリダイレクトするように指定します。
http server enable	HTTP サーバをイネーブルにします。
show running-config http	HTTP サーバにアクセスできるホストを表示し、さらに HTTP サーバがイネーブルであるかどうかを表示します。

clear configure http-map

HTTP マップ コンフィギュレーションを消去するには、**clear configure http-map** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure http-map

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure http-map コマンドは、HTTP マップ コンフィギュレーションを削除します。

例

次の例では、HTTP マップ コンフィギュレーションを消去します。

```
hostname# clear configure http-map
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
debug http-map	HTTP マップに関連付けられているトラフィックに関する詳細情報を表示します。
http-map	高度な HTTP 検査を設定するための HTTP マップを定義します。
inspect http	アプリケーション検査用に特定の HTTP マップを適用します。
policy-map	クラスマップを特定のセキュリティ アクションに関連付けます。

clear configure icmp

ICMP トラフィックの設定済みアクセス規則を消去するには、**clear configure icmp** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure icmp

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure icmp コマンドは、ICMP トラフィックの設定済みアクセス規則を消去します。

例

次の例では、ICMP トラフィックの設定済みアクセス規則を消去します。

```
hostname# clear configure icmp
```

関連コマンド

コマンド	説明
clear configure icmp	ICMP コンフィギュレーションを消去します。
debug icmp	ICMP に関するデバッグ情報の表示をイネーブルにします。
show icmp	ICMP コンフィギュレーションを表示します。
timeout icmp	ICMP のアイドル タイムアウトを設定します。

clear configure imap4s

コンフィギュレーションからすべての IMAP4S コマンドを削除してデフォルト値に戻すには、**clear configure imap4s** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure imap4s

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、IMAP4S コンフィギュレーションを削除する方法を示します。

```
hostname(config)# clear configure imap4s
hostname(config)#
```

関連コマンド

コマンド	説明
show running-config imap4s	IMAP4S の実行コンフィギュレーションを表示します。
imap4s	IMAP4S 電子メール プロキシのコンフィギュレーションを作成または編集します。

clear configure interface

インターフェイス コンフィギュレーションを消去するには、**clear configure interface** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure interface [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*]

シンタックスの説明

interface_name	（オプション）**nameif** コマンドで設定したインターフェイス名を指定します。
mapped_name	（オプション）マルチ コンテキスト モードで、マッピング名を **allocate-interface** コマンドを使用して割り当てた場合、その名前を指定します。
physical_interface	（オプション）インターフェイス ID（***gigabit*ethernet0/1** など）を指定します。使用できる値については、**interface** コマンドを参照してください。
subinterface	（オプション）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。

デフォルト

インターフェイスを指定しない場合、セキュリティ アプライアンスはすべてのインターフェイス コンフィギュレーションを消去します。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更
7.0(1)	このコマンドが、**clear interface** から変更されました。また、新しいインターフェイスの番号付け方式も含めるように修正されました。

使用上のガイドライン

メインの物理インターフェイスのインターフェイス コンフィギュレーションを消去する場合、セキュリティ アプライアンスではデフォルト設定が使用されます。

インターフェイス名をシステム実行スペースで使用することはできません。これは、**nameif** コマンドはコンテキスト内でのみ使用できるためです。同様に、**allocate-interface** コマンドを使用してインターフェイス ID をマッピング名にマッピングした場合、そのマッピング名はコンテキスト内でのみ使用できます。

例

次の例では、GigabitEthernet0/1 コンフィギュレーションを消去します。

```
hostname(config)# clear configure interface gigabitethernet0/1
```

次の例では、内部インターフェイス コンフィギュレーションを消去します。

```
hostname(config)# clear configure interface inside
```

次の例では、コンテキスト内で int1 インターフェイス コンフィギュレーションを消去します。「int1」はマッピング名です。

```
hostname/contexta(config)# clear configure interface int1
```

次の例では、すべてのインターフェイス コンフィギュレーションを消去します。

```
hostname(config)# clear configure interface
```

関連コマンド

コマンド	説明
allocate-interface	セキュリティ コンテキストにインターフェイスおよびサブインターフェイスを割り当てます。
clear interface	**show interface** コマンドのカウンタをクリアします。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
show interface	インターフェイスのランタイム ステータスと統計情報を表示します。

clear configure ip

ip address コマンドで設定されたすべての IP アドレスを消去するには、**clear configure ip** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure ip

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドがサポートされるようになりました。

使用上のガイドライン

透過ファイアウォール モードの場合、このコマンドは管理 IP アドレスを消去します。

古い IP アドレスを使用する現在の接続をすべて停止するには、**clear xlate** コマンドを入力します。入力しない場合、接続は通常どおりタイムアウトします。

例

次の例では、すべての IP アドレスを消去します。

```
hostname(config)# clear configure ip
```

関連コマンド

コマンド	説明
allocate-interface	セキュリティ コンテキストにインターフェイスおよびサブインターフェイスを割り当てます。
clear configure interface	インターフェイスのコンフィギュレーションをすべて消去します。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
ip address	インターフェイスの IP アドレスを設定します。
show running-config interface	インターフェイスのコンフィギュレーションを表示します。

clear configure ip audit

監査ポリシー コンフィギュレーション全体を消去するには、**clear configure ip audit** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure ip audit [**configuration**]

シンタックスの説明

configuration	（オプション）このキーワードを入力できますが、使用しない場合も結果は同じです。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが **clear ip audit** から変更されました。

例

次の例では、すべての **ip audit** コマンドを消去します。

```
hostname# clear configure ip audit
```

関連コマンド

コマンド	説明
ip audit attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit info	情報シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit interface	インターフェイスに監査ポリシーを割り当てます。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
ip audit signature	シグニチャをディセーブルにします。

clear configure ip local pool

IP アドレス プールを削除するには、**clear configure ip local pool** コマンドをグローバル コンフィギュレーション モードで使用します。

clear ip local pool [*poolname*]

シンタックスの説明

poolname	（オプション）IP アドレス プールの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、実行コンフィギュレーションからすべての IP アドレス プールを削除します。

```
hostname(config)# clear config ip local pool
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure ip local pool	すべての ip ローカル プールを削除します。
ip local pool	IP アドレス プールを設定します。

clear configure ip verify reverse-path

ip verify reverse-path コンフィギュレーションを消去するには、**clear configure ip verify reverse-path** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure ip verify reverse-path

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが、**clear ip verify reverse-path** から変更されました。

例

次の例では、すべてのインターフェイスの **ip verify reverse-path** コンフィギュレーションを消去します。

```
hostname(config)# clear configure ip verify reverse-path
```

関連コマンド

コマンド	説明
clear ip verify statistics	Unicast RPF の統計情報を消去します。
ip verify reverse-path	Unicast Reverse Path Forwarding 機能をイネーブルにして IP スプーフィングを防止します。
show ip verify statistics	Unicast RPF の統計情報を表示します。
show running-config ip verify reverse-path	**ip verify reverse-path** コンフィギュレーションを表示します。

clear configure ipv6

実行コンフィギュレーションからグローバル IPv6 コマンドを消去するには、**clear configure ipv6** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure ipv6 [*route* | *access-list*]

シンタックスの説明

route	（オプション）実行コンフィギュレーションから IPv6 ルーティング テーブル内のルートをスタティックに定義するコマンドを消去します。
access-list	（オプション）実行コンフィギュレーションから IPv6 アクセスリスト コマンドを消去します。

デフォルト

キーワードを指定しない場合、このコマンドでは実行コンフィギュレーションからすべての IPv6 コマンドが消去されます。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドでは、実行コンフィギュレーションからグローバル IPv6 コマンドだけが消去されます。インターフェイス コンフィギュレーション モードで入力した IPv6 コマンドは消去されません。

例

次の例では、IPv6 ルーティング テーブルからスタティックに定義された IPv6 ルートを消去する方法を示します。

```
hostname(config)# clear configure ipv6 route
hostname(config)#
```

関連コマンド

コマンド	説明
ipv6 route	IPv6 ルーティング テーブル内のスタティック ルートを定義します。
show ipv6 route	IPv6 ルーティング テーブルの内容を表示します。
show running-config ipv6	実行コンフィギュレーション内の IPv6 コマンドを表示します。

clear configure isakmp

すべての ISAKMP コンフィギュレーションを削除するには、**clear configure isakmp** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure isakmp

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで発行した次の例では、セキュリティ アプライアンスからすべての ISAKMP コンフィギュレーションを削除します。

```
hostname(config)# clear configure isakmp
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show isakmp stats	実行時の統計情報を表示します。
show isakmp sa	追加情報を含め、IKE ランタイム SA データベースを表示します。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

clear configure isakmp policy

すべての ISAKMP ポリシー コンフィギュレーションを削除するには、**clear configure isakmp policy** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure isakmp policy *priority*

シンタックスの説明

priority	消去する ISAKMP ポリシーの優先順位を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、コンフィギュレーションから優先順位 3 の ISAKMP ポリシーを削除します。

```
hostname(config)# clear configure isakmp policy 3
hostname(config)#
```

関連コマンド

コマンド	説明
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show isakmp stats	実行時の統計情報を表示します。
show isakmp sa	追加情報を含め、IKE ランタイム SA データベースを表示します。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

clear configure logging

ロギング コンフィギュレーションを消去するには、**clear configure logging** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure logging [*disabled* | *level* | *rate-limit*]

シンタックスの説明

disabled	（オプション）ディセーブルになっているすべてのシステム ログ メッセージを再度イネーブルにすることを指定します。このオプションを使用する場合、他のロギング コンフィギュレーションは消去されません。
level	（オプション）システム ログ メッセージへの重大度の割り当てをデフォルト値にリセットすることを指定します。このオプションを使用する場合、他のロギング コンフィギュレーションは消去されません。
rate-limit	（オプション）ロギング レート制限をリセットします。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。
7.0(4)	**rate-limit** キーワードが導入されました。

使用上のガイドライン

show running-config logging コマンドを使用して、すべてのロギング コンフィギュレーションを表示できます。**clear configure logging** コマンドを disabled または level キーワードなしで使用した場合、すべてのロギング コンフィギュレーションが消去されます。

例

次の例では、ロギング コンフィギュレーションを消去する方法を示します。**show logging** コマンドの出力は、すべてのロギング機能がディセーブルになっていることを示します。

```
hostname(config)# clear configure logging
hostname(config)# show logging
Syslog logging: disabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
```

関連コマンド

コマンド	説明
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのロギング関連の部分を表示します。

clear configure mac-address-table

mac-address-table static および **mac-address-table aging-time** コンフィギュレーションを消去するには、**clear configure mac-address-table** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure mac-address-table

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトの動作や値はありません。

コマンドのモード　次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例　次の例では、**mac-address-table static** および **mac-address-table aging-time** コンフィギュレーションを消去します。

```
hostname# clear configure mac-address-table
```

関連コマンド

コマンド	説明
firewall transparent	ファイアウォール モードを透過に設定します。
mac-address-table aging-time	ダイナミック MAC アドレス エントリのタイムアウトを設定します。
mac-address-table static	MAC アドレス テーブルにスタティック MAC アドレス エントリを追加します。
mac-learn	インターフェイスの MAC アドレス ラーニングをディセーブルにします。
show mac-address-table	ダイナミック エントリとスタティック エントリを含め、MAC アドレス テーブルを表示します。

clear configure mac-learn

mac-learn コンフィギュレーションを消去するには、**clear configure mac-learn** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure mac-learn

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、**mac-learn** コンフィギュレーションを消去します。

```
hostname# clear configure mac-learn
```

関連コマンド

コマンド	説明
firewall transparent	ファイアウォール モードを透過に設定します。
mac-address-table static	MAC アドレス テーブルにスタティック MAC アドレス エントリを追加します。
mac-learn	インターフェイスの MAC アドレス ラーニングをディセーブルにします。
show mac-address-table	ダイナミック エントリとスタティック エントリを含め、MAC アドレス テーブルを表示します。

clear configure mac-list

以前に **mac-list** コマンドで指定された MAC アドレスの指定したリストを削除するには、**clear configure mac-list** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure mac-list *id*

シンタックスの説明

id	MAC アドレス リスト名。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	CLI 規格に適合するように、このコマンドが修正されました。

使用上のガイドライン

MAC アドレスのリストを削除するには、**clear mac-list** コマンドを使用します。

例

次の例では、MAC アドレス リストを消去する方法を示します。

```
hostname(config)# clear configure mac-list firstmaclist
```

関連コマンド

コマンド	説明
mac-list	先頭一致検索を使用して MAC アドレスのリストを追加します。
show running-config mac-list	*id* 値によって示される MAC アドレス リストの MAC アドレスを表示します。

clear configure management-access

セキュリティ アプライアンスの管理アクセスのための内部インターフェイスのコンフィギュレーションを削除するには、***clear configure management-access*** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure management-access

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更
7.0(1)	キーワード ***configure*** が追加されました。

使用上のガイドライン

management-access コマンドを使用すると、*mgmt_if* で指定したファイアウォール インターフェイスの IP アドレスを使用して、内部管理インターフェイスを定義できます（インターフェイス名は **nameif** コマンドによって定義され、**show interface** コマンドの出力で引用符 " " に囲まれて表示されます）。***clear configure management-access*** コマンドは、***management-access*** コマンドで指定した内部管理インターフェイスのコンフィギュレーションを削除します。

例

次の例では、セキュリティ アプライアンスの管理アクセスのための、内部インターフェイスのコンフィギュレーションを削除します。

```
hostname(config)# clear configure management-access
```

関連コマンド

コマンド	説明
management-access	管理アクセス用の内部インターフェイスを設定します。
show running-config management-access	管理アクセス用に設定されている内部インターフェイスの名前を表示します。

clear configure mgcp-map

MGCP マップ コンフィギュレーションを消去するには、**clear configure mgcp-map** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure mgcp-map

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure mgcp-map は、MGCP マップ コンフィギュレーションを消去します。

例

次の例では、MGCP マップ コンフィギュレーションを消去します。

```
hostname# clear configure mgcp-map
```

関連コマンド

コマンド	説明
debug mgcp	MGCP デバッグ情報をイネーブルにします。
mgcp-map	MGCP マップを定義し、MGCP マップ コンフィギュレーション モードをイネーブルにします。
show conn	さまざまな接続タイプの接続状態を表示します。
show mgcp	セキュリティ アプライアンスを介して確立された MGCP セッションに関する情報を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

clear configure mroute

実行コンフィギュレーションから **mroute** コマンドを削除するには、**clear configure mroute** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure mroute

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、コンフィギュレーションから **mroute** コマンドを削除する方法を示します。

```
hostname(config)# clear configure mroute
hostname(config)#
```

関連コマンド

コマンド	説明
mroute	スタティック マルチキャスト ルートを設定します。
show mroute	IPv4 マルチキャスト ルーティング テーブルを表示します。
show running-config mroute	実行コンフィギュレーション内の **mroute** コマンドを表示します。

clear configure mtu

すべてのインターフェイスの設定済み最大伝送ユニット値を消去するには、**clear configure mtu** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure mtu

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

clear configure mtu コマンドを使用すると、すべてのイーサネット インターフェイスの最大伝送ユニットがデフォルトの 1500 に設定されます。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

例

次の例では、すべてのインターフェイスの現在の最大伝送ユニット値を消去します。

```
hostname(config)# clear configure mtu
```

関連コマンド

コマンド	説明
mtu	インターフェイスの最大伝送ユニットを指定します。
show running-config mtu	現在の最大伝送ユニットのブロック サイズを表示します。

clear configure multicast-routing

実行コンフィギュレーションから **multicast-routing** コマンドを削除するには、**clear configure multicast-routing** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure *multicast-routing*

シンタックスの説明

このコマンドには、キーワードも引数もありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure multicast-routing コマンドは、実行コンフィギュレーションから **multicast-routing** を削除します。**no multicast-routing** コマンドも、実行コンフィギュレーションから multicast-routing コマンドを削除します。

例

次の例では、実行コンフィギュレーションから **multicast-routing** コマンドを削除する方法を示します。

```
hostname(config)# clear configure multicast-routing
```

関連コマンド

コマンド	説明
multicast-routing	セキュリティ アプライアンス上のマルチキャスト ルーティングをイネーブルにします。

clear configure name

コンフィギュレーションから名前のリストを消去するには、**clear configure name** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure name

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	キーワード ***configure*** が追加されました。

使用上のガイドライン

このコマンドに使用上のガイドラインはありません。

例

次の例では、名前のリストを消去する方法を示します。

```
hostname(config)# clear configure name
```

関連コマンド

コマンド	説明
name	名前を IP アドレスに関連付けます。
show running-config name	IP アドレスに関連付けられている名前のリストを表示します。

clear configure nat

NAT コンフィギュレーションを削除するには、**clear configure nat** コマンドを特権 EXEC モードで使用します。

clear configure nat

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更
7.0(1)	キーワード ***configure*** が追加されました。

使用上のガイドライン

透過ファイアウォール モードには、次の注意事項が適用されます。

（注）　透過ファイアウォール モードでは、NAT id 0 のみが有効です。

例

次の例では、NAT コンフィギュレーションを削除する方法を示します。

```
hostname(config)# clear configure nat
```

関連コマンド

コマンド	説明
nat	ネットワークをグローバル IP アドレス プールに関連付けます。
show running-config nat	ネットワークに関連付けられているグローバル IP アドレスのプールを表示します。

clear configure ntp

NTP コンフィギュレーションを消去するには、**clear configure ntp** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure ntp

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが、**clear ntp** から変更されました。

例

次の例では、すべての **ntp** コマンドを消去します。

```
hostname# clear configure ntp
```

関連コマンド

コマンド	説明
ntp authenticate	NTP 認証をイネーブルにします。
ntp authentication-key	NTP 認証キーを設定します。
ntp server	セキュリティ アプライアンスの時間を設定する NTP サーバを指定します。
ntp trusted-key	NTP の信頼できるキーを指定します。
show running-config ntp	NTP コンフィギュレーションを表示します。

clear configure object-group

コンフィギュレーションからすべての **object group** コマンドを削除するには、**clear configure object-group** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure object-group [{**protocol** | **service** | **icmp-type** | **network**}]

シンタックスの説明

icmp-type	（オプション）すべての ICMP グループを消去します。
network	（オプション）すべてのネットワーク グループを消去します。
protocol	（オプション）すべてのプロトコル グループを消去します。
service	（オプション）すべてのサービス グループを消去します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

例

次の例では、コンフィギュレーションからすべての **object-group** コマンドを削除する方法を示します。

```
hostname(config)# clear configure object-group
```

関連コマンド

コマンド	説明
group-object	ネットワーク オブジェクト グループを追加します。
network-object	ネットワーク オブジェクト グループにネットワーク オブジェクトを追加します。
object-group	コンフィギュレーションを最適化するためのオブジェクト グループを定義します。
port-object	サービス オブジェクト グループにポート オブジェクトを追加します。
show running-config object-group	現在のオブジェクト グループを表示します。

clear configure passwd

ログイン パスワード コンフィギュレーションを消去し、デフォルト設定の「cisco」に戻すには、**clear configure passwd** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure {**passwd** | **password**}

シンタックスの説明

***passwd*	*password***	どちらのコマンドでも入力できます。これらは互いにエイリアス関係にあります。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更
7.0(1)	このコマンドが、**clear passwd** から変更されました。

例

次の例では、ログイン パスワードを消去し、デフォルトの「cisco」に戻します。

```
hostname(config)# clear configure passwd
```

関連コマンド

コマンド	説明
enable	特権 EXEC モードに入ります。
enable password	イネーブル パスワードを設定します。
passwd	ログイン パスワードを設定します。
show curpriv	現在ログインしているユーザの名前および特権レベルを表示します。
show running-config passwd	ログイン パスワードを暗号化された形式で表示します。

clear configure pim

実行コンフィギュレーションからすべてのグローバル **pim** コマンドを消去するには、**clear configure pim** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure *pim*

シンタックスの説明

このコマンドには、キーワードも引数もありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure pim コマンドは、実行コンフィギュレーションからすべての **pim** コマンドを消去します。PIM トラフィック カウンタおよびトポロジ情報を消去するには、**clear pim counters** コマンドおよび **clear pim topology** コマンドを使用します。

clear configure pim コマンドはグローバル コンフィギュレーション モードで入力された **pim** コマンドだけを消去します。インターフェイス固有の **pim** コマンドは消去しません。

例

次の例では、実行コンフィギュレーションからすべての **pim** コマンドを消去する方法を示します。

```
hostname(config)# clear configure pim
```

関連コマンド

コマンド	説明
clear pim topology	PIM トポロジ テーブルをクリアします。
clear pim counters	PIM トラフィック カウンタをクリアします。
show running-config pim	実行コンフィギュレーション内の **pim** コマンドを表示します。

clear configure policy-map

コンフィギュレーションからポリシーマップの指定を削除するには、**clear configure policy-map** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure policy-map

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次に、**clear configure policy-map** コマンドの例を示します。

```
hostname(config)# clear configure policy-map
```

関連コマンド

コマンド	説明
policy-map	ポリシー（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
show running-config policy-map	ポリシー コンフィギュレーション全体を表示します。

clear configure pop3s

コンフィギュレーションからすべての POP3S コマンドを削除してデフォルト値に戻すには、**clear configure pop3s** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure pop3s

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、POP3S コンフィギュレーションを削除する方法を示します。

```
hostname(config)# clear configure pop3s
hostname(config)#
```

関連コマンド

コマンド	説明
show running-config pop3s	POP3S の実行コンフィギュレーションを表示します。
pop3s	POP3S 電子メール プロキシのコンフィギュレーションを作成または編集します。

clear configure port-forward

WebVPN ユーザが転送 TCP ポート経由でアクセスする設定済みのアプリケーションのセットを削除するには、**clear configure port-forward** コマンドをグローバル コンフィギュレーション モードで使用します。設定済みのアプリケーションをすべて削除するには、このコマンドを *listname* 引数なしで使用します。特定のリストのアプリケーションだけを削除するには、このコマンドに *listname* を付けて使用します。

clear configure port-forward [*listname*]

シンタックスの説明

listname	WebVPN ユーザがアクセスできるアプリケーション（転送 TCP ポート）のセットをグループ化します。最大 64 文字です。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、*SalesGroupPorts* という名前のポート転送リストを削除する方法を示します。

```
hostname(config)# clear configure port-forward SalesGroupPorts
```

関連コマンド

コマンド	説明
port-forward	WebVPN ユーザがアクセスできるアプリケーションのセットを設定するには、このコマンドを WebVPN コンフィギュレーション モードで使用します。
port-forward	ユーザまたはグループポリシーの WebVPN アプリケーション アクセスをイネーブルにするには、webvpn モードでこのコマンドを使用します。
show running-configuration port-forward	現在設定されている **port-forward** コマンドのセットを表示します。

clear configure prefix-list

実行コンフィギュレーションから **prefix-list** コマンドを削除するには、**clear configure prefix-list** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure prefix-list [*prefix-list-name*]

シンタックスの説明

prefix-list-name	（オプション）プレフィックス リストの名前。プレフィックス リスト名を指定した場合は、そのプレフィックス リストのコマンドだけがコンフィギュレーションから削除されます。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが、**clear prefix-list** から **clear configure prefix-list** に変更されました。

使用上のガイドライン

clear configure prefix-list コマンドは、実行コンフィギュレーションから **prefix-list** コマンドおよび **prefix-list description** コマンドを削除します。プレフィックス リスト名を指定した場合は、実行コンフィギュレーションからそのプレフィックス リストの **prefix-list** コマンドと **prefix-list description** コマンド（存在する場合）だけが削除されます。

このコマンドは、実行コンフィギュレーションから **no prefix-list sequence** コマンドを削除しません。

例

次の例では、実行コンフィギュレーションから MyPrefixList という名前のプレフィックス リストのすべての **prefix-list** コマンドを削除します。

```
hostname# clear configure prefix-list MyPrefixList
```

関連コマンド

コマンド	説明
show running-config prefix-list	実行コンフィギュレーション内の **prefix-list** コマンドを表示します。

clear configure priority-queue

コンフィギュレーションからプライオリティキューの指定を削除するには、**clear configure priority-queue** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure priority queue *interface-name*

シンタックスの説明

interface-name	プライオリティキューの詳細を表示するインターフェイスの名前を指定します。

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、**clear configure priority-queue** コマンドを使用して、test という名前のインターフェイスでプライオリティキュー コンフィギュレーションを削除する方法を示します。

```
hostname(config)# clear configure priority-queue test
```

関連コマンド

コマンド	説明
priority-queue	インターフェイスにプライオリティ キューイングを設定します。
show running-config priority-queue	指定したインターフェイスの現在のプライオリティキュー コンフィギュレーションを表示します。

clear configure privilege

コマンドの設定済みの特権レベルを削除するには、**clear configure privilege** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure privilege

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトの動作や値はありません。

コマンドのモード　次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	CLI ガイドラインに沿うように、このコマンドが変更されました。

使用上のガイドライン　元に戻すことはできません。

例　次の例では、コマンドの設定済みの特権レベルをリセットする方法を示します。

```
hostname(config)# clear configure privilege
```

関連コマンド

コマンド	説明
privilege	コマンド特権レベルを設定します。
show curpriv	現在の特権レベルを表示します。
show running-config privilege	コマンドの特権レベルを表示します。

clear configure rip

実行コンフィギュレーションから **rip** コマンドを消去するには、**clear configure rip** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure *rip*

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが、**clear rip** から **clear configure rip** に変更されました。

使用上のガイドライン

clear configure rip コマンドは、コンフィギュレーションからすべての **rip** コマンドを削除します。特定のコマンドを消去するには、このコマンドの **no** 形式を使用します。

例

次の例では、実行コンフィギュレーションからすべての RIP コマンドを消去します。

```
hostname(config)# clear configure rip
```

関連コマンド

コマンド	説明
debug rip	RIP に関するデバッグ情報を表示します。
rip	指定したインターフェイスに RIP を設定します。
show running-config rip	実行コンフィギュレーション内の RIP コマンドを表示します。

clear configure route

connect キーワードを含んでいないコンフィギュレーションから **route** コマンドを削除するには、**clear configure route** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure route [*interface_name ip_address* [*netmask gateway_ip*]]

シンタックスの説明

gateway_ip	（オプション）ゲートウェイ ルータの IP アドレスを指定します（このルートのネクストホップ アドレス）。
interface_name	（オプション）内部または外部のネットワーク インターフェイス名。
ip_address	（オプション）内部または外部のネットワーク IP アドレス。
netmask	（オプション）*ip_address* に適用するネットワーク マスクを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	キーワード ***configure*** が追加されました。

使用上のガイドライン

デフォルト ルートを指定するには、**0.0.0.0** を使用します。0.0.0.0 IP アドレスは **0** に、0.0.0.0 *netmask* は **0** に省略できます。

例

次の例では、**connect** キーワードを含んでいないコンフィギュレーションから **route** コマンドを削除する方法を示します。

```
hostname(config)# clear configure route
```

関連コマンド

コマンド	説明
route	インターフェイスのスタティック ルートまたはデフォルト ルートを指定します。
show route	ルート情報を表示します。
show running-config route	設定されているルートを表示します。

clear configure route-map

すべてのルートマップを削除するには、**clear configure route-map** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure route-map

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

コンフィギュレーション内のすべての **route-map** コマンドを削除するには、**clear configure route-map** コマンドをグローバル コンフィギュレーション モードで使用します。**route-map** コマンドは、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設定するために使用します。

個々の **route-map** コマンドを削除するには、**no route-map** コマンドを使用します。

例

次の例では、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削除する方法を示します。

```
hostname(config)# clear configure route-map
```

関連コマンド

コマンド	説明
route-map	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ための条件を定義します。
show running-config route-map	ルートマップ コンフィギュレーションに関する情報を表示します。

clear configure router

実行コンフィギュレーションからすべてのルータ コマンドを消去するには、**clear configure router** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure router [**ospf** *id*]

シンタックスの説明

id	OSPF プロセス ID。
ospf	コンフィギュレーションから OSPF コマンドだけを削除することを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが、**clear router** コマンドから **clear configure router** コマンドに変更されました。

例

次の例では、実行コンフィギュレーションから OSPF プロセス 1 に関連付けられたすべての OSPF コマンドを消去します。

```
hostname(config)# clear configure router ospf 1
hostname(config)#
```

関連コマンド

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内のコマンドを表示します。

clear configure service-policy

イネーブルになっているポリシーのサービス ポリシー コンフィギュレーションを消去するには、***clear configure service-policy*** コマンドを特権 EXEC モードで使用します。

clear configure service-policy

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更
PIX Version 7.0	このコマンドが導入されました。

例

次に、***clear service-policy*** コマンドの例を示します。

```
hostname(config)# clear configure service-policy
```

関連コマンド

コマンド	説明
show service-policy	サービス ポリシーを表示します。
show running-config service-policy	実行コンフィギュレーションに設定されているサービス ポリシーを表示します。
service-policy	サービス ポリシーを設定します。
clear service-policy	サービス ポリシーの統計情報を消去します。

clear configure smtps

コンフィギュレーションからすべての SMTPS コマンドを削除してデフォルト値に戻すには、**clear configure smtps** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure smtps

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、SMTPS コンフィギュレーションを削除する方法を示します。

```
hostname(config)# clear configure smtps
hostname(config)#
```

関連コマンド

コマンド	説明
show running-configuration smtps	SMTPS の実行コンフィギュレーションを表示します。
smtps	SMTPS 電子メール プロキシのコンフィギュレーションを作成または編集します。

clear configure snmp-map

SNMP マップ コンフィギュレーションを消去するには、**clear configure snmp-map** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure snmp-map

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure snmp-map コマンドは、SNMP マップ コンフィギュレーションを削除します。

例

次の例では、SNMP マップ コンフィギュレーションを消去します。

```
hostname# clear configure snmp-map
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
deny version	特定のバージョンの SNMP を使用するトラフィックを拒否します。
inspect snmp	SNMP アプリケーション検査をイネーブルにします。
snmp-map	SNMP マップを定義し、SNMP マップ コンフィギュレーション モードをイネーブルにします。

clear configure snmp-server

簡易ネットワーク管理プロトコル（SNMP）サーバをディセーブルにするには、**clear configure snmp-server** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure snmp-server

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

このコマンドにデフォルト設定はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更
7.0(1)	セキュリティ アプライアンスでこのコマンドがサポートされるようになりました。

例

この例は、SNMP サーバをディセーブルにする方法を示しています。

```
hostname #clear snmp-server
```

関連コマンド

コマンド	説明
snmp-server	SNMP を介してセキュリティ アプライアンスのイベント情報を提供します。
show snmp-server statistics	SNMP サーバのコンフィギュレーションに関する情報を表示します。

clear configure ssh

実行コンフィギュレーションからすべての SSH コマンドを消去するには、**clear configure ssh** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure ***ssh***

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが、**clear ssh** コマンドから **clear configure ssh** コマンドに変更されました。

使用上のガイドライン

このコマンドは、コンフィギュレーションからすべての SSH コマンドを消去します。特定のコマンドを消去するには、このコマンドの **no** 形式を使用します。

例

次の例では、コンフィギュレーションからすべての SSH コマンドを消去します。

```
hostname(config)# clear configure ssh
```

関連コマンド

コマンド	説明
show running-config ssh	実行コンフィギュレーション内の現在の SSH コマンドを表示します。
ssh	指定したクライアントまたはネットワークからセキュリティ アプライアンスへの SSH 接続を許可します。
ssh scopy enable	セキュリティ アプライアンス上でセキュア コピー サーバをイネーブルにします。
ssh timeout	アイドル状態の SSH セッションのタイムアウト値を設定します。
ssh version	セキュリティ アプライアンスが SSH Version 1 または SSH Version 2 のいずれかだけを使用するように制限します。

clear configure ssl

コンフィギュレーションからすべての SSL コマンドを削除してデフォルト値に戻すには、**clear config ssl** コマンドをグローバル コンフィギュレーション モードで使用します。

clear config ssl

デフォルト

デフォルトは次のとおりです。

- SSL クライアントおよび SSL サーバのバージョンは両方とも **any** です。
- SSL 暗号化は、3des-sha1 | des-sha1 | rc4-md5 の順序です。
- トラストポイント アソシエーションはありません。セキュリティ アプライアンスはデフォルトの RSA キーペア証明書を使用します。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、**clear config ssl** コマンドの使用方法を示します。

```
hostname(config)# clear config ssl
```

関連コマンド

コマンド	説明
show running-config ssl	現在設定されている ssl コマンドのセットを表示します。
ssl client-version	セキュリティ アプライアンスがクライアントとして動作する場合に使用する SSL プロトコルおよび TLS プロトコルのバージョンを指定します。
ssl server-version	セキュリティ アプライアンスがサーバとして動作する場合に使用する SSL プロトコルおよび TLS プロトコルのバージョンを指定します。
ssl trust-point	インターフェイスの SSL 証明書を表す証明書トラストポイントを指定します。

clear configure static

コンフィギュレーションからすべての **static** コマンドを削除するには、**clear configure static** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure static

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	キーワード ***configure*** が追加されました。

例

次の例では、コンフィギュレーションからすべての **static** コマンドを削除する方法を示します。

```
hostname(config)# clear configure static
```

関連コマンド

コマンド	説明
show running-config static	コンフィギュレーション内のすべての **static** コマンドを表示します。
static	ローカル IP アドレスをグローバル IP アドレスにマッピングすることによって、固定の 1 対 1 のアドレス変換規則を設定します。

clear configure sunrpc-server

セキュリティ アプライアンスからリモート プロセッサ コール サービスを消去するには、**clear configure sunrpc-server** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure sunrpc-server [**active**]

シンタックスの説明

active	（オプション）セキュリティ アプライアンスで現在アクティブな SunRPC サービスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

sunrpc-server コマンドは、設定された **router ospf** コマンドを表示します。

（注）　セキュリティ アプライアンス上で最上位の IP アドレスがプライベート アドレスの場合、このアドレスは hello パケットおよびデータベース定義で送信されます。このアクションを防止するには、**router-id** *ip_address* をグローバル アドレスに設定します。

例

次の例では、セキュリティ アプライアンスから SunRPC サービスを消去する方法を示します。

```
hostname(config)# clear configure sunrpc-server active
```

関連コマンド

コマンド	説明
sunrpc-server	SunRPC サービス テーブルを作成します。
show running-config sunrpc-server	SunRPC コンフィギュレーションに関する情報を表示します。

clear configure sysopt

すべての **sysopt** コマンドのコンフィギュレーションを消去するには、**clear configure sysopt** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure sysopt

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが、**clear sysopt** から変更されました。

例

次の例では、すべての **sysopt** コマンドのコンフィギュレーションを消去します。

```
hostname(config)# clear configure sysopt
```

関連コマンド

コマンド	説明
show running-config sysopt	**sysopt** コマンドのコンフィギュレーションを表示します。
sysopt connection permit-ipsec	ACL でインターフェイスをチェックせずに IPSec トンネルからのすべてのパケットを許可します。
sysopt connection tcpmss	TCP セグメントの最大サイズを上書きします。または、最大サイズが指定したサイズよりも小さくならないようにします。
sysopt connection timewait	最後の標準 TCP クローズダウン シーケンスの後、各 TCP 接続が短縮 TIME_WAIT 状態を保持するようにします。
sysopt nodnsalias	**alias** コマンドを使用するときに、DNS の A レコード アドレスの変更をディセーブルにします。

clear configure tcp-map

tcp マップ コンフィギュレーションを消去するには、**clear configure tcp-map** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure tcp-map

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、TCP マップ コンフィギュレーションを消去する方法を示します。

```
hostname(config)# clear configure tcp-map
```

関連コマンド

コマンド	説明
tcp-map	TCP マップを作成し、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。
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。

clear configure telnet

コンフィギュレーションから Telnet 接続およびアイドル タイムアウトを削除するには、**clear configure telnet** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure telnet

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	キーワード ***configure*** が追加されました。

例

次の例では、セキュリティ アプライアンスのコンフィギュレーションから Telnet 接続およびアイドル タイムアウトを削除する方法を示します。

```
hostname(config)# clear configure telnet
```

関連コマンド

コマンド	説明
show running-config telnet	セキュリティ アプライアンスへの Telnet 接続を使用することを認可されている IP アドレスの現在のリストを表示します。
telnet	Telnet アクセスをコンソールに追加し、アイドル タイムアウトを設定します。

clear configure terminal

端末の表示幅設定を消去するには、***clear configure terminal*** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure terminal

シンタックスの説明

このコマンドには、キーワードも引数もありません。

デフォルト

デフォルトの表示幅は 80 カラムです。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更
7.0(1)	***configure*** キーワードが追加されました。

例

次の例では、表示幅を消去します。

```
hostname# clear configure terminal
```

関連コマンド

コマンド	説明
terminal	端末回線のパラメータを設定します。
terminal width	端末の表示幅を設定します。
show running-config terminal	現在の端末設定を表示します。

clear configure timeout

コンフィギュレーションのデフォルトのアイドル状態の継続時間に戻すには、**clear configure timeout** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure timeout

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

例

次の例では、コンフィギュレーションからアイドル状態の最大継続時間を削除する方法を示します。

```
hostname(config)# clear configure timeout
```

関連コマンド

コマンド	説明
show running-config timeout	指定したプロトコルのタイムアウト値を表示します。
timeout	アイドル状態の最大継続時間を設定します。

clear configure tunnel-group

コンフィギュレーションからすべてのまたは指定したトンネルグループを削除するには、**clear config tunnel-group** コマンドをグローバル コンフィギュレーション モードで使用します。

clear config tunnel-group [*name*]

シンタックスの説明

name	（オプション）トンネルグループの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで入力した次の例では、コンフィギュレーションから toengineering トンネルグループを削除します。

```
hostname(config)# clear config tunnel-group toengineering
hostname(config)#
```

関連コマンド

コマンド	説明
show running-config tunnel-group	すべてのまたは選択したトンネルグループに関する情報を表示します。
tunnel-group	指定したタイプのトンネルグループ サブコンフィギュレーション モードに入ります。

clear configure url-block

URL 保留ブロック バッファおよび長い URL サポート コンフィギュレーションを消去するには、**clear configure url-block** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure url-block

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure url-block コマンドは、URL 保留ブロック バッファおよび長い URL サポート コンフィギュレーションを消去します。

例

次の例では、URL 保留ブロック バッファおよび長い URL サポート コンフィギュレーションを消去します。

```
hostname# clear configure url-block
```

関連コマンド

コマンド	説明
clear url-block block statistics	ブロック バッファ使用状況カウンタをクリアします。
show url-block	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-block	Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンド用の N2H2 サーバまたは Websense サーバを指定します。

clear configure url-cache

URL キャッシュを消去するには、**clear configure url-cache** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure url-cache

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure url-cache コマンドは、URL キャッシュを消去します。

例

次の例では、URL キャッシュを消去します。

```
hostname# clear configure url-cache
```

関連コマンド

コマンド	説明
clear url-cache statistics	コンフィギュレーションから **url-cache** コマンド文を削除します。
filter url	トラフィックを URL フィルタリング サーバに誘導します。
show url-cache statistics	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**scsc** コマンド用の N2H2 サーバまたは Websense サーバを指定します。

clear configure url-list

WebVPN ユーザがアクセスできる設定済みの URL のセットを削除するには、**clear configure url-list** コマンドをグローバル コンフィギュレーション モードで使用します。設定済みの URL をすべて削除するには、このコマンドを *listname* 引数なしで使用します。特定のリストの URL だけを削除するには、このコマンドに *listname* を付けて使用します。

clear configure url-list [*listname***]**

シンタックスの説明

listname	WebVPN ユーザがアクセスできる URL のセットをグループ化します。最大 64 文字です。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、*Marketing URLs* という名前の URL リストを削除する方法を示します。

```
hostname(config)# clear configure url-list Marketing URLs
```

関連コマンド

コマンド	説明
show running-configuration url-list	現在設定されている **url-list** コマンドのセットを表示します。
url-list	WebVPN ユーザがアクセスできる URL のセットを設定するには、このコマンドをグローバル コンフィギュレーション モードで使用します。
url-list	特定のグループポリシーまたはユーザの WebVPN URL アクセスをイネーブルにするには、グループポリシーまたはユーザ名モードからアクセスする WebVPN モードでこのコマンドを使用します。

clear configure url-server

URL フィルタリング サーバ コンフィギュレーションを消去するには、**clear configure url-server** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure url-server

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure url-server コマンドは、URL フィルタリング サーバ コンフィギュレーションを消去します。

例

次の例では、URL フィルタリング サーバ コンフィギュレーションを消去します。

```
hostname# clear configure url-server
```

関連コマンド

コマンド	説明
clear url-server	URL フィルタリング サーバの統計情報を消去します。
show url-server	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間に Web サーバの応答に使用される URL バッファを管理します。
url-server	**filter** コマンド用の N2H2 サーバまたは Websense サーバを指定します。

clear configure username

ユーザ名データベースを消去するには、**clear configure username** コマンドを使用します。特定のユーザのコンフィギュレーションを消去するには、このコマンドを使用し、ユーザ名を付加します。

clear configure username [*name*]

シンタックスの説明

name	（オプション）ユーザの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

内部ユーザ認証データベースは、username コマンドを使用して入力されたユーザで構成されています。login コマンドは、このデータベースを認証用に使用します。

例

次の例では、anyuser という名前のユーザのコンフィギュレーションを消去する方法を示します。

```
hostname(config)# clear configure username anyuser
```

関連コマンド

コマンド	説明
show running-config username	特定のユーザまたはすべてのユーザの実行コンフィギュレーションを表示します。
username	セキュリティ アプライアンス データベースにユーザを追加します。
username attributes	特定のユーザの AVP を設定できます。

clear configure virtual

コンフィギュレーションから認証仮想サーバを削除するには、**clear configure virtual** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure virtual

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	CLI ガイドラインに沿うように、このコマンドが変更されました。

使用上のガイドライン

元に戻すことはできません。

例

次に、**clear configure virtual** コマンドの例を示します。

```
hostname(config)# clear configure virtual
```

関連コマンド

コマンド	説明
show running-config virtual	認証仮想サーバの IP アドレスを表示します。
virtual http	セキュリティ アプライアンスと HTTP サーバでの別々の認証を可能にします。
virtual telnet	セキュリティ アプライアンスが認証プロンプトを提供しないトラフィック タイプの仮想 Telnet サーバを使用してユーザを認証します。

clear configure vpn load-balancing

以前に指定した VPN ロードバランシング コンフィギュレーションを削除して、VPN ロードバランシングをディセーブルにするには、**clear configure vpn load-balancing** コマンドをグローバル コンフィギュレーション モードで使用します。

clear configure vpn load-balancing

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure vpn load-balancing コマンドは、次の関連コマンドも消去します。**cluster encryption**、**cluster ip address**、**cluster key**、**cluster port**、**nat**、**participate**、および **priority**。

例

次のコマンドは、コンフィギュレーションから vpn ロードバランシング コンフィギュレーション文を削除します。

```
hostname(config)# clear configure vpn load-balancing
```

関連コマンド

show running-config vpn load-balancing	現在の VPN ロードバランシング コンフィギュレーションを表示します。
vpn load-balancing	vpn ロードバランシング モードに入ります。

clear console-output

現在キャプチャされているコンソール出力を削除するには、**clear console-output** コマンドを特権 EXEC モードで使用します。

clear console-output

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

例

次の例では、現在キャプチャされているコンソール出力を削除する方法を示します。

```
hostname# clear console-output
```

関連コマンド

コマンド	説明
show console-output	キャプチャされたコンソール出力を表示します。

clear counters

プロトコル スタック カウンタをクリアするには、**clear counters** コマンドをグローバル コンフィギュレーション モードで使用します。

clear counters [all | **context** *context-name* | **summary** | **top** *N* **]** [**detail**] [**protocol** *protocol_name* [**:***counter_name*]] [**threshold** *N*]

シンタックスの説明

all	（オプション）すべてのフィルタの詳細を消去します。
context *context-name*	（オプション）コンテキスト名を指定します。
:*counter_name*	（オプション）カウンタの名前を指定します。
detail	（オプション）詳細なカウンタ情報を消去します。
protocol *protocol_name*	（オプション）指定したプロトコルのカウンタをクリアします。
summary	（オプション）カウンタ情報を消去します。
threshold *N*	（オプション）指定したしきい値以上のカウンタをクリアします。範囲は 1 ～ 4294967295 です。
top *N*	（オプション）指定したしきい値以上のカウンタをクリアします。範囲は 1 ～ 4294967295 です。

デフォルト

clear counters summary detail

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、プロトコル スタック カウンタをクリアする方法を示します。

```
hostname(config)# clear counters
```

関連コマンド

コマンド	説明
show counters	プロトコル スタック カウンタを表示します。

clear crashinfo

フラッシュ メモリ内のクラッシュ ファイルの内容を削除するには、***clear crashinfo*** コマンドを特権 EXEC モードで入力します。

clear crashinfo

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトの動作や値はありません。

コマンドのモード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン　このコマンドに使用上のガイドラインはありません。

例　次のコマンドは、クラッシュ ファイルを削除する方法を示します。

```
hostname# clear crashinfo
```

関連コマンド

crashinfo force	セキュリティ アプライアンスを強制的にクラッシュさせます。
crashinfo save disable	フラッシュ メモリへのクラッシュ情報の書き込みをディセーブルにします。
crashinfo test	フラッシュ メモリ内のファイルにクラッシュ情報を保存する、セキュリティ アプライアンスの機能をテストします。
show crashinfo	フラッシュ メモリに保存されているクラッシュ ファイルの内容を表示します。

clear crypto accelerator statistics

暗号アクセラレータ MIB からグローバルな統計情報およびアクセラレータ固有の統計情報を消去するには、**clear crypto accelerator statistics** コマンドをグローバル コンフィギュレーション モードおよび特権 EXEC モードで使用します。

clear crypto accelerator statistics

シンタックスの説明

このコマンドには、キーワードも変数もありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで入力した次の例では、暗号アクセラレータの統計情報を表示します。

```
hostname(config)# clear crypto accelerator statistics
hostname(config)#
```

関連コマンド

コマンド	説明
clear crypto protocol statistics	暗号アクセラレータ MIB 内のプロトコル固有の統計情報を消去します。
show crypto accelerator statistics	暗号アクセラレータ MIB 内のグローバルな統計情報およびアクセラレータ固有の統計情報を表示します。
show crypto protocol statistics	暗号アクセラレータ MIB 内のプロトコル固有の統計情報を表示します。

clear crypto ca crls

指定したトラストポイントに関連付けられたすべての CRL の CRL キャッシュを削除、またはすべての CRL の CRL キャッシュを削除するには、**clear crypto ca crls** コマンドをグローバル コンフィギュレーション モードで使用します。

clear crypto ca crls [*trustpointname*]

シンタックスの説明

trustpointname	（オプション）トラストポイントの名前。名前を指定しない場合、このコマンドはシステム上のキャッシュされた CRL をすべて消去します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで発行した次の例では、セキュリティ アプライアンスのすべての CRL からすべての CRL キャッシュを削除します。

```
hostname(config)# clear crypto ca crls
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ca crl request	トラストポイントの CRL コンフィギュレーションに基づいて CRL をダウンロードします。
show crypto ca crls	キャッシュされたすべての CRL または指定したトラストポイントのキャッシュされた CRL を表示します。

clear [crypto] ipsec sa

IPSec SA のカウンタ、エントリ、暗号マップ、またはピア接続を削除するには、**clear [crypto] ipsec sa** コマンドをグローバル コンフィギュレーション モードで使用します。すべての IPSec SA を消去するには、このコマンドを引数なしで使用します。

clear [crypto] ipsec sa [counters | entry {*hostname* | *IP address*} **{esp | ah}** {*SPI*}**| map** {*map name*} **| peer** {*hostname* | *IP address*}**]**

このコマンドは、慎重に使用してください。

シンタックスの説明

ah	認証ヘッダー。
counters	各 SA 統計情報のすべての IPSec を消去します。
entry	指定した IP アドレス、ホスト名、プロトコル、および SPI 値に一致するトンネルを削除します。
esp	暗号化セキュリティ プロトコル。
hostname	IP アドレスに割り当てられたホスト名を指定します。
IP address	IP アドレスを指定します。
map	マップ名で識別される指定した暗号マップに関連付けられたすべてのトンネルを削除します。
map name	暗号マップを識別する英数字の文字列。最大 64 文字です。
peer	指定したホスト名または IP アドレスによって識別されたピアへのすべての IPSec SA を削除します。
SPI	セキュリティ パラメータ インデックス（16 進数）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。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで発行した次の例では、セキュリティ アプライアンスからすべての IPSec SA を削除します。

```
hostname(config)# clear ipsec sa
hostname(config)#
```

グローバル コンフィギュレーション モードで発行した次の例では、10.86.1.1 のピア IP アドレスを持つ SA を削除します。

```
hostname(config)# clear ipsec peer 10.86.1.1
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべてのまたは指定した暗号マップをコンフィギュレーションから消去します。
clear configure isakmp	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
show ipsec sa	カウンタ、エントリ、マップ名、ピア IP アドレス、ホスト名などの IPSec SA に関する情報を表示します。
show running-config crypto	IPSec、暗号マップ、ダイナミック暗号マップ、ISAKMP など、暗号コンフィギュレーション全体を表示します。

clear crypto protocol statistics

暗号アクセラレータ MIB 内のプロトコル固有の統計情報を消去するには、**clear crypto protocol statistics** コマンドをグローバル コンフィギュレーション モードまたは特権 EXEC モードで使用します。

clear crypto protocol statistics *protocol*

シンタックスの説明

protocol	統計情報を消去するプロトコルの名前を指定します。指定できるプロトコルは、次のとおりです。 ***ikev1***：Internet Key Exchange バージョン 1。 ***ipsec***：IP セキュリティ フェーズ 2 プロトコル。 ***ssl***：Secure Socket Layer。 ***other***：新しいプロトコル用に予約されます。 ***all***：現在サポートされているすべてのプロトコル。 このコマンドのオンライン ヘルプでは、今後のリリースでサポートされる他のプロトコルが表示される場合があります。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで入力した次の例では、暗号アクセラレータの統計情報をすべて消去します。

```
hostname(config)# clear crypto protocol statistics all
hostname(config)#
```

関連コマンド

コマンド	説明
clear crypto accelerator statistics	暗号アクセラレータ MIB 内のグローバルな統計情報およびアクセラレータ固有の統計情報を消去します。
show crypto accelerator statistics	暗号アクセラレータ MIB 内のグローバルな統計情報およびアクセラレータ固有の統計情報を表示します。
show crypto protocol statistics	暗号アクセラレータ MIB 内のプロトコル固有の統計情報を表示します。

clear dhcpd

DHCP サーバのバインディングおよび統計情報を消去するには、**clear dhcp** コマンドを使用します。

clear dhcpd {***binding*** [*IP_address*] | ***statistics***}

シンタックスの説明

binding	すべてのクライアント アドレスのバインディングを消去します。
IP_address	指定した IP アドレスのバインディングを消去します。
statistics	統計情報カウンタをクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

clear dhcpd binding コマンドに任意の IP アドレスを含めた場合、その IP アドレスのバインディングだけが消去されます。

すべての DHCP サーバ コマンドを消去するには、**clear configure dhcpd** コマンドを使用します。

例

次の例では、**dhcpd** 統計情報を消去する方法を示します。

```
hostname(config)# clear dhcpd statistics
```

関連コマンド

コマンド	説明
clear configure dhcpd	DHCP サーバの設定をすべて削除します。
show dhcpd	DHCP のバインディング、統計情報、または状態情報を表示します。

clear dhcprelay statistics

DHCP リレー統計情報カウンタをクリアするには、**clear dhcprelay statistics** コマンドを特権 EXEC モードで使用します。

clear dhcprelay ***statistics***

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトの動作や値はありません。

コマンドのモード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン　**clear dhcprelay statistics** コマンドは、DHCP リレー統計情報カウンタだけをクリアします。DHCP リレー コンフィギュレーション全体を消去するには、**clear configure dhcprelay** コマンドを使用します。

例　次の例では、DHCP リレー統計情報を消去する方法を示します。

```
hostname# clear dhcprelay statistics
hostname#
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
debug dhcprelay	DHCP リレー エージェントに関するデバッグ情報を表示します。
show dhcprelay statistics	DHCP リレー エージェントの統計情報を表示します。
show running-config dhcprelay	現在の DHCP リレー エージェント コンフィギュレーションを表示します。

clear dns-hosts cache

DNS キャッシュを消去するには、**clear dns-hosts cache** コマンドを特権 EXEC モードで使用します。このコマンドは、**name** コマンドで追加したスタティック エントリを消去しません。

clear dns-hosts cache

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、DNS キャッシュを消去します。

```
hostname# clear dns-hosts cache
```

関連コマンド

コマンド	説明
dns domain-lookup	セキュリティ アプライアンスがネーム ルックアップを実行できるようにします。
dns name-server	DNS サーバのアドレスを設定します。
dns retries	セキュリティ アプライアンスが応答を受け取らなかった場合に、DNS サーバのリストを再試行する回数を指定します。
dns timeout	次の DNS サーバを試すまでに待つ時間を指定します。
show dns-hosts	DNS キャッシュを表示します。

clear failover statistics

フェールオーバー統計情報カウンタをクリアするには、**clear failover statistics** コマンドを特権 EXEC モードで使用します。

clear failover statistics

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更
既存	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、**show failover statistics** コマンドで表示される統計情報および **show failover** コマンド出力の Stateful Failover Logical Update Statistics セクションのカウンタを消去します。フェールオーバー コンフィギュレーションを削除するには、**clear configure failover** コマンドを使用します。

例

次の例では、フェールオーバー統計情報カウンタをクリアする方法を示します。

```
hostname# clear failover statistics
hostname#
```

関連コマンド

コマンド	説明
debug fover	フェールオーバーのデバッグ情報を表示します。
show failover	フェールオーバー コンフィギュレーションに関する情報および動作統計情報を表示します。

clear fragment

IP フラグメント再構成モジュールの運用データを消去するには、***clear fragment*** コマンドを特権 EXEC モードで入力します。このコマンドは、現在キューに入っている再組み立てを待っているフラグメント（***queue*** キーワードが入力されている場合）またはすべての IP フラグメント再構成統計情報（***statistics*** キーワードが入力されている場合）のいずれかを消去します。統計情報は、再組み立てに成功したフラグメント チェーンの数、再組み立てに失敗したチェーンの数、および最大サイズの超過によってバッファのオーバーフローが発生した回数を示すカウンタです。

clear fragment {**queue** | **statistics**} [*interface*]

シンタックスの説明

interface	（オプション）セキュリティ アプライアンスのインターフェイスを指定します。
queue	IP フラグメント再構成キューを消去します。
statistics	IP フラグメント再構成統計情報を消去します。

デフォルト

interface が指定されていない場合、このコマンドはすべてのインターフェイスに適用されます。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更
7.0(1)	このコマンドは、運用データの消去とコンフィギュレーション データの消去を区別するため、***clear fragment*** と ***clear configure fragment*** の 2 つのコマンドに分けられました。

例

次の例では、IP フラグメント再構成モジュールの運用データを消去する方法を示します。

```
hostname# clear fragment queue
```

関連コマンド

コマンド	説明
clear configure fragment	IP フラグメント再構成コンフィギュレーションを消去し、デフォルトにリセットします。
fragment	特別なパケット フラグメント化の管理を提供して、NFS との互換性を改善します。
show fragment	IP フラグメント再構成モジュールの運用データを表示します。
show running-config fragment	IP フラグメント再構成コンフィギュレーションを表示します。

clear gc

ガーベッジ コレクション プロセスの統計情報を削除するには、**clear gc** コマンドを特権 EXEC モードで使用します。

clear gc

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、ガーベッジ コレクション プロセスの統計情報を削除する方法を示します。

```
hostname# clear gc
```

関連コマンド

コマンド	説明
show gc	ガーベッジ コレクション プロセスの統計情報を表示します。

clear igmp counters

すべての IGMP カウンタをクリアするには、**clear igmp counters** コマンドを特権 EXEC モードで使用します。

clear igmp counters [*if_name*]

シンタックスの説明

if_name	**nameif** コマンドで指定されたインターフェイスの名前。このコマンドにインターフェイスの名前を含めると、指定したインターフェイスのカウンタだけがクリアされます。

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、IGMP 統計情報カウンタをクリアします。

```
hostname# clear igmp counters
```

関連コマンド

コマンド	説明
clear igmp group	検出されたグループを IGMP グループ キャッシュから消去します。
clear igmp traffic	IGMP トラフィック カウンタをクリアします。

clear igmp group

IGMP グループ キャッシュから検出されたグループを消去するには、**clear igmp** コマンドを特権 EXEC モードで使用します。

clear igmp group [*group* | ***interface*** *name*]

シンタックスの説明

group	IGMP グループ アドレス。キャッシュから指定したグループを削除する特定のグループを指定します。
interface *name*	**namif** コマンドで指定されたインターフェイスの名前。指定した場合は、インターフェイスに関連付けられたすべてのグループが削除されます。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

グループまたはインターフェイスを指定しない場合は、すべてのインターフェイスからすべてのグループが消去されます。グループを指定した場合は、そのグループのエントリだけが消去されます。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のすべてのグループが消去されます。グループとインターフェイスの両方を指定した場合は、指定したインターフェイスの指定したグループだけが消去されます。

このコマンドはスタティックに設定されたグループを消去しません。

例

次の例では、IGMP グループ キャッシュから検出されたすべての IGMP グループを消去する方法を示します。

```
hostname# clear igmp
```

関連コマンド

コマンド	説明
clear igmp counters	すべての IGMP カウンタをクリアします。
clear igmp traffic	IGMP トラフィック カウンタをクリアします。

clear igmp traffic

IGMP トラフィック カウンタをクリアするには、**clear igmp traffic** コマンドを特権 EXEC モードで使用します。

clear igmp traffic

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、IGMP 統計情報トラフィック カウンタをクリアします。

```
hostname# clear igmp traffic
```

関連コマンド

コマンド	説明
clear igmp group	検出されたグループを IGMP グループ キャッシュから消去します。
clear igmp counters	すべての IGMP カウンタをクリアします。

clear interface

インターフェイス統計情報を消去するには、**clear interface** コマンドを特権 EXEC モードで使用します。

clear interface [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*]

シンタックスの説明

interface_name	（オプション）**nameif** コマンドで設定したインターフェイス名を指定します。
mapped_name	（オプション）マルチ コンテキスト モードで、マッピング名を **allocate-interface** コマンドを使用して割り当てた場合、その名前を指定します。
physical_interface	（オプション）インターフェイス ID（***gigabit*ethernet0/1** など）を指定します。使用できる値については、**interface** コマンドを参照してください。
subinterface	（オプション）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。

デフォルト

デフォルトでは、このコマンドはすべてのインターフェイス統計情報を消去します。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

clear interface コマンドは、入力バイト数以外のインターフェイスの統計情報をすべてクリアします。インターフェイス統計情報の詳細については、**show interface** コマンドを参照してください。

インターフェイスがコンテキスト間で共有されている場合にコンテキスト内でこのコマンドを入力すると、セキュリティ アプライアンスは現在のコンテキストの統計情報だけを消去します。システム実行スペースでこのコマンドを入力した場合、セキュリティ アプライアンスは結合された統計情報を消去します。

インターフェイス名をシステム実行スペースで使用することはできません。これは、**nameif** コマンドはコンテキスト内でのみ使用できるためです。同様に、**allocate-interface** コマンドを使用してインターフェイス ID をマッピング名にマッピングした場合、そのマッピング名はコンテキスト内でのみ使用できます。

例

次の例では、インターフェイス統計情報をすべて消去します。

```
hostname# clear interface
```

関連コマンド

コマンド	説明
clear configure interface	インターフェイス コンフィギュレーションを消去します。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
show interface	インターフェイスのランタイム ステータスと統計情報を表示します。
show running-config interface	インターフェイスのコンフィギュレーションを表示します。

clear ip audit count

監査ポリシーの一致するシグニチャ数を消去するには、**clear ip audit count** コマンドを特権 EXEC モードで使用します。

clear ip audit count [**global** | **interface** *interface_name*]

シンタックスの説明

global	（デフォルト）すべてのインターフェイスの一致する数を消去します。
interface interface_name	（オプション）指定したインターフェイスの一致する数を消去します。

デフォルト

キーワードを指定しない場合、このコマンドはすべてのインターフェイスの一致を消去します（***global***）。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

例

次の例では、すべてのインターフェイスの数を消去します。

```
hostname# clear ip audit count
```

関連コマンド

コマンド	説明
ip audit interface	インターフェイスに監査ポリシーを割り当てます。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
show ip audit count	監査ポリシーの一致するシグニチャの数を表示します。
show running-config ip audit attack	**ip audit attack** コマンドのコンフィギュレーションを表示します。

clear ip verify statistics

Unicast RPF 統計情報を消去するには、**clear ip verify statistics** コマンドを特権 EXEC モードで使用します。Unicast RPF をイネーブルにするには、**ip verify reverse-path** コマンドを参照してください。

clear ip verify statistics [**interface** *interface_name*]

シンタックスの説明

interface *interface_name*	Unicast RPF 統計情報を消去するインターフェイスを設定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

例

次の例では、Unicast RPF 統計情報を消去します。

```
hostname# clear ip verify statistics
```

関連コマンド

コマンド	説明
clear configure ip verify reverse-path	**ip verify reverse-path** コンフィギュレーションを消去します。
ip verify reverse-path	Unicast Reverse Path Forwarding 機能をイネーブルにして IP スプーフィングを防止します。
show ip verify statistics	Unicast RPF の統計情報を表示します。
show running-config ip verify reverse-path	**ip verify reverse-path** コンフィギュレーションを表示します。

clear ipsec sa

IPSec SA を完全に消去、または指定したパラメータに基づいて消去するには、**clear ipsec sa** コマンドをグローバル コンフィギュレーション モードおよび特権 EXEC モードで使用します。代替の形式 **clear crypto ipsec sa** も使用できます。

clear ipsec sa [***counters*** | **entry** *peer-addr protocol spi* | **peer** *peer-addr* | **map** *map-name*]

シンタックスの説明

counters	（オプション）すべてのカウンタをクリアします。
entry	（オプション）指定した IPSec ピア、プロトコル、および SPI の IPSec SA を消去します。
map *map-name*	（オプション）指定した暗号マップの IPSec SA を消去します。
peer	（オプション）指定したピアの IPSec SA を消去します。
peer-addr	IPSec ピアの IP アドレスを指定します。
protocol	IPSec プロトコル ***esp*** または **ah** を指定します。
spi	IPSec SPI 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。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

例

グローバル コンフィギュレーション モードで入力した次の例では、すべての IPSec SA カウンタをクリアします。

```
hostname(config)# clear ipsec sa counters
hostname(config)#
```

関連コマンド

コマンド	説明
show ipsec sa	指定したパラメータに基づいて IPSec SA を表示します。
show ipsec stats	IPSec フロー MIB からのグローバル IPSec 統計情報を表示します。

clear ipv6 access-list counters

IPv6 アクセスリスト統計情報カウンタをクリアするには、**clear ipv6 access-list counters** コマンドを特権 EXEC モードで使用します。

clear ipv6 access-list *id* ***counters***

シンタックスの説明

id	IPv6 アクセスリストの識別子。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、IPv6 アクセスリスト 2 の統計情報データを消去する方法を示します。

```
hostname# clear ipv6 access-list 2 counters
hostname#
```

関連コマンド

コマンド	説明
clear configure ipv6	現在のコンフィギュレーションから **ipv6 access-list** コマンドを消去します。
ipv6 access-list	IPv6 アクセスリストを設定します。
show ipv6 access-list	現在のコンフィギュレーションにある **ipv6 access-list** コマンドを表示します。

clear ipv6 neighbors

IPv6 近隣探索キャッシュを消去するには、**clear ipv6 neighbors** コマンドを特権 EXEC モードで使用します。

clear ipv6 neighbors

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、検出されたすべての IPv6 近隣をキャッシュから削除します。スタティック エントリは削除しません。

例

次の例では、スタティック エントリを除く、IPv6 近隣探索キャッシュ内のすべてのエントリを削除します。

```
hostname# clear ipv6 neighbors
hostname#
```

関連コマンド

コマンド	説明
ipv6 neighbor	IPv6 探索キャッシュにスタティック エントリを設定します。
show ipv6 neighbor	IPv6 近隣 キャッシュ情報を表示します。

clear ipv6 traffic

IPv6 トラフィック カウンタをリセットするには、**clear ipv6 traffic** コマンドを特権 EXEC モードで使用します。

clear ipv6 traffic

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトの動作や値はありません。

コマンドのモード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン　このコマンドを使用すると、show ipv6 traffic コマンドからの出力のカウンタがリセットされます。

例

次の例では、IPv6 トラフィック カウンタをリセットします。**ipv6 traffic** コマンドからの出力は、カウンタがリセットされることを示します。

```
hostname# clear ipv6 traffic
hostname# show ipv6 traffic
IPv6 statistics:
  Rcvd:  1 total, 1 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  1 generated, 0 forwarded
         0 fragmented into 0 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
  Mcast: 0 received, 0 sent

ICMP statistics:
  Rcvd: 1 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 1 neighbor advert
  Sent: 1 output
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 1 neighbor advert

UDP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 0 output

TCP statistics:
  Rcvd: 0 input, 0 checksum errors
  Sent: 0 output, 0 retransmitted
```

関連コマンド

コマンド	説明
show ipv6 traffic	IPv6 トラフィックの統計情報を表示します。

clear isakmp sa

すべての IKE ランタイム SA データベースを削除するには、**clear isakmp sa** コマンドをグローバル コンフィギュレーション モードまたは特権 EXEC モードで使用します。

clear isakmp sa

シンタックスの説明

このコマンドには、キーワードも引数もありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•		•		
特権 EXEC	•		•		

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、コンフィギュレーションから IKE ランタイム SA データベースを削除します。

```
hostname<config># clear isakmp sa
hostname<config>#
```

関連コマンド

コマンド	説明
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show isakmp stats	実行時の統計情報を表示します。
show isakmp sa	追加情報を含め、IKE ランタイム SA データベースを表示します。
show running-config isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

clear local-host

show local-host コマンドを入力することによって表示されるローカル ホストからネットワーク接続を解放するには、**clear local-host** コマンドを特権 EXEC モードで使用します。

clear local-host [*ip_address*] [**all**]

シンタックスの説明

all	（オプション）セキュリティ アプライアンスへの接続およびセキュリティ アプライアンスからの接続を含むローカル ホスト状態のホストが作成した接続を消去することを指定します。
ip_address	（オプション）ローカル ホストの IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

clear local-host コマンドは、クリアされたホストをライセンス制限から除外します。ライセンス制限にカウントされているホストの数は、**show local-host** コマンドを入力して表示できます。

注意　ローカル ホストのネットワーク状態をクリアすると、ローカル ホストに関連するネットワーク接続と xlate がすべて停止します。

例

次の例では、**clear local-host** コマンドでローカル ホストに関する情報を消去する方法を示します。

```
hostname# clear local-host 10.1.1.15
```

情報がクリアされると、ホストが接続を再び確立するまで、何も表示されません。

関連コマンド

コマンド	説明
show local-host	ローカル ホストのネットワーク状態を表示します。

clear logging asdm

ASDM ロギング バッファを消去するには、**clear logging asdm** コマンドを特権 EXEC モードで使用します。

clear logging asdm

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更
7.0(1)	このコマンドが、**show pdm logging** コマンドから **show asdm log** コマンドに変更されました。

使用上のガイドライン

ASDM syslog メッセージは、セキュリティ アプライアンス syslog メッセージとは別のバッファに保存されます。ASDM ロギング バッファを消去すると、ASDM syslog メッセージだけが消去されます。セキュリティ アプライアンスのシステム メッセージは消去されません。ASDM syslog メッセージを表示するには、**show asdm log** コマンドを使用します。

例

次の例では、ASDM ロギング バッファを消去します。

```
hostname(config)# clear logging asdm
hostname(config)#
```

関連コマンド

コマンド	説明
show asdm log_sessions	ASDM ロギング バッファの内容を表示します。

clear logging buffer

ロギング バッファを消去するには、**clear logging buffer** コマンドをグローバル コンフィギュレーション モードで使用します。

clear logging buffer

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

このコマンドにデフォルト設定はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更
7.0(1)	セキュリティ アプライアンスでこのコマンドがサポートされるようになりました。

例

この例は、SNMP サーバをディセーブルにする方法を示しています。

```
hostname #clear logging buffer
```

関連コマンド

コマンド	説明
logging buffered	ロギングを設定します。
show logging	ロギング情報を表示します。

clear mac-address-table

ダイナミック MAC アドレス テーブル エントリを消去するには、**clear mac-address-table** コマンドを特権 EXEC モードで使用します。

clear mac-address-table [*interface_name*]

シンタックスの説明

interface_name	（オプション）選択したインターフェイスの MAC アドレス テーブル エントリを消去します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	—	•	•	•	—

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、ダイナミック MAC アドレス テーブル エントリを消去します。

```
hostname# clear mac-address-table
```

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。
firewall transparent	ファイアウォール モードを透過に設定します。
mac-address-table aging-time	ダイナミック MAC アドレス エントリのタイムアウトを設定します。
mac-learn	MAC アドレス ラーニングをディセーブルにします。
show mac-address-table	MAC アドレス テーブルのエントリを表示します。

clear memory profile

メモリ プロファイリング機能によって保持されるメモリ バッファを消去するには、***clear memory profile*** コマンドを特権 EXEC コンフィギュレーション モードで使用します。

clear memory profile [peak]

シンタックスの説明

peak	（オプション）ピーク メモリ バッファの内容を消去します。

デフォルト

デフォルトで現在「使用されている」プロファイル バッファを消去します。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	•	•

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear memory profile コマンドはプロファイリング機能によって保持されるメモリ バッファを解放するため、消去する前にプロファイリングを停止する必要があります。

例

次の例では、プロファイリング機能によって保持されるメモリ バッファを消去します。

```
hostname# clear memory profile
```

関連コマンド

コマンド	説明
memory profile enable	メモリ使用状況のモニタリング（メモリ プロファイリング）をイネーブルにします。
memory profile text	プロファイルするメモリのテキスト範囲を設定します。
show memory profile	セキュリティ アプライアンスのメモリ使用状況に関する情報（プロファイリング）を表示します。

clear mfib counters

MFIB ルータ パケット カウンタをクリアするには、**clear mfib counters** コマンドを特権 EXEC モードで使用します。

clear mfib counters [*group* [*source*]]

シンタックスの説明

group	（オプション）マルチキャスト グループの IP アドレス。
source	（オプション）マルチキャスト ルート送信元の IP アドレス。これは、4 分割ドット 10 進表記のユニキャスト IP アドレスです。

デフォルト

このコマンドを引数なしで使用した場合、すべてのルートのルート カウンタがクリアされます。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、すべての MFIB ルート カウンタをクリアします。

```
hostname# clear mfib route counters
```

関連コマンド

コマンド	説明
show mfib count	MFIB ルートおよびパケット カウントのデータを表示します。

clear module recover

hw-module module recover コマンドで設定された AIP SSM のリカバリ ネットワーク設定を消去するには、**clear module recover** コマンドを特権 EXEC モードで使用します。

clear module 1 recover

シンタックスの説明

1	スロット番号を指定します。これは、常に 1 です。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、AIP SSM のリカバリ設定を消去します。

```
hostname# clear module 1 recover
```

関連コマンド

コマンド	説明
hw-module module recover	TFTP サーバからリカバリ イメージをロードすることにより、AIP SSM を回復します。
hw-module module reset	SSM をシャットダウンし、ハードウェア リセットを実行します。
hw-module module reload	AIP SSM ソフトウェアをリロードします。
hw-module module shutdown	コンフィギュレーション データを失わずに電源を切るため、SSM ソフトウェアをシャットダウンします。
show module	SSM 情報を表示します。

clear ospf

OSPF プロセス情報を消去するには、**clear ospf** コマンドを特権 EXEC モードで使用します。

clear ospf [*pid*] {***process*** | ***counters*** [***neighbor*** [*neighbor-intf*] [*neighbr-id*]]}

シンタックスの説明

counters	OSPF カウンタをクリアします。
neighbor	OSPF 隣接カウンタをクリアします。
neighbor-intf	（オプション）OSPF インターフェイス ルータ指定を消去します。
neighbr-id	（オプション）OSPF 隣接ルータ ID を消去します。
pid	（オプション）OSPF ルーティング プロセス用に内部的に使用される ID パラメータ。有効値は、1 ～ 65535 です。
process	OSPF ルーティング プロセスを消去します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

このコマンドはコンフィギュレーションのいずれの部分も削除しません。コンフィギュレーションから特定のコマンドを消去するには、コンフィギュレーション コマンドの **no** 形式を使用します。または、コンフィギュレーションからすべてのグローバル OSPF コマンドを削除するには、**clear configure router ospf** コマンドを使用します。

（注）　**clear configure router ospf** コマンドは、インターフェイス コンフィギュレーション モードで入力された OSPF コマンドを消去しません。

例

次の例では、OSPF プロセス カウンタをクリアする方法を示します。

```
hostname# clear ospf process
```

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グローバル ルータ コマンドを消去します。

clear pim counters

PIM のカウンタおよび統計情報を消去するには、**clear pim counters** コマンドを特権 EXEC モードで使用します。

clear pim counters

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、PIM の統計情報およびカウンタをすべてクリアします。

```
hostname# clear pim counters
```

関連コマンド

コマンド	説明
clear pim reset	リセットによって MRIB の同期化を強制します。
clear pim topology	PIM トポロジ テーブルをクリアします。
clear pim traffic	PIM トラフィック カウンタをクリアします。

clear pim reset

リセットによって MRIB の同期化を強制するには、**clear pim reset** コマンドを特権 EXEC モードで使用します。

clear pim reset

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

トポロジ テーブルからのすべての情報が消去され、MRIB 接続がリセットされます。このコマンドは、PIM トポロジ テーブルと MRIB データベース間の状態を同期化するために使用できます。

例

次の例では、トポロジ テーブルを消去し、MRIB 接続をリセットします。

```
hostname# clear pim reset
```

関連コマンド

コマンド	説明
clear pim counters	PIM のカウンタおよび統計情報をクリアします。
clear pim topology	PIM トポロジ テーブルをクリアします。
clear pim counters	PIM トラフィック カウンタをクリアします。

clear pim topology

PIM トポロジ テーブルを消去するには、**clear pim topology** コマンドを特権 EXEC モードで使用します。

clear pim topology [*group*]

シンタックスの説明

group	（オプション）トポロジ テーブルから削除するマルチキャスト グループのアドレスまたは名前を指定します。

デフォルト

任意の *group* 引数を指定しない場合、トポロジ テーブルからすべてのエントリが消去されます。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、PIM トポロジ テーブルから既存の PIM ルートを消去します。IGMP ローカル メンバーシップなど、MRIB テーブルから取得した情報は保持されます。マルチキャスト グループを指定した場合は、それらのグループ エントリだけが消去されます。

例

次の例では、PIM トポロジ テーブルを消去します。

```
hostname# clear pim topology
```

関連コマンド

コマンド	説明
clear pim counters	PIM のカウンタおよび統計情報をクリアします。
clear pim reset	リセットによって MRIB の同期化を強制します。
clear pim counters	PIM トラフィック カウンタをクリアします。

clear priority-queue statistics

インターフェイスまたは設定されたすべてのインターフェイスのプライオリティキュー統計情報カウンタをクリアするには、**clear priority-queue statistics** コマンドをグローバル コンフィギュレーション モードまたは特権 EXEC モードで使用します。

clear priority-queue statistics [*interface-name*]

シンタックスの説明

interface-name	（オプション）ベストエフォート キューおよび低遅延キューの詳細を表示するインターフェイスの名前を指定します。

デフォルト

インターフェイス名を省略した場合、このコマンドは設定されたすべてのインターフェイスのプライオリティキュー統計情報を消去します。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、**clear priority-queue statistics** コマンドを特権 EXEC モードで使用して、「test」という名前のインターフェイスのプライオリティキュー統計情報を削除します。

```
hostname# clear priority-queue statistics test
hostname#
```

関連コマンド

コマンド	説明
clear configure priority-queue	指定したインターフェイスからプライオリティキュー コンフィギュレーションを削除します。
priority-queue	インターフェイスにプライオリティ キューイングを設定します。
show priority-queue statistics	指定したインターフェイスまたはすべてのインターフェイスのプライオリティキュー統計情報を表示します。
show running-config priority-queue	指定したインターフェイスの現在のプライオリティキュー コンフィギュレーションを表示します。

clear resource usage

リソース使用状況の統計情報を消去するには、**clear resource usage** コマンドを特権 EXEC モードで使用します。

clear resource usage [**context** *context_name* | **all** | **summary**] [**resource** {*resource_name* | **all**}]

シンタックスの説明

context *context_name*	（マルチ モードのみ）統計情報を消去するコンテキスト名を指定します。すべてのコンテキストの場合は、**all** を指定します。
resource *resource_name*	特定のリソースの使用状況を消去します。すべてのリソースの場合は、***all***（デフォルト）を指定します。リソースには、次のタイプがあります。 • **conns**：1 つのホストと複数の他のホスト間の接続を含む 2 つのホスト間の TCP または UDP 接続。 • **hosts**：セキュリティ アプライアンス経由で接続できるホスト。 • **ipsec**：（シングルモードのみ）IPSec セッション。 • **ssh**：SSH セッション。 • **telnet**：Telnet セッション。 • **xlates**：NAT 変換。
summary	（マルチ モードのみ）結合されたコンテキスト統計情報を消去します。

デフォルト

マルチ コンテキスト モードの場合、デフォルトのコンテキストは **all** です。これを指定することにより、すべてのコンテキストのリソース使用状況が消去されます。シングルモードの場合、コンテキスト名は無視され、すべてのリソース統計情報が消去されます。

デフォルトのリソース名は **all** で、すべてのリソース タイプが消去されます。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、リソース使用状況の統計情報をすべて消去します。

```
hostname# clear resource usage
```

関連コマンド

コマンド	説明
context	セキュリティ コンテキストを追加します。
show resource types	リソース タイプのリストを表示します。
show resource usage	セキュリティ アプライアンスのリソース使用状況を表示します。

clear route

コンフィギュレーションからダイナミックにラーニングされたルートを削除するには、**clear route** コマンドを特権 EXEC モードで使用します。

clear route [*interface_name*]

シンタックスの説明

interface_name	（オプション）内部または外部のネットワーク インターフェイス名。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

例

次の例では、ダイナミックにラーニングされたルートを削除する方法を示します。

```
hostname# clear route
```

関連コマンド

コマンド	説明
route	インターフェイスのスタティック ルートまたはデフォルト ルートを指定します。
show route	ルート情報を表示します。
show running-config route	設定されているルートを表示します。

clear service-policy

イネーブルになっているポリシーの運用データまたは統計情報（存在する場合）を消去するには、***clear service-policy*** コマンドをグローバル コンフィギュレーション モードで使用します。

clear service-policy [global | interface *intf* **| inspect]**

シンタックスの説明

global	（オプション）グローバル サービス ポリシーの統計情報を消去します。
interface	（オプション）特定のインターフェイスのサービス ポリシーの統計情報を消去します。
intf	***nameif*** コマンドで定義したインターフェイス名。
inspect	検査サービス ポリシーの統計情報を消去します。

デフォルト

デフォルトでは、このコマンドはすべてのイネーブルなサービス ポリシーの統計情報をすべて消去します。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

インターフェイス名が指定されている場合、ポリシーマップはそのインターフェイスだけに適用されます。インターフェイス名は ***nameif*** コマンドで定義され、インターフェイス ポリシーマップはグローバル ポリシーマップを上書きします。1 つのインターフェイスにつき 1 つのポリシーマップだけを適用できます。

グローバル ポリシーは 1 つしか適用できません。

例

次の例では、***clear service-policy*** コマンドのシンタックスを示します。

```
hostname(config)# clear service-policy outside_security_map outside
```

関連コマンド

コマンド	説明
show service-policy	サービス ポリシーを表示します。
show running-config service-policy	実行コンフィギュレーションに設定されているサービス ポリシーを表示します。
clear configure service-policy	サービス ポリシーのコンフィギュレーションを消去します。
service-policy	サービス ポリシーを設定します。

clear service-policy inspect gtp

グローバル GTP 統計情報を消去するには、**clear service-policy inspect gtp** コマンドを特権 EXEC モードで使用します。

clear service-policy inspect gtp {**pdp-context** [**all** | **apn** *ap_name* | **imsi** *IMSI_value* | **ms-addr** *IP_address* | **tid** *tunnel_ID* | **version** *version_num*] | **requests** | **statistics** [**gsn** *IP_address*] }

シンタックスの説明.

all	すべての GTP PDP コンテキストを消去します。
apn	（オプション）指定した APN に基づいて PDP コンテキストを消去します。
ap_name	特定のアクセス ポイント名を指定します。
gsn	（オプション）GPRS ワイヤレス データ ネットワークと他のネットワーク間のインターフェイスである GPRS サポート ノードを指定します。
gtp	（オプション）GTP のサービス ポリシーを消去します。
imsi	（オプション）指定した IMSI に基づいて PDP コンテキストを消去します。
IMSI_value	特定の IMSI を識別する 16 進値。
interface	（オプション）特定のインターフェイスを指定します。
int	情報を消去するインターフェイスを指定します。
IP_address	統計情報を消去する IP アドレス。
ms-addr	（オプション）指定した MS アドレスに基づいて PDP コンテキストを消去します。
pdp-context	（オプション）パケット データ プロトコル コンテキストを指定します。
requests	（オプション）GTP 要求を消去します。
statistics	（オプション）**inspect gtp** コマンドの GTP 統計情報を消去します。
tid	（オプション）指定した TID に基づいて PDP コンテキストを消去します。
tunnel_ID	特定のトンネルを識別する 16 進値。
version	（オプション）GTP バージョンに基づいて PDP コンテキストを消去します。
version_num	PDP コンテキストのバージョンを指定します。有効な範囲は 0 ～ 255 です。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

パケット データ プロトコル コンテキストは、IMSI と NSAPI の組み合せであるトンネル ID によって識別されます。GTP トンネルは、それぞれ別個の GSN ノードにある、2 つの関連する PDP コンテキストによって定義され、トンネル ID によって識別されます。GTP トンネルは、パケットを外部パケット データ ネットワークとモバイル ステーション（MS）ユーザの間で転送するために必要なものです。

例

次の例では、GTP 統計情報を消去します。

```
hostname# clear service-policy inspect gtp statistics
```

関連コマンド

コマンド	説明
debug gtp	GTP 検査に関する詳細情報を表示します。
gtp-map	GTP マップを定義し、GTP マップ コンフィギュレーション モードをイネーブルにします。
inspect gtp	アプリケーション検査用に 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。
show running-config gtp-map	設定されている GTP マップを表示します。

clear shun

現在イネーブルであるすべての排除をディセーブルにして、排除統計情報を消去するには、**clear shun** コマンドを特権 EXEC モードで使用します。

clear shun [*statistics*]

シンタックスの説明

statistics	（オプション）インターフェイス カウンタだけをクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更
1.1(1)	このコマンドが導入されました。

例

次の例では、現在イネーブルであるすべての排除をディセーブルにして、排除統計情報を消去する方法を示します。

```
hostname(config)# clear shun
```

関連コマンド

コマンド	説明
shun	新しい接続を阻止し、既存の接続からのパケットを拒否することによって、攻撃ホストへのダイナミックな応答をイネーブルにします。
show shun	排除情報を表示します。

clear sunrpc-server active

Sun RPC アプリケーション検査によって開けられたピンホールを消去するには、**clear sunrpc-server active** コマンドをグローバル コンフィギュレーション モードで使用します。

clear sunrpc-server active

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

Sun RPC アプリケーション検査によって開けられた、NFS や NIS などのサービス トラフィックがセキュリティ アプライアンスを通過できるようにするピンホールを消去するには、**clear sunrpc-server active** コマンドを使用します。

例

次の例では、Sun RPC サービス テーブルを消去する方法を示します。

```
hostname(config)# clear sunrpc-server
```

関連コマンド

コマンド	説明
clear configure sunrpc-server	セキュリティ アプライアンスから Sun リモート プロセッサ コール サービスを消去します。
inspect sunrpc	Sun RPC アプリケーション検査をイネーブルまたはディセーブルにし、使用されるポートを設定します。
show running-config sunrpc-server	Sun RPC サービスのコンフィギュレーションに関する情報を表示します。
show sunrpc-server active	アクティブな Sun RPC サービスに関する情報を表示します。

clear traffic

送信アクティビティおよび受信アクティビティのカウンタをリセットするには、***clear traffic*** コマンドを特権 EXEC モードで使用します。

clear traffic

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトの動作や値はありません。

コマンドのモード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン　**clear traffic** コマンドは、***show traffic*** コマンドで表示される送信アクティビティおよび受信アクティビティのカウンタをリセットします。このカウンタは、最後に clear traffic コマンドが入力されてから、またはセキュリティ アプライアンスがオンラインになってから、各インターフェイスを通過したパケット数およびバイト数を示します。秒数は、最後にリブートされてからセキュリティ アプライアンスがオンラインである時間を示します。

例　次に、**clear traffic** コマンドの例を示します。

```
hostname# clear traffic
```

関連コマンド

コマンド	説明
show traffic	送信アクティビティおよび受信アクティビティのカウンタを表示します。

clear uauth

1 人のユーザまたはすべてのユーザのすべてのキャッシュされた認証および認可情報を削除するには、**clear uauth** コマンドを特権 EXEC モードで使用します。

clear uauth [*username*]

シンタックスの説明

username	（オプション）削除するユーザ認証情報をユーザ名で指定します。

デフォルト

ユーザ名を省略すると、すべてのユーザの認証および認可情報が削除されます。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

clear uauth コマンドは、1 人のユーザまたはすべてのユーザの AAA 認可および認証キャッシュを削除します。したがって、ユーザは、次回接続を作成するときに強制的に再認証されます。

timeout コマンドと共に使用します。

各ユーザ ホストの IP アドレスには、認可キャッシュが付加されます。ユーザが適切なホストから、キャッシュされたサービスにアクセスしようとすると、セキュリティ アプライアンスはユーザを認可済みであると見なし、すぐに接続を代理処理します。ある Web サイトへのアクセスを一度認可されると、たとえば、イメージを読み込むときに、各イメージごとに認可サーバと通信しません（イメージが同じ IP アドレスからであると想定されます）。このプロセスにより、認可サーバ上でパフォーマンスが大幅に向上し、負荷も大幅に軽減されます。

ユーザ ホストごとにアドレスとサービスのペアを最大 16 個までキャッシュできます。

（注） Xauth をイネーブルにすると、クライアントに割り当てられている IP アドレスのエントリが uauth テーブル（**show uauth** コマンドで表示できます）に追加されます。ただし、Xauth を Easy VPN Remote 機能とともにネットワーク拡張モードで使用すると、ネットワーク間に IPSec トンネルが作成されるため、ファイアウォールの向こう側にいるユーザを 1 つの IP アドレスに関連付けることができません。したがって、Xauth の完了時に uauth エントリが作成されません。AAA 認可またはアカウンティング サービスが必要な場合は、AAA 認証プロキシをイネーブルにして、ファイアウォールの背後のユーザを認証できます。AAA 認証プロキシの詳細については、AAA コマンドを参照してください。

ユーザの接続がアイドルになった後にキャッシュを保持する期間を指定するには、**timeout uauth** コマンドを使用します。すべてのユーザのすべての認可キャッシュを削除するには、**clear uauth** コマンドを使用します。次回接続を作成するときには再認証される必要が生じます。

例

次の例では、ユーザ「Lee」が再認証されるようにする方法を示します。

```
hostname(config)# clear uauth lee
```

関連コマンド

コマンド	説明
aaa authentication	**aaa-server** コマンドで指定されたサーバ上の LOCAL、TACACS+、または RADIUS のユーザ認証をイネーブル化、ディセーブル化、または表示します。
aaa authorization	**aaa-server** コマンドで指定されたサーバ上の TACACS+ または RADIUS のユーザ認可をイネーブル化、ディセーブル化、または表示します。
show uauth	現在のユーザ認証および認可情報を表示します。
timeout	アイドル状態の最大継続時間を設定します。

clear url-block block statistics

ブロック バッファ使用状況カウンタをクリアするには、**clear url-block block statistics** コマンドを特権 EXEC モードで使用します。

clear url-block block statistics

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

clear url-block block statistics コマンドは、`Current number of packets held (global)` カウンタ以外のブロック バッファ使用状況カウンタをクリアします。

例

次の例では、URL ブロック統計情報を消去し、消去後のカウンタの状態を表示します。

```
hostname# clear url-block block statistics
hostname# show url-block block statistics

URL Pending Packet Buffer Stats with max block  0
----------------------------------------------------
Cumulative number of packets held: | 0
Maximum number of packets held (per URL): | 0
Current number of packets held (global): | 38
Packets dropped due to
 | exceeding url-block buffer limit: | 0
 | HTTP server retransmission: | 0
Number of packets released back to client: | 0
```

関連コマンド

コマンド	説明
filter url	トラフィックを URL フィルタリング サーバに誘導します。
show url-block	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-block	Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンド用の N2H2 サーバまたは Websense サーバを指定します。

clear url-cache statistics

コンフィギュレーションから **url-cache** コマンド文を削除するには、**clear url-cache** コマンドを特権 EXEC モードで使用します。

clear url-cache statistics

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

clear url-cache コマンドは、コンフィギュレーションから **url-cache** 統計情報を削除します。

URL キャッシュを使用しても、Websense プロトコル Version 1 の Websense アカウンティング ログはアップデートされません。Websense プロトコル Version 1 を使用している場合は、Websense を実行してログを記録し、Websense アカウンティング情報を表示できるようにします。セキュリティの要求に合致する使用状況プロファイルを取得した後、**| url-cache** コマンドを入力してスループットを向上させます。Websense プロトコル Version 4 および N2H2 URL フィルタリングでは、**url-cache** コマンドの使用時にアカウンティング ログがアップデートされます。

例

次の例では、URL キャッシュ統計情報を消去します。

```
hostname# clear url-cache statistics
```

関連コマンド

コマンド	説明
filter url	トラフィックを URL フィルタリング サーバに誘導します。
show url-cache statistics	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間に Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンド用の N2H2 サーバまたは Websense サーバを指定します。

clear url-server

URL フィルタリング サーバの統計情報を消去するには、**clear url-server** コマンドを特権 EXEC モードで使用します。

clear url-server statistics

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

clear url-server コマンドは、コンフィギュレーションから URL フィルタリング サーバの統計情報を削除します。

例

次の例では、URL サーバの統計情報を消去します。

```
hostname# clear url-server statistics
```

関連コマンド

コマンド	説明
filter url	トラフィックを URL フィルタリング サーバに誘導します。
show url-server	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間に Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンド用の N2H2 サーバまたは Websense サーバを指定します。

clear xlate

現在の変換情報および接続情報を消去するには、**clear xlate** コマンドを特権 EXEC モードで使用します。

clear xlate [***global*** *ip1*[***-***_ip2_] [***netmask*** *mask*]] [***local*** *ip1*[***-***_ip2_] [***netmask*** *mask*]] [***gport*** *port1*[***-***_port2_]] [***lport*** *port1*[***-***_port2_]] [***interface*** *if_name*] [***state*** *state*]

シンタックスの説明

global *ip1*[***-***_ip2_]	（オプション）アクティブな変換をグローバル IP アドレスまたはアドレスの範囲別に消去します。
gport *port1*[***-***_port2_]	（オプション）アクティブな変換をグローバル ポートまたはポートの範囲別に消去します。
interface *if_name*	（オプション）アクティブな変換をインターフェイス別に表示します。
local *ip1*[***-***_ip2_]	（オプション）アクティブな変換をローカル IP アドレスまたはアドレスの範囲別に消去します。
lport *port1*[***-***_port2_]	（オプション）アクティブな変換をローカル ポートまたはポートの範囲別に消去します。
netmask *mask*	（オプション）グローバル IP アドレスまたはローカル IP アドレスを限定するネットワーク マスクを指定します。
state *state*	（オプション）アクティブな変換を状態別に消去します。次の状態を 1 つまたは複数入力できます。 • ***static*** : **スタティック**変換を指定します。 • ***portmap*** : PAT グローバル変換を指定します。 • ***norandomseq*** : ***norandomseq*** 設定での **nat** または**スタティック**変換を指定します。 • ***identity*** : **nat 0** 識別アドレス変換を指定します。 複数の状態を指定する場合は、状態をカンマで区切ります。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

clear xlate コマンドは、変換スロットの内容を消去します（「xlate」は変換スロットを意味します）。変換スロットは、キーの変更後も残ります。コンフィギュレーション内で **aaa-server**、**access-list**、**alias**、**global**、**nat**、**route**、または **static** コマンドを追加、変更、または削除した後には、必ず **clear xlate** コマンドを使用します。

xlate は、NAT または PAT セッションを示します。これらのセッションは、***detail*** オプションの **show xlate** コマンドで表示できます。xlate には、スタティックとダイナミックの 2 種類があります。

スタティック xlate は、**static** コマンドを使用して作成される固定の xlate です。スタティック xlate は、コンフィギュレーションから **static** コマンドを削除することによってのみ削除できます。**clear xlate** は、スタティック変換規則を削除しません。コンフィギュレーションから **static** コマンドを削除しても、スタティック規則を使用する既存の接続はトラフィックを転送できます。これらの接続を無効にするには、**clear local-host** を使用します。

ダイナミック xlate は、**nat** または **global** コマンドを使用して、トラフィック処理によってオンデマンドで作成されます。**clear xlate** は、ダイナミック xlate および関連付けられた接続を削除します。また、**clear local-host** コマンドを使用して、xlate および関連付けられた接続を消去することもできます。コンフィギュレーションから **nat** または **global** コマンドを削除しても、ダイナミック xlate および関連付けられた接続はアクティブのままとなる場合があります。これらの接続を削除するには、**clear xlate** または **clear local-host** コマンドを使用します。

例

次の例では、現在の変換スロット情報および接続スロット情報を消去する方法を示します。

```
hostname# clear xlate global
```

関連コマンド

コマンド	説明
clear local-host	ローカル ホストのネットワーク情報を消去します。
clear uauth	キャッシュされたユーザ認証および認可情報を消去します。
show conn	アクティブな接続をすべて表示します。
show local-host	ローカル ホストのネットワーク情報を表示します。
show xlate	現在の変換情報を表示します。

client-access-rule

リモートアクセス クライアントのタイプを制限する規則およびセキュリティ アプライアンスを通して IPSec 経由で接続できるバージョンを設定するには、**client-access-rule** コマンドをグループポリシー コンフィギュレーション モードで使用します。規則を削除するには、このコマンドの **no** 形式を使用します。

すべての規則を削除するには、**no client-access-rule** コマンドの priority 引数だけを指定して使用します。この指定により、**client-access-rule none** コマンドを入力して作成されたヌル規則を含む、設定されたすべての規則が削除されます。

クライアントのアクセス規則がない場合、ユーザはデフォルトのグループポリシー内に存在するすべての規則を継承します。ユーザがクライアントのアクセス規則を継承しないようにするには、**client-access-rule none** コマンドを使用します。クライアントのアクセス規則を継承しない場合、すべてのクライアント タイプおよびバージョンに接続できます。

client-access-rule *priority* **{permit | deny} type** *type* **version** *version* **| none**

no client-access-rule *priority* [**{permit | deny} type** *type* **version** *version*]

シンタックスの説明

deny	特定のタイプとバージョンの両方またはいずれか一方のデバイスの接続を拒否します。
none	クライアントのアクセス規則を許可しません。client-access-rule をヌル値に設定して、制限を許可しません。デフォルトのグループポリシーまたは指定されているグループポリシーから値を継承しないようにします。
permit	特定のタイプとバージョンの両方またはいずれか一方のデバイスの接続を許可します。
priority	規則の優先順位を決定します。最も小さい整数の規則が、一番高い優先順位となります。したがって、クライアント タイプとバージョンの両方またはいずれか一方に一致する最も小さい整数の規則が、適用される規則です。優先順位の低い規則が矛盾している場合、セキュリティ アプライアンスはその規則を無視します。
type *type*	VPN 3002 などの自由形式の文字列を利用して、デバイス タイプを指定します。* 記号をワイルドカードとして使用できる場合を除き、文字列は **show vpn-sessiondb remote** 表示の外観と完全に一致する必要があります。
version *version*	7.0(1) などの自由形式の文字列を使用して、デバイス バージョンを指定します。* 記号をワイルドカードとして使用できる場合を除き、文字列は **show vpn-sessiondb remote** 表示の外観と完全に一致する必要があります。

デフォルト

デフォルトでは、アクセス規則はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

次の注意に従って規則を作成します。

- 規則を定義しない場合、セキュリティ アプライアンスはすべての接続タイプを許可します。
- クライアントが規則のいずれにも一致しない場合、セキュリティ アプライアンスは接続を拒否します。つまり deny 規則を定義する場合は、少なくとも 1 つの permit 規則も定義する必要があります。permit 規則を定義しないと、セキュリティ アプライアンスはすべての接続を拒否します。
- ソフトウェア クライアントとハードウェア クライアントのどちらも、タイプおよびバージョンが **show vpn-sessiondb remote** 表示の外観と完全に一致する必要があります。
- * 記号はワイルドカードで、各規則内で複数回使用できます。たとえば、**client-access-rule 3 deny type * version 3.*** は、リリース バージョン 3.x ソフトウェアを実行しているすべてのクライアント タイプを拒否する優先順位 3 のクライアントのアクセス規則を作成します。
- 1 つのグループポリシーにつき最大 25 の規則を作成できます。
- 一連の規則全体に 255 文字の制限があります。
- クライアント タイプとバージョンの両方またはいずれか一方を送信しないクライアントに n/a を使用できます。

例

次の例では、FirstGroup という名前のグループポリシーのクライアントのアクセス規則を作成する方法を示します。これらの規則は、ソフトウェア バージョン 4.1 を実行している VPN クライアントを許可する一方、すべての VPN 3002 ハードウェア クライアントを拒否します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-access-rule 1 d t VPN3002 v *
hostname(config-group-policy)# client-access-rule 2 p * v 4.1
```

client-firewall

セキュリティ アプライアンスが IKE トンネル ネゴシエーション中に VPN クライアントにプッシュするパーソナル ファイアウォール ポリシーを設定するには、**client-firewall** コマンドをグループポリシー コンフィギュレーション モードで使用します。ファイアウォール ポリシーを削除するには、このコマンドの **no** 形式を使用します。

ファイアウォール ポリシーがない場合、ユーザはデフォルトまたはその他のグループポリシー内に存在するすべてのファイアウォール ポリシーを継承します。ユーザがそれらのファイアウォール ポリシーを継承しないようにするには、**client-firewall none** コマンドを使用します。

client-firewall none

client-firewall opt | req custom vendor-id *num* product-id *num* policy AYT | {CPP acl-in *ACL* acl-out *ACL*} [description *string*]

client-firewall opt | req zonelabs-zonealarm policy AYT | {CPP acl-in *ACL* acl-out *ACL*}

client-firewall opt | req zonelabs-zonealarmorpro policy AYT | {CPP acl-in *ACL* acl-out *ACL*}

client-firewall opt | req zonelabs-zonealarmpro policy AYT | {CPP acl-in *ACL* acl-out *ACL*}

client-firewall opt | req cisco-integrated acl-in *ACL* **acl-out** *ACL*

client-firewall opt | req sygate-personal

client-firewall opt | req sygate-personal-pro

client-firewall opt | req sygate-security-agent

client-firewall opt | req networkice-blackice

client-firewall opt | req cisco-security-agent

シンタックスの説明

acl-in *<ACL>*	クライアントが着信トラフィックに使用するポリシーを指定します。
acl-out *<ACL>*	クライアントが発信トラフィックに使用するポリシーを指定します。
AYT	クライアント PC のファイアウォール アプリケーションがファイアウォール ポリシーを制御することを指定します。セキュリティ アプライアンスは、ファイアウォールが確実に実行されていることを確認します。「Are You There?」と表示され、応答がない場合、セキュリティ アプライアンスはトンネルを終了します。
cisco-integrated	Cisco Integrated ファイアウォール タイプを指定します。
cisco-security-agent	Cisco Intrusion Prevention Security Agent ファイアウォール タイプを指定します。
CPP	VPN クライアント ファイアウォール ポリシーのソースとしてプッシュされるポリシーを指定します。
custom	Custom ファイアウォール タイプを指定します。
description *<string>*	ファイアウォールについて説明します。
networkice-blackice	Network ICE Black ICE ファイアウォール タイプを指定します。
none	クライアント ファイアウォール ポリシーがないことを指定します。ファイアウォール ポリシーをヌル値に設定して、拒否します。デフォルトのグループポリシーまたは指定されているグループポリシーからファイアウォール ポリシーを継承しないようにします。
opt	オプションのファイアウォール タイプを指定します。
product-id	ファイアウォール製品を指定します。

req	必要なファイアウォール タイプを指定します。
sygate-personal	Sygate Personal ファイアウォール タイプを指定します。
sygate-personal-pro	Sygate Personal Pro ファイアウォール タイプを指定します。
sygate-security-agent	Sygate Security Agent ファイアウォール タイプを指定します。
vendor-id	ファイアウォール ベンダーを指定します。
zonelabs-zonealarm	Zone Labs Zone Alarm ファイアウォール タイプを指定します。
zonelabs-zonealarmorpro policy	Zone Labs Zone Alarm または Pro ファイアウォール タイプを指定します。
zonelabs-zonealarmpro policy	Zone Labs Zone Alarm Pro ファイアウォール タイプを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループポリシー	•	—	•	—	—

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドで設定できるインスタンスは 1 つだけです。

例

次の例では、FirstGroup という名前のグループポリシーの Cisco Intrusion Prevention Security Agent を必要とするクライアント ファイアウォール ポリシーを設定する方法を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-firewall req cisco-security-agent
```

client-update

クライアント アップデート パラメータを設定および変更するには、**client-update** コマンドをトンネルグループ ipsec アトリビュート コンフィギュレーション モードで使用します。クライアントがリビジョン番号のリストにあるソフトウェア バージョンをすでに実行している場合は、ソフトウェアをアップデートする必要はありません。クライアントがリストにあるソフトウェア バージョンを実行していない場合は、アップデートする必要があります。これらのクライアント アップデートのエントリは最大 4 つまで指定できます。

クライアント アップデートをディセーブルにするには、このコマンドの ***no*** 形式を使用します。

client-update type *type* {***url*** *url-string*} {***rev-nums*** *rev-nums*}

no client-update [*type*]

シンタックスの説明

rev-nums *rev-nums*	このクライアントのソフトウェア イメージまたはファームウェア イメージを指定します。カンマ区切りで最大 4 つまで入力できます。
type	クライアント アップデートを通知するオペレーティング システムを指定します。オペレーティング システムのリストには次のものが含まれます。 • Windows：Windows ベースのすべてのプラットフォーム • WIN9X：Windows 95、Windows 98、および Windows ME プラットフォーム • WinNT：Windows NT 4.0、Windows 2000、および Windows XP プラットフォーム • vpn3002：VPN 3002 ハードウェア クライアント
url *url-string*	ソフトウェア イメージまたはファームウェア イメージの URL を指定します。この URL は、このクライアントに応じたファイルを示す必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネルグループ ipsec アトリビュート コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このアトリビュートは、IPSec リモートアクセス トンネルグループ タイプだけに適用できます。

例

config-ipsec コンフィギュレーション モードで入力した次の例では、remotegrp という名前のリモートアクセス トンネルグループのクライアント アップデート パラメータを設定します。リビジョン番号 4.6.1、および更新を取得する URL（https://support/updates）を指定します。

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp ipsec-attributes
hostname(config-ipsec)# client-update type windows url https://support/updates/
rev-nums 4.6.1
hostname(config-ipsec)#
```

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消去します。
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 enable	**crypto ca certificate map** コマンドで作成された証明書マップ エントリをトンネルグループに関連付けます。

clock set

セキュリティ アプライアンスのクロックを手動で設定するには、**clock set** コマンドを特権 EXEC モードで使用します。

clock set *hh:mm:ss* {*month day* | *day month*} *year*

シンタックスの説明

day	1 ～ 31 の日を設定します。たとえば、標準の日付形式に応じて、月日を **april 1** や **1 april** のように入力できます。
hh:mm:ss	時、分、秒を 24 時間形式で設定します。たとえば、午後 8 時 54 分は **20:54:00** のように設定します。
month	月を設定します。標準の日付形式に応じて、月日を **april 1** や **1 april** のように入力できます。
year	4 桁で西暦年を設定します（たとえば、**2004**）。西暦年の範囲は 1993 ～ 2035 です。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

clock コンフィギュレーション コマンドを入力していない場合、**clock set** コマンドのデフォルトの時間帯は UTC です。**clock timezone** コマンドを使用して **clock set** コマンドを入力した後に時間帯を変更した場合、時間は自動的に新しい時間帯に調整されます。ただし、**clock timezone** コマンドを使用して時間帯を確立した後に **clock set** コマンドを入力した場合は、UTC ではなく新しい時間帯に応じた時間を入力します。同様に、**clock set** コマンドの後に **clock summer-time** コマンドを入力した場合、時間は夏時間に調整されます。**clock summer-time** コマンドの後に **clock set** コマンドを入力した場合は、夏時間の正しい時間を入力します。

このコマンドはハードウェア チップ内の時間を設定しますが、コンフィギュレーション ファイル内の時間は保存しません。この時間はリブート後も保持されます。他の **clock** コマンドとは異なり、このコマンドは特権 EXEC コマンドです。クロックをリセットするには、**clock set** コマンドに新しい時間を設定する必要があります。

例

次の例では、時間帯を MST に設定し、夏時間を米国のデフォルト期間に設定し、MDT の現在の時間を西暦 2004 年 7 月 27 日の 午後 1 時 15 分に設定します。

```
hostname(config)# clock timezone MST -7
hostname(config)# clock summer-time MDT recurring
hostname(config)# exit
hostname# clock set 13:15:0 jul 27 2004
hostname# show clock
13:15:00.652 MDT Tue Jul 27 2004
```

次の例では、クロックを UTC 時間帯で西暦 2004 年 7 月 27 日の 8 時 15 分に設定し、次に時間帯を MST に、夏時間を米国のデフォルト期間に設定します。終了時間（MDT の 1 時 15 分）は上記の例と同じです。

```
hostname# clock set 20:15:0 jul 27 2004
hostname# configure terminal
hostname(config)# clock timezone MST -7
hostname(config)# clock summer-time MDT recurring
hostname# show clock
13:15:00.652 MDT Tue Jul 27 2004
```

関連コマンド

コマンド	説明
clock summer-time	夏時間を表示する日付範囲を設定します。
clock timezone	時間帯を設定します。
show clock	現在の時刻を表示します。

clock summer-time

セキュリティ アプライアンスの時間の表示用に夏時間の日付範囲を設定するには、**clock summer-time** コマンドをグローバル コンフィギュレーション モードで使用します。夏時間の日付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。

clock summer-time *zone* ***recurring*** [*week weekday month hh:mm week weekday month hh:mm*] [*offset*]

no clock summer-time [*zone* ***recurring*** [*week weekday month hh:mm week weekday month hh:mm*] [*offset*]]

clock summer-time *zone* ***date*** {*day month* | *month day*} *year hh:mm* {*day month* | *month day*} *year hh:mm* [*offset*]

no clock summer-time [*zone* ***date*** {*day month* | *month day*} *year hh:mm* {*day month* | *month day*} *year hh:mm* [*offset*]]

シンタックスの説明

date	夏時間の開始日と終了日を、特定の年の特定の日付として指定します。このキーワードを使用した場合は、日付を毎年リセットする必要があります。
day	1 ～ 31 の日を設定します。たとえば、標準の日付形式に応じて、月日を **April 1** や **1 April** のように入力できます。
hh:mm	時間と分を 24 時間形式で設定します。
month	月を文字列で設定します。***date*** コマンドでは、たとえば、標準の日付形式に応じて、月日を **April 1** や **1 April** のように入力できます。
offset	（オプション）夏時間の時間を変更する分数を設定します。この値は、デフォルトで 60 分です。
recurring	夏時間の開始日と終了日を、年の特定の日付ではなく、月の日と時間の形式で指定します。このキーワードを使用すると、毎年変更する必要がない定期的な日付範囲を設定できます。日付を指定しない場合、セキュリティ アプライアンスは、米国のデフォルトの日付範囲（4 月の最初の日曜日の午前 2 時～10 月の最後の日曜日の午前 2 時）を使用します。
week	（オプション）週を 1 ～ 4 の整数で、あるいは ***first*** または ***last*** の語で指定します。たとえば、日が 5 週目になった場合は、**last** を指定します。
weekday	（オプション）**Monday**、**Tuesday**、**Wednesday** など、曜日を指定します。
year	4 桁で西暦年を設定します（たとえば、**2004**）。西暦年の範囲は 1993 ～ 2035 です。
zone	たとえば、太平洋夏時間は **PDT** のように、時間帯を文字列で指定します。このコマンドで設定した日付範囲に従ってセキュリティ アプライアンスが夏時間を表示する場合、時間帯はここで設定した値に変更されます。基本の時間帯を UTC 以外の時間帯に設定するには、**clock timezone** を参照してください。

デフォルト

デフォルトのオフセットは 60 分です。

デフォルトの定期的な日付範囲は、4 月の最初の日曜日の午前 2 時から 10 月の最後の日曜日の午前 2 時です。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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	透過	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	•	•	•	—	•

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

南半球の場合、セキュリティ アプライアンスは、たとえば 10 月から 3 月のように、開始月が終了月よりも後に来ることを受け入れます。

例

次の例では、オーストラリアの夏時間の範囲を設定します。

```
hostname(config)# clock summer-time PDT recurring last Sunday October 2:00 last Sunday
March 2:00
```

国によっては、夏時間は特定の日付に開始されます。次の例では、夏時間を西暦 2004 年 4 月 1 日午前 3 時に開始し、西暦 2004 年 10 月 1 日午前 4 時に終了するように設定します。

```
hostname(config)# clock summer-time UTC date 1 April 2004 3:00 1 October 2004 4:00
```

関連コマンド

コマンド	説明
clock set	セキュリティ アプライアンスのクロックを手動で設定します。
clock timezone	時間帯を設定します。
ntp server	NTP サーバを指定します。
show clock	現在の時刻を表示します。

clock timezone

セキュリティ アプライアンスのクロックの時間帯を設定するには、**clock timezone** コマンドをグローバル コンフィギュレーション モードで使用します。時間帯を UTC の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。**clock set** コマンドまたは NTP サーバから生成された時間は、時間を UTC で設定します。このコマンドを使用して、時間帯を UTC のオフセットとして設定する必要があります。

clock timezone *zone* [**-**]*hours* [*minutes*]

no clock timezone [*zone* [**-**]*hours* [*minutes*]]

シンタックスの説明

zone	たとえば、太平洋標準時間は **PST** のように、時間帯を文字列で指定します。
[**-**]*hours*	UTC からのオフセットの時間を設定します。たとえば、PST は **-8** 時間です。
minutes	（オプション）UTC からのオフセットの分数を設定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

夏時間を設定するには、**clock summer-time** コマンドを参照してください。

例

次の例では、時間帯を UTC から -8 時間の太平洋標準時間に設定します。

```
hostname(config)# clock timezone PST -8
```

関連コマンド

コマンド	説明
clock set	セキュリティ アプライアンスのクロックを手動で設定します。
clock summer-time	夏時間を表示する日付範囲を設定します。
ntp server	NTP サーバを指定します。
show clock	現在の時刻を表示します。

cluster encryption

仮想ロードバランシング クラスタ上で交換されるメッセージの暗号化をイネーブルにするには、**cluster encryption** コマンドを VPN ロードバランシング モードで使用します。暗号化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。

cluster encryption

no cluster encryption

（注）　VPN ロードバランシングには、アクティブな 3DES または AES ライセンスが必要です。セキュリティ アプライアンスは、ロードバランシングをイネーブルにする前に、この暗号ライセンスが存在するかどうかをチェックします。有効な 3DES ライセンスまたは AES ライセンスが検出されなかった場合、セキュリティ アプライアンスはロードバランシングをイネーブルにしません。また、ライセンスで許可されていない限り、ロードバランシング システムが 3DES の内部設定を行わないようにします。

シンタックスの説明

このコマンドには、引数も変数もありません。

デフォルト

暗号化は、デフォルトではディセーブルになっています。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
VPN ロードバランシング モード	•	—	•	—	—

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、仮想ロードバランシング クラスタ上で交換されるメッセージの暗号化のオンとオフを切り替えます。

cluster encryption コマンドを設定する前に、まず **vpn load-balancing** コマンドを使用して VPN ロードバランシング モードに入る必要があります。また、クラスタの暗号化をイネーブルにする前に、**cluster key** コマンドを使用してクラスタ共有秘密鍵も設定する必要があります。

（注）　暗号化を使用する場合は、最初にコマンド **isakmp enable** *inside* を設定する必要があります。ここで、*inside* は、ロードバランシングの内部インターフェイスです。ロードバランシングの内部インターフェイスで isakmp がイネーブルでない場合は、クラスタの暗号化を設定しようとすると、エラー メッセージが表示されます。

例

次に、仮想ロードバランシング クラスタの暗号化をイネーブルにする **cluster encryption** コマンドを含む VPN ロードバランシング コマンド シーケンスの例を示します。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
cluster key	クラスタの共有秘密鍵を指定します。
vpn load-balancing	VPN ロードバランシング モードに入ります。

cluster ip address

仮想ロードバランシング クラスタの IP アドレスを設定するには、**cluster ip address** コマンドを VPN ロードバランシング モードで使用します。IP アドレス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。

cluster ip address *ip-address*

no cluster ip address [*ip-address*]

シンタックスの説明

ip-address	仮想ロードバランシング クラスタに割り当てる IP アドレス。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
VPN ロードバランシング モード	•	—	•	—	—

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

まず、**vpn load-balancing** コマンドを使用して VPN ロードバランシング モードに入り、仮想クラスタ IP アドレスが指すインターフェイスを設定する必要があります。

cluster ip address は、仮想クラスタを設定しているインターフェイスと同じサブネット上にある必要があります。

このコマンドの ***no*** 形式では、オプションの *ip-address* 値を指定した場合、その値は **no cluster ip address** コマンドが完了される前に、既存のクラスタの IP アドレスと一致する必要があります。

例

次に、仮想ロードバランシング クラスタの IP アドレスを 209.165.202.224 に設定する **cluster ip address** コマンドを含む VPN ロードバランシング コマンド シーケンスの例を示します。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
interface	デバイスのインターフェイスを設定します。
nameif	インターフェイスに名前を割り当てます。
vpn load-balancing	VPN ロードバランシング モードに入ります。

cluster key

仮想ロードバランシング クラスタ上で交換される IPSec サイトツーサイト トンネルの共有秘密を設定するには、**cluster key** コマンドを VPN ロードバランシング モードで使用します。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。

cluster key *shared-secret*

no cluster key [*shared-secret*]

シンタックスの説明

shared-secret	VPN ロードバランシング クラスタの共有秘密を定義する文字列。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
VPN ロードバランシング モード	•	—	•	—	—

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

まず、**vpn load-balancing** コマンドを使用して、VPN ロードバランシング モードに入る必要があります。クラスタの暗号化には、**cluster key** コマンドで定義されたシークレットも使用されます。

共有秘密を設定するには、クラスタの暗号化をイネーブルにする前に **cluster key** コマンドを使用する必要があります。

このコマンドの **no cluster key** 形式で *shared-secret* の値を指定した場合、共有秘密の値は既存のコンフィギュレーションと一致する必要があります。

例

次に、仮想ロードバランシング クラスタの共有秘密を 123456789 に設定する **cluster key** コマンドを含む VPN ロードバランシング コマンド シーケンスの例を示します。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
vpn load-balancing	VPN ロードバランシング モードに入ります。

cluster port

仮想ロードバランシング クラスタの UDP ポートを設定するには、**cluster port** コマンドを VPN ロードバランシング モードで使用します。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。

cluster port *port*

no cluster port [*port*]

シンタックスの説明

port	仮想ロードバランシング クラスタに割り当てる UDP ポート。

デフォルト

デフォルトのクラスタ ポートは、9023 です。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
VPN ロードバランシング モード	•	—	•	—	—

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

まず、**vpn load-balancing** コマンドを使用して、VPN ロードバランシング モードに入る必要があります。

任意の有効な UDP ポート番号を指定できます。範囲は 1 ～ 65535 です。

このコマンドの **no cluster port** 形式で *port* の値を指定した場合、指定したポート番号は既存の設定済みのポート番号と一致する必要があります。

例

次に、仮想ロードバランシング クラスタの UDP ポートを 9023 に設定する **cluster port address** コマンドを含む VPN ロードバランシング コマンド シーケンスの例を示します。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster port 9023
hostname(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
vpn load-balancing	VPN ロードバランシング モードに入ります。

command-alias

コマンドのエイリアスを作成するには、***command-alias*** コマンドをグローバル コンフィギュレーション モードで使用します。エイリアスを削除するには、このコマンドの **no** 形式を使用します。コマンド エイリアスを入力すると、元のコマンドが実行されます。たとえば、コマンド エイリアスを作成して、長いコマンドのショートカットにすることもできます。

command-alias *mode command_alias original_command*

no command-alias *mode command_alias original_command*

シンタックスの説明

mode	たとえば、**exec**（ユーザおよび特権 EXEC モードの場合）、**configure**、**interface** などの、コマンド エイリアスを作成するコマンド モードを指定します。
command_alias	既存のコマンドに付ける新しい名前を指定します。
original_command	コマンド エイリアスを作成する既存のコマンドまたはキーワードがあるコマンドを指定します。

デフォルト

デフォルトでは、ユーザ EXEC モードで次のエイリアスが設定されています。

h（***help*** のエイリアス）

lo（***logout*** のエイリアス）

p（***ping*** のエイリアス）

s（***show*** のエイリアス）

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

任意のコマンドの最初の部分のエイリアスを作成し、さらに通常どおりキーワードと引数を入力できます。

CLI ヘルプを使用する場合、コマンド エイリアスはアスタリスク（*）で示され、次の形式で表示されます。

```
*command-alias=original-command
```

たとえば、**lo** コマンド エイリアスは、次のように、「lo」で始まる他の特権 EXEC モードのコマンドとともに表示されます。

```
hostname# lo?
*lo=logout login  logout
```

同じエイリアスを別のモードで使用できます。たとえば、次のように、「happy」を特権 EXEC モードとコンフィギュレーション モードで異なるコマンドのエイリアスに使用できます。

```
hostname(config)# happy?

configure mode commands/options:
*happy="username crichton password test"

exec mode commands/options:
*happy=enable
```

コマンドだけを表示し、エイリアスを省略するには、入力行の先頭にスペースを入力します。また、コマンド エイリアスを避けるには、コマンドを入力する前にスペースを使用します。次の例では、happy? コマンドの前にスペースがあるため、エイリアス happy は表示されません。

```
hostname(config)# alias exec test enable
hostname(config)# exit
hostname#   happy?
ERROR: % Unrecognized command
```

コマンドと同様に、CLI ヘルプを使用して、コマンド エイリアスの後に続く引数およびキーワードを表示できます。

完全なコマンド エイリアスを入力する必要があります。短縮されたエイリアスは使用できません。次の例では、パーサーはコマンド hap を、エイリアス happy を示しているとは認識しません。

```
hostname# hap
% Ambiguous command: "hap"
```

例

次の例では、***copy running-config startup-config*** コマンドに対して「***save***」という名前のコマンド エイリアスを作成する方法を示します。

```
hostname(config)# command-alias exec save copy running-config startup-config
hostname(config)# exit
hostname# save

Source filename [running-config]?
Cryptochecksum: 50d131d9 8626c515 0c698f7f 613ae54e

2209 bytes copied in 0.210 secs
hostname#
```

関連コマンド

コマンド	説明
clear configure command-alias	デフォルト以外のコマンド エイリアスをすべて消去します。
show running-config command-alias	デフォルト以外の設定済みのコマンド エイリアスをすべて表示します。

command-queue

応答を待つキューに入る MGCP コマンドの最大数を指定するには、**command-queue** コマンドを MGCP マップ コンフィギュレーション モードで使用します。この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。

command-queue *limit*

no command-queue *limit*

シンタックスの説明

limit	キューに入るコマンドの最大数（1 ～ 2,147,483,647）を指定します。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

MGCP コマンド キューのデフォルトは 200 です。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
MGCP マップ コンフィギュレーション	•	•	•	•	No

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

応答を待つキューに入る MGCP コマンドの最大数を指定するには、**command-queue** コマンドを使用します。許容値の範囲は、1 ～ 4,294,967,295 です。デフォルトは 200 です。限度に到達していて新しいコマンドが着信すると、最も長時間キューに入っているコマンドが削除されます。

例

次の例では、MGCP コマンド キューを 150 コマンドに制限します。

```
hostname(config)# mgcp-map mgcp_policy
hostname(config-mgcp-map)#command-queue 150
```

関連コマンド

コマンド	説明
debug mgcp	MGCP に関するデバッグ情報の表示をイネーブルにします。
mgcp-map	MGCP マップを定義し、MGCP マップ コンフィギュレーション モードをイネーブルにします。
show mgcp	MGCP のコンフィギュレーションおよびセッション情報を表示します。
timeout mgcp	MGCP メディア接続のアイドル タイムアウトを設定します。このタイムアウト後、その MGCP メディア接続が終了します。
timeout mgcp-pat	MGCP PAT xlate のアイドル タイムアウトを設定します。このタイムアウト後、その MGCP PAT xlate が削除されます。

compatible rfc1583

RFC 1583 単位のサマリー ルート コスト計算で使用した方式に戻すには、**compatible rfc1583** コマンドをルータ コンフィギュレーション モードで使用します。RFC 1583 互換性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。

compatible rfc1583

no compatible rfc1583

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

このコマンドは、デフォルトではイネーブルになっています。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

コンフィギュレーションには、このコマンドの **no** 形式だけが表示されます。

例

次の例では、RFC 1583 互換ルート サマリー コスト計算をディセーブルにする方法を示します。

```
hostname(config-router)# no compatible rfc1583
hostname(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 モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

config-register

次にセキュリティ アプライアンスをリロードするときに使用されるコンフィギュレーション レジスタ値を設定するには、**config-register** コマンドをグローバル コンフィギュレーション モードで使用します。値をデフォルトに戻すには、このコマンドの **no** 形式を使用します。このコマンドは、ASA 5500 適応型セキュリティ アプライアンスでのみサポートされています。コンフィギュレーション レジスタ値は、ブート イメージおよび他のブート パラメータを決定します。

config-register *hex_value*

no config-register

シンタックスの説明

hex_value	コンフィギュレーション レジスタ値を 0x0 ～ 0xFFFFFFFF の 16 進数値に設定します。この数は 32 ビットを表し、各 16 進文字は 4 ビットを表します。各ビットは異なる特性を制御します。ただし、ビット 32 ～ 20 は、将来の使用のために予約され、ユーザが設定できないか、または現在セキュリティ アプライアンスで使用されていません。したがって、それらのビットを表す 3 つの文字は常に 0 に設定されているため、無視できます。関連するビットは 5 桁の 16 進文字（0x*nnnnn*）で表されます。 文字の前の 0 は含める必要はありません。後続の 0 は含める必要があります。たとえば、0x2001 は 0x02001 と同じですが、0x10000 の 0 はすべて必要です。関連するビットに使用できる値の詳細については、表 3-1 を参照してください。

デフォルト

デフォルト値は 0x1 で、ローカル イメージおよびスタートアップ コンフィギュレーションからブートします。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

5 つの文字には、右から左へ 0 ～ 4 の番号が付けられています。これは、16 進数および 2 進数の規格です。各文字に対して 1 つの値を選択し、必要に応じて値を組み合せたり一致させたりできます。たとえば、文字番号 3 に対して 0 または 2 を選択できます。値によっては、他の値と競合した場合に優先するものがあります。たとえば、セキュリティ アプライアンスを TFTP サーバとローカル イメージの両方からブートするよう設定する 0x2011 を設定する場合、セキュリティ アプライアンスは TFTP サーバからブートします。この値は TFTP のブートが失敗した場合、セキュリティ アプライアンスが直接 ROMMON でブートすることも定めているため、デフォルト イメージからブートすることを指定したアクションは無視されます。

0 の値は、他に指定されていなければ、アクションを実行しないことを意味します。

表 3-1 に、各 16 進文字に関連付けられたアクションを一覧表示します。各文字に対して 1 つの値を選択します。

表 3-1　コンフィギュレーション レジスタ値

Prefix	16 進文字番号 4、3、2、1、および 0				
0x	0	0	0[1]	0[2]	0[2]
	1 起動中に ROMMON のカウントダウンを 10 秒間ディセーブルにします。通常は、カウントダウン中に Escape キーを押して ROMMON に入ることができます。	2 セキュリティ アプライアンスを TFTP サーバからブートするように設定し、ブートが失敗した場合、この値は直接 ROMMON でブートします。		1 ROMMON ブート パラメータ（存在する場合は、**boot system tftp** コマンドと同じ）で指定されたように TFTP サーバ イメージからブートします。この値は、文字 1 に設定された値に優先します。	1 最初の **boot system** *local_flash* コマンドで指定されたイメージをブートします。そのイメージが読み込まれない場合、セキュリティ アプライアンスは、正常にブートするまで後続の **boot system** コマンドで指定された各イメージのブートを試行します。
					3, **5**, **7**, **9** 特定の **boot system** *local_flash* コマンドで指定されたイメージをブートします。値が 3 であると最初の **boot system** コマンドで指定されたイメージがブートされ、値が 5 であると 2 番目のイメージがブートされます（以降同様）。 イメージが正常にブートしない場合、セキュリティ アプライアンスは他の **boot system** コマンド イメージ（値 1 と値 3 の使用の違い）に戻ることを試行しません。ただし、セキュリティ アプライアンスには、ブートが失敗した場合に内部フラッシュ メモリのルート ディレクトリ内で検出されたいずれかのイメージからブートを試行するフェールセーフ機能があります。フェールセーフ機能を有効にしない場合は、ルート以外のディレクトリにイメージを保存します。
				4[3] スタートアップ コンフィギュレーションを無視してデフォルト コンフィギュレーションを読み込みます。	**2**, **4**, **6**, **8** ROMMON から、引数なしで **boot** コマンドを入力した場合、セキュリティ アプライアンスは特定の **boot system** *local_flash* コマンドで指定されたイメージをブートします。値が 3 であると最初の **boot system** コマンドで指定されたイメージがブートされ、値が 5 であると 2 番目のイメージがブートされます（以降同様）。この値はイメージを自動的にブートしません。
				5 上記の両方のアクションを実行します。	

1. 将来の使用のために予約されています。
2. 文字番号 0 および 1 がイメージを自動的にブートするように設定されていない場合、セキュリティ アプライアンスは直接 ROMMON でブートします。
3. **service password-recovery** コマンドを使用してパスワードを回復できなくした場合は、スタートアップ コンフィギュレーションを無視するようにコンフィギュレーション レジスタを設定できません。

コンフィギュレーション レジスタ値はスタンバイ装置に複製されませんが、アクティブ装置にコンフィギュレーション レジスタを設定すると、次の警告が表示されます。

```
WARNING The configuration register is not synchronized with the standby, their values
may not match.
```

また、**confreg** コマンドを使用して、コンフィギュレーション レジスタ値を ROMMON で設定することもできます。

例

次の例では、デフォルト イメージからブートするようにコンフィギュレーション レジスタを設定します。

```
hostname(config)# config-register 0x1
```

関連コマンド

コマンド	説明
boot	ブート イメージおよびスタートアップ コンフィギュレーションを設定します。
service password-recovery	パスワードの回復をイネーブルまたはディセーブルにします。

configure factory-default

コンフィギュレーションを工場出荷時のデフォルトに戻すには、**configure factory-default** コマンドをグローバル コンフィギュレーション モードで使用します。工場出荷時のデフォルト コンフィギュレーションは、シスコによって新しいセキュリティ アプライアンスに適用されたコンフィギュレーションです。このコマンドは、すべてのプラットフォームでサポートされているわけではありません。コマンドがサポートされているかどうかを確認するには、**configure** コマンドの CLI ヘルプを参照してください（グローバル コンフィギュレーション プロンプトで **configure ?** を入力します）。工場出荷時のデフォルト コンフィギュレーションは管理用のインターフェイスを自動的に設定するため、ASDM を使用して接続し、その後コンフィギュレーションを完了できます。

configure factory-default [*ip_address* [*mask*]]

シンタックスの説明

ip_address	デフォルトのアドレス 192.168.1.1 を使用する代わりに、管理インターフェイスの IP アドレスを設定します。プラットフォームに専用の管理インターフェイスが含まれている場合は、この IP アドレスがインターフェイスに適用されます。プラットフォームにデータ インターフェイスしか含まれていない場合、このアドレスはイーサネット 1 インターフェイスに適用されます。
mask	インターフェイスのサブネット マスクを設定します。マスクを設定しない場合、セキュリティ アプライアンスは IP アドレス クラスに適したマスクを使用します。

デフォルト

デフォルトの IP アドレスとマスクは 192.168.1.1 および 255.255.255.0 です。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•		•		

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

configure factory-default コマンドは、ASDM を使用してセキュリティ アプライアンスに接続するために必要な最少のコマンドを設定します。このコマンドは、ルーテッド ファイアウォール モードでのみ使用可能です。透過モードはインターフェイスの IP アドレスをサポートしていません。インターフェイス IP アドレスの設定は、このコマンドが行うアクションの 1 つです。また、このコマンドはシングル コンテキスト モードでのみ使用できます。コンフィギュレーションを消去されたセキュリティ アプライアンスには、このコマンドを使用して自動的に設定される定義済みのコンテキストはありません。

このコマンドは現在の実行コンフィギュレーションを消去してから、複数のコマンドを設定します。設定されるインターフェイスはプラットフォームによって異なります。専用の管理インターフェイスがあるプラットフォームの場合、インターフェイスは「management」という名前が付けられます。その他のプラットフォームの場合、設定されるインターフェイスはイーサネット 1 で、「inside」という名前が付けられます。

次のコマンドは、専用の管理インターフェイス Management 0/0 に適用されます（専用の管理インターフェイスがないプラットフォームの場合、インターフェイスはイーサネット 1 です）。

```
interface management 0/0
   ip address 192.168.1.1 255.255.255.0
   nameif management
   security-level 100
   no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

configure factory-default コマンドで IP アドレスを設定した場合、**http** コマンドは指定したサブネットを使用します。同様に、**dhcpd address** コマンドの範囲は指定したサブネット内のアドレスで構成されます。

工場出荷時のデフォルト コンフィギュレーションに戻した後、**copy running-config startup-config** コマンドを使用して内部フラッシュ メモリに保存します。別の位置を設定するように **boot config** コマンドを設定済みの場合にも、**copy** コマンドは、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のデフォルト位置に保存します。コンフィギュレーションが消去された場合は、このパスも消去されます。

（注） このコマンドは、**boot system** コマンドが存在する場合は、残りのコンフィギュレーションとともにこのコマンドも消去します。**boot system** コマンドを使用すると、外部フラッシュ メモリ カードのイメージを含む特定のイメージからブートできます。工場出荷時のコンフィギュレーションに戻した後、次にセキュリティ アプライアンスをリロードするとき、セキュリティ アプライアンスは内部フラッシュ メモリの最初のイメージからブートします。内部フラッシュ メモリにイメージがない場合はブートしません。

完全なコンフィギュレーションに有効な追加の設定を行うには、**setup** コマンドを参照してください。

例

次の例では、コンフィギュレーションを工場出荷時のデフォルトにリセットし、IP アドレス 10.1.1.1 をインターフェイスに割り当て、次に新しい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として保存します。

```
hostname(config)# configure factory-default 10.1.1.1 255.255.255.0
Based on the inside IP address and mask, the DHCP address
pool size is reduced to 253 from the platform limit 256

WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.

Begin to apply factory-default configuration:
Clear all configuration
...
hostname(config)#
hostname(config)# copy running-config startup-config
```

関連コマンド

コマンド	説明
boot system	ブートするソフトウェア イメージを設定します。
clear configure	実行コンフィギュレーションを消去します。
copy running-config startup-config	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コピーします。
setup	セキュリティ アプライアンスの基本設定を設定するよう要求します。
show running-config	実行コンフィギュレーションを表示します。

configure http

HTTP（S）サーバからのコンフィギュレーション ファイルを実行コンフィギュレーションとマージするには、**configure http** コマンドをグローバル コンフィギュレーション モードで使用します。このコマンドは、IPv4 アドレスと IPv6 アドレスをサポートしています。

**configure *http*[*s*]*://*[*user*[*:password*]*@*]*server*[*:port*]*/*[*path/*]*filename*

シンタックスの説明

*:*password	（オプション）HTTP（S）認証の場合、パスワードを指定します。
:port	（オプション）ポートを指定します。HTTP の場合、デフォルトは 80 です。HTTPS の場合、デフォルトは 443 です。
@	（オプション）名前とパスワードの両方またはいずれか一方を入力する場合は、サーバの IP アドレスにアットマーク（@）を付けます。
filename	コンフィギュレーション ファイル名を指定します。
http[**s**]	HTTP または HTTPS を指定します。
path	（オプション）ファイル名へのパスを指定します。
server	サーバの IP アドレスまたは名前を指定します。IPv6 サーバ アドレスの場合、ポートを指定した場合は、IP アドレス内のコロンがポート番号の前のコロンと間違われないように、IP アドレスを角カッコで囲む必要があります。たとえば、アドレスとポートを次のように入力します。 `[fe80::2e0:b6ff:fe01:3b7a]:8080`
user	（オプション）HTTP（S）認証の場合、ユーザ名を指定します。

デフォルト

HTTP の場合、デフォルト ポートは 80 です。HTTPS の場合、デフォルト ポートは 443 です。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

マージでは、新しいコンフィギュレーションのすべてのコマンドが実行コンフィギュレーションに追加され、競合するすべてのコマンドが新しいバージョンで上書きされます。たとえば、コマンドが複数のインスタンスを許可している場合は、新しいコマンドが実行コンフィギュレーション内の既存のコマンドに追加されます。コマンドが 1 つのインスタンスしか許可していない場合は、実行コンフィギュレーション内のコマンドが新しいコマンドで上書きされます。実行コンフィギュレーション内に存在するが、新しいコンフィギュレーションには設定されていないコマンドは、マージによって削除されません。

このコマンドは、**copy http running-config** コマンドと同じです。マルチ コンテキスト モードの場合、このコマンドを使用できるのはシステム実行スペースに限られるため、**configure http** コマンドはコンテキスト内で使用するための代替です。

例

次の例では、コンフィギュレーション ファイルを HTTPS サーバから実行コンフィギュレーションにコピーします。

```
hostname(config)# configure https://user1:pa$$w0rd@10.1.1.1/configs/newconfig.cfg
```

関連コマンド

コマンド	説明
clear configure	実行コンフィギュレーションを消去します。
configure memory	スタートアップ コンフィギュレーションを実行コンフィギュレーションとマージします。
configure net	指定した TFTP URL からのコンフィギュレーション ファイルを実行コンフィギュレーションとマージします。
configure factory-default	CLI で入力するコマンドを実行コンフィギュレーションに追加します。
show running-config	実行コンフィギュレーションを表示します。

configure memory

スタートアップ コンフィギュレーションを実行コンフィギュレーションとマージするには、**configure memory** コマンドをグローバル コンフィギュレーション モードで使用します。

configure memory

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

マージでは、新しいコンフィギュレーションのすべてのコマンドが実行コンフィギュレーションに追加され、競合するすべてのコマンドが新しいバージョンで上書きされます。たとえば、コマンドが複数のインスタンスを許可している場合は、新しいコマンドが実行コンフィギュレーション内の既存のコマンドに追加されます。コマンドが 1 つのインスタンスしか許可していない場合は、実行コンフィギュレーション内のコマンドが新しいコマンドで上書きされます。実行コンフィギュレーション内に存在するが、新しいコンフィギュレーションには設定されていないコマンドは、マージによって削除されません。

コンフィギュレーションをマージしない場合は、セキュリティ アプライアンスを経由する通信を妨げる実行コンフィギュレーションを消去してから、**configure memory** コマンドを入力して新しいコンフィギュレーションを読み込むことができます。

このコマンドは **copy startup-config running-config** コマンドと同じです。

マルチ コンテキスト モードの場合、コンテキストのスタートアップ コンフィギュレーションは **config-url** コマンドで指定した場所にあります。

例

次の例では、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーします。

```
hostname(config)# configure memory
```

関連コマンド

コマンド	説明
clear configure	実行コンフィギュレーションを消去します。
configure http	指定した HTTP(S) URL からのコンフィギュレーション ファイルを実行コンフィギュレーションとマージします。
configure net	指定した TFTP URL からのコンフィギュレーション ファイルを実行コンフィギュレーションとマージします。
configure factory-default	CLI で入力するコマンドを実行コンフィギュレーションに追加します。
show running-config	実行コンフィギュレーションを表示します。

configure net

TFTP サーバからのコンフィギュレーション ファイルを実行コンフィギュレーションとマージするには、**configure net** コマンドをグローバル コンフィギュレーション モードで使用します。このコマンドは、IPv4 アドレスと IPv6 アドレスをサポートしています。

configure net [*server:*[*filename*] | *:filename*]

シンタックスの説明

:filename	パスとファイル名を指定します。**tftp-server** コマンドを使用してファイル名をすでに設定している場合、この引数はオプションです。 **tftp-server** コマンドで名前を指定したように、このコマンドでファイル名を指定すると、セキュリティ アプライアンスは **tftp-server** コマンド ファイル名をディレクトリとして扱い、***configure net*** コマンド ファイル名をディレクトリの下のファイルとして追加します。 **tftp-server** コマンドの値を上書きするには、パスとファイル名の前にスラッシュを入力します。スラッシュは、パスが tftpboot ディレクトリに対する相対パスではなく、絶対パスであることを示します。このファイル用に生成される URL には、ファイル名パスの前にダブル スラッシュ（//）が含まれます。必要なファイルが tftpboot ディレクトリにある場合は、ファイル名パスに tftpboot ディレクトリへのパスを含めることができます。 **tftp-server** コマンドを使用して TFTP サーバのアドレスを指定した場合、コロン（:）の後にファイル名だけを入力できます。
server:	TFTP サーバの IP アドレスまたは名前を設定します。このアドレスが存在する場合は、**tftp-server** コマンドで設定したアドレスを上書きします。IPv6 サーバ アドレスの場合、IP アドレス内のコロンがファイル名の前のコロンと間違われないように、IP アドレスを角カッコで囲む必要があります。たとえば、アドレスを次のように入力します。 [fe80::2e0:b6ff:fe01:3b7a] デフォルト ゲートウェイ インターフェイスは最高レベルのセキュリティ インターフェイスですが、**tftp-server** コマンドを使用して別のインターフェイス名を設定できます。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

マージでは、新しいコンフィギュレーションのすべてのコマンドが実行コンフィギュレーションに追加され、競合するすべてのコマンドが新しいバージョンで上書きされます。たとえば、コマンドが複数のインスタンスを許可している場合は、新しいコマンドが実行コンフィギュレーション内の既存のコマンドに追加されます。コマンドが 1 つのインスタンスしか許可していない場合は、実行コンフィギュレーション内のコマンドが新しいコマンドで上書きされます。実行コンフィギュレーション内に存在するが、新しいコンフィギュレーションには設定されていないコマンドは、マージによって削除されません。

このコマンドは、**copy tftp running-config** コマンドと同じです。マルチ コンテキスト モードの場合、このコマンドを使用できるのはシステム実行スペースに限られるため、**configure net** コマンドはコンテキスト内で使用するための代替です。

例

次の例では **tftp-server** コマンドにサーバとファイル名を設定した後、**configure net** コマンドを使用してサーバを上書きします。同じファイル名が使用されています。

```
hostname(config)# tftp-server inside 10.1.1.1 configs/config1
hostname(config)# configure net 10.2.2.2:
```

次の例では、サーバとファイル名を上書きします。ファイル名へのデフォルト パスは /tftpboot/configs/config1 です。ファイル名をスラッシュ（/）で始めない場合、パスの /tftpboot/ の部分はデフォルトで含まれます。このパスを上書きし、ファイルも tftpboot にある場合は、tftpboot パスを **configure net** コマンドに含めます。

```
hostname(config)# tftp-server inside 10.1.1.1 configs/config1
hostname(config)# configure net 10.2.2.2:/tftpboot/oldconfigs/config1
```

次の例では、サーバだけを **tftp-server** コマンドに設定します。**configure net** コマンドはファイル名だけを指定します。

```
hostname(config)# tftp-server inside 10.1.1.1
hostname(config)# configure net :configs/config1
```

関連コマンド

コマンド	説明
configure http	指定した HTTP(S) URL からのコンフィギュレーション ファイルを実行コンフィギュレーションとマージします。
configure memory	スタートアップ コンフィギュレーションを実行コンフィギュレーションとマージします。
show running-config	実行コンフィギュレーションを表示します。
tftp-server	他のコマンドで使用するためのデフォルトの TFTP サーバおよびパスを設定します。
write net	実行コンフィギュレーションを TFTP サーバにコピーします。

configure terminal

実行コンフィギュレーションをコマンドラインで設定するには、**configure terminal** コマンドを特権 EXEC モードで使用します。このコマンドは、コンフィギュレーションを変更するコマンドを入力できるグローバル コンフィギュレーション モードに入ります。

configure terminal

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

例

次の例では、グローバル コンフィギュレーション モードに入ります。

```
hostname# configure terminal
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure	実行コンフィギュレーションを消去します。
configure http	指定した HTTP(S) URL からのコンフィギュレーション ファイルを実行コンフィギュレーションとマージします。
configure memory	スタートアップ コンフィギュレーションを実行コンフィギュレーションとマージします。
configure net	指定した TFTP URL からのコンフィギュレーション ファイルを実行コンフィギュレーションとマージします。
show running-config	実行コンフィギュレーションを表示します。

config-url

システムがコンテキスト コンフィギュレーションをダウンロードする URL を指定するには、**config-url** コマンドをコンテキスト コンフィギュレーション モードで使用します。

config-url *url*

シンタックスの説明

url　コンテキスト コンフィギュレーションの URL を設定します。すべてのリモート URL は、管理コンテキストからアクセスできる必要があります。次の URL シンタックスを参照してください。

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

  ASA 5500 シリーズ適応型セキュリティ アプライアンスの場合、この URL は内部フラッシュ メモリを指します。***disk0*** ではなく ***flash*** を使用することもできます。これらは、エイリアス関係にあります。

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

  ASA 5500 シリーズ適応型セキュリティ アプライアンスの場合、この URL は外部フラッシュ メモリ カードを指します。

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

  この URL は内部フラッシュ メモリを指します。

- ***ftp://*[*user*[***:***password*]***@***]*server*[*:port*]***/***[*path/*]*filename*[***;type=***xx*]**

  type には、次のいずれかのキーワードを指定できます。

  - ***ap***：ASCII パッシブ モード
  - ***an***：ASCII 通常モード
  - ***ip***：（デフォルト）バイナリ パッシブ モード
  - ***in***：バイナリ通常モード

- ***http*[*s*]*://*[*user*[***:***password*]***@***]*server*[*:port*]***/***[*path/*]*filename***

- ***tftp://*[*user*[***:***password*]***@***]*server*[*:port*]***/***[*path/*]*filename*[***;int=***interface_name*]**

  サーバ アドレスへのルートを上書きする場合は、インターフェイス名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン　コンテキスト URL を追加すると、システムはただちにコンテキストを読み込み実行中になります。

（注）　**config-url** コマンドを入力する前に、**allocate-interface** コマンドを入力します。セキュリティ アプライアンスは、コンテキスト コンフィギュレーションを読み込む前に、コンテキストにインターフェイスを割り当てる必要があります。コンテキスト コンフィギュレーションには、インターフェイス（**interface**、**nat**、**global** など）を示すコマンドが含まれている場合があります。最初に **config-url** コマンドを入力した場合、セキュリティ アプライアンスはただちにコンテキスト コンフィギュレーションを読み込みます。コンテキストにインターフェイスを示すコマンドが含まれていない場合、それらのコマンドは失敗します。

ファイル名にファイル拡張子は必要ありませんが、「.cfg」を使用することを推奨します。

管理コンテキスト ファイルは、内部フラッシュ メモリに保存する必要があります。

HTTP または HTTPS サーバからコンテキスト コンフィギュレーションをダウンロードした場合、**copy running-config startup-config** コマンドを使用して変更内容をそれらのサーバに保存することはできません。ただし、**copy tftp** コマンドを使用して実行コンフィギュレーションを TFTP サーバにコピーできます。

サーバが利用できない、またはファイルがまだ存在しないためにシステムがコンテキスト コンフィギュレーション ファイルを取得できない場合、システムは、コマンドライン インターフェイスでただちに設定できるブランクのコンテキストを作成します。

URL を変更するには、新しい URL で **config-url** コマンドを再入力します。

セキュリティ アプライアンスは、新しいコンフィギュレーションを現在の実行コンフィギュレーションとマージします。同じ URL を再入力しても、保存されたコンフィギュレーションが実行コンフィギュレーションとマージされます。マージにより、新しいコンフィギュレーションのすべての新しいコマンドが実行コンフィギュレーションに追加されます。コンフィギュレーションが同じ場合、変更は行われません。コマンドが競合する場合、またはコマンドがコンテキストの実行に影響を与える場合、マージの効果はコマンドによって異なります。エラーが発生したり、予期しない結果が生じたりすることがあります。実行コンフィギュレーションがブランクの場合（たとえば、サーバが利用不可能でコンフィギュレーションがダウンロードされなかった場合）は、新しいコンフィギュレーションが使用されます。コンフィギュレーションをマージしない場合は、コンテキストを経由する通信を妨げる実行コンフィギュレーションを消去してから、新しい URL からコンフィギュレーションをリロードすることができます。

例

次の例では、管理コンテキストを「administrator」と設定し、内部フラッシュ メモリに「administrator」という名前のコンテキストを作成してから、FTP サーバから 2 つのコンテキストを追加しています。

```
hostname(config)# admin-context administrator
hostname(config)# context administrator
hostname(config-ctx)# allocate-interface gigabitethernet0/0.1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.1
hostname(config-ctx)# config-url flash:/admin.cfg

hostname(config-ctx)# context test
hostname(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg

hostname(config-ctx)# context sample
hostname(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
```

関連コマンド

コマンド	説明
allocate-interface	コンテキストにインターフェイスを割り当てます。
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードに入ります。
show context	コンテキストのリスト（システム実行スペース）または現在のコンテキストに関する情報を表示します。

console timeout

セキュリティ アプライアンスへのコンソール接続のアイドル タイムアウトを設定するには、**console timeout** コマンドをグローバル コンフィギュレーション モードで使用します。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。

console timeout *number*

no console timeout [*number*]

シンタックスの説明

number	経過後にコンソール セッションが終了するアイドル タイムアウトを分単位（0 ～ 60）で指定します。

デフォルト

デフォルトのタイムアウトは 0 で、コンソール セッションはタイムアウトしません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	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	•	•	•	•	•

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

console timeout コマンドは、セキュリティ アプライアンスへの認証済みのすべてのイネーブル モード ユーザ セッションとコンフィギュレーション モード ユーザ セッションにタイムアウト値を設定します。**console timeout** コマンドによって、Telnet タイムアウトや SSH タイムアウトが変更されることはありません。これらのアクセス方式については、それぞれ独自のタイムアウト値が保持されています。

no console timeout コマンドは、コンソール タイムアウト値をデフォルトのタイムアウトの 0 にリセットします。この値は、コンソールがタイムアウトしないことを意味します。

例

次の例では、コンソール タイムアウトを 15 分に設定する方法を示します。

```
hostname(config)# console timeout 15
```

関連コマンド

コマンド	説明
clear configure console	デフォルトのコンソール接続設定に戻します。
show running-config console timeout	セキュリティ アプライアンスへのコンソール接続のアイドル タイムアウトを表示します。

content-length

HTTP メッセージ本文の長さに基づいて HTTP トラフィックを制限するには、**http-map** コマンドを使用してアクセスできる **content-length** コマンドを HTTP マップ コンフィギュレーション モードで使用します。このコマンドを削除するには、このコマンドの **no** 形式を使用します。

content-length { **min** *bytes* [**max** *bytes*] | **max** *bytes*] } **action** {**allow** | **reset** | **drop**} [**log**]

no content-length { **min** *bytes* [**max** *bytes*] | **max** *bytes*] } **action** {**allow** | **reset** | **drop**} [**log**]

シンタックスの説明

action	メッセージがこの検査に合格しなかったときに実行されるアクションを指定します。
allow	メッセージを許可します。
bytes	バイト数を指定します。許容される範囲は、**min** オプションでは 1 ～ 65,535、**max** オプションでは 1 ～ 50,000,000 です。
drop	接続を終了します。
log	（オプション）syslog を生成します。
max	（オプション）使用可能な最大コンテキスト長を指定します。
min	使用可能な最小コンテキスト長を指定します。
reset	クライアントまたはサーバに TCP リセット メッセージを送信します。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
HTTP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

content-length コマンドをイネーブルにすると、セキュリティ アプライアンスは設定された範囲内のメッセージだけを許可し、許可しない場合は指定されたアクションを実行します。セキュリティ アプライアンスが TCP 接続をリセットして syslog エントリを作成するようにするには、**action** キーワードを使用します。

例

次の例では、HTTP トラフィックを 100 バイト以上 2,000 バイト以下のメッセージに制限しています。メッセージがこの範囲外の場合、セキュリティ アプライアンスは TCP 接続をリセットし、syslog エントリを作成します。

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# content-length min 100 max 2000 action reset log
hostname(config-http-map)# exit
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
http-map	高度な HTTP 検査を設定するための HTTP マップを定義します。
debug appfw	高度な HTTP 検査に関連付けられているトラフィックに関する詳細情報を表示します。
inspect http	アプリケーション検査用に特定の HTTP マップを適用します。
policy-map	クラスマップを特定のセキュリティ アクションに関連付けます。

content-type-verification

HTTP メッセージのコンテキスト タイプに基づいて HTTP トラフィックを制限するには、**http-map** コマンドを使用してアクセスできる **content-type-verification** コマンドを HTTP マップ コンフィギュレーション モードで使用します。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。

content-type-verification [**match-req-rsp**] **action** {**allow** | **reset** | **drop**} [**log**]

no content-type-verification [**match-req-rsp**] **action** {**allow** | **reset** | **drop**} [**log**]

シンタックスの説明

action	メッセージがコマンド検査に合格しなかったときに実行されるアクションを指定します。
allow	メッセージを許可します。
drop	接続を終了します。
log	（オプション）syslog メッセージを生成します。
match-req-rsp	（オプション）HTTP 応答の content-type フィールドが、対応する HTTP 要求メッセージの accept フィールドに一致するかどうかを確認します。
reset	クライアントまたはサーバに TCP リセット メッセージを送信します。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
HTTP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは次のチェックをイネーブルにします。

- ヘッダーの content-type の値が、サポートされているコンテンツ タイプの内部リストにあることを確認します。
- ヘッダーの content-type が、データ内の実際のコンテンツまたはメッセージのエンティティ本体の部分と一致していることを確認します。
- **match-req-rsp** キーワードは、HTTP 応答の content-type フィールドが、対応する HTTP 要求メッセージの **accept** フィールドに一致することを確認する追加のチェックをイネーブルにします。

メッセージが上記のいずれかのチェックに合格しなかった場合、セキュリティ アプライアンスは設定されたアクションを実行します。

次に、サポートされているコンテンツ タイプのリストを示します。

audio/* |	audio/basic |	video/x-msvideo
audio/mpeg |	audio/x-adpcm |	audio/midi
audio/x-ogg |	audio/x-wav |	audio/x-aiff |
application/octet-stream	application/pdf	application/msword
application/vnd.ms-excel	application/vnd.ms-powerpoint	application/postscript
application/x-java-arching	application/x-msn-messenger	application/x-gzip
image |	application/x-java-xm	application/zip
image/jpeg |	image/cgf |	image/gif |
image/x-3ds |	image/png |	image/tiff |
image/x-portable-bitmap |	image/x-bitmap |	image/x-niff |
text/* |	image/x-portable-greymap |	image/x-xpm |
text/plain |	text/css	text/html |
text/xmcd	text/richtext |	text/sgml
video/-flc	text/xml	video/*
video/sgi	video/mpeg	video/quicktime
video/x-mng	video/x-avi	video/x-fli

このリストの一部のコンテンツ タイプは、対応する正規表現（マジック ナンバー）がないためにメッセージの本体部分で確認できない場合があります。その場合、HTTP メッセージが許可されます。

例

次の例では、HTTP メッセージのコンテンツ タイプに基づいて HTTP トラフィックを制限します。サポートされていないコンテンツ タイプがメッセージに含まれている場合、セキュリティ アプライアンスは TCP 接続を制限し、syslog エントリを作成します。

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# content-type-verification match-req-rsp reset log
hostname(config-http-map)# exit
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
http-map	高度な HTTP 検査を設定するための HTTP マップを定義します。
debug appfw	高度な HTTP 検査に関連付けられているトラフィックに関する詳細情報を表示します。
inspect http	アプリケーション検査用に特定の HTTP マップを適用します。
policy-map	クラスマップを特定のセキュリティ アクションに関連付けます。

context

システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードに入るには、**context** コマンドをグローバル コンフィギュレーション モードで使用します。コン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。コンテキスト コンフィギュレーション モードでは、コンテキストで使用できるコンフィギュレーション ファイルの URL とインターフェイスを指定できます。

context *name*

no context *name* [***noconfirm***]

シンタックスの説明

name	名前を最大 32 文字の文字列で指定します。この名前では大文字と小文字が区別されるため、たとえば、「customerA」と「CustomerA」という名前で 2 つのコンテキストを作成できます。文字、数字、またはハイフンを使用できますが、名前の先頭または末尾にハイフンを使用することはできません。 「System」および「Null」（大文字および小文字）は予約されている名前であるため、使用できません。
noconfirm	（オプション）確認を求めるプロンプトを表示せずにコンテキストを削除します。このオプションは、自動スクリプトに役立ちます。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

管理コンテキストがない場合（たとえば、コンフィギュレーションを消去した場合）、追加する最初のコンテキストは管理コンテキストである必要があります。管理コンテキストを追加するには、**admin-context** コマンドを参照してください。管理コンテキストを指定した後、**context** コマンドを入力して管理コンテキストを設定します。

コンテキストは、システム コンフィギュレーションを編集することによってのみ削除できます。現在の管理コンテキストはこのコマンドの **no** 形式を使用して削除できません。**clear configure context** コマンドを使用してすべてのコンテキストを削除した場合のみ削除できます。

例

次の例では、管理コンテキストを「administrator」と設定し、内部フラッシュ メモリに「administrator」という名前のコンテキストを作成してから、FTP サーバから 2 つのコンテキストを追加しています。

```
hostname(config)# admin-context administrator
hostname(config)# context administrator
hostname(config-ctx)# allocate-interface gigabitethernet0/0.1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.1
hostname(config-ctx)# config-url flash:/admin.cfg

hostname(config-ctx)# context test
hostname(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg

hostname(config-ctx)# context sample
hostname(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
```

関連コマンド

コマンド	説明
allocate-interface	コンテキストにインターフェイスを割り当てます。
changeto	コンテキストとシステム実行スペースの間で切り替えを行います。
config-url	コンテキスト コンフィギュレーションの場所を指定します。
join-failover-group	フェールオーバー グループにコンテキストを割り当てます。
show context	コンテキスト情報を表示します。

copy

ファイルをある場所から別の場所にコピーするには、**copy** コマンドを使用します。

copy [*/options*] {*url* | *local*:[*path*] | *running-config* | *startup-config*} {*running-config* | *startup-config* | *url* | *local*:[*path*]}

no **copy** [*/options*] {*url* | *local*:[*path*] | *running-config* | *startup-config*} {*running-config* | *startup-config* | *url* | *local*:[*path*]}

シンタックスの説明

/options	copy コマンドで使用するオプション。 • noconfirm 確認プロンプトなしでファイルをコピーします。 • pcap 事前に設定した TFTP サーバのデフォルトを指定します。
url	コンテキスト コンフィギュレーションの URL を設定します。すべてのリモート URL は、管理コンテキストからアクセスできる必要があります。次の URL シンタックスを参照してください。 • ***disk0:/***[*path/*]*filename* このオプションは ASA プラットフォームだけで使用でき、内部フラッシュ メモリを示します。***disk0*** ではなく ***flash*** を使用することもできます。これらは、エイリアス関係にあります。 • ***disk1:/***[*path/*]*filename* このオプションは ASA プラットフォームだけで使用でき、外部フラッシュ メモリ カードを示します。 • ***flash:/***[*path/*]*filename* このオプションは、内部フラッシュ カードを示します。ASA プラットフォームの場合、***flash*** は ***disk0*** のエイリアスです。 • ***ftp://***[*user*[***:****password*]***@***]*server*[*:port*]***/***[*path/*]*filename*[***;type=****xx*] ***type*** には、次のいずれかのキーワードを指定できます。 － ***ap***：ASCII パッシブ モード － ***an***：ASCII 通常モード － ***ip***：（デフォルト）バイナリ パッシブ モード － ***in***：バイナリ通常モード • ***http***[***s***]***://***[*user*[***:****password*]***@***]*server*[*:port*]***/***[*path/*]*filename* • ***tftp://***[*user*[***:****password*]***@***]*server*[*:port*]***/***[*path/*]*filename*[***;int=****interface_name*] サーバ アドレスへのルートを上書きする場合は、インターフェイス名を指定します。
path	サーバ上のファイル パスの最後の要素を示すパス名。

デフォルト

このコマンドにデフォルト設定はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権モード	•	•	•	•	•

コマンド履歴

リリース	変更
7.0(1)	このコマンドがサポートされるようになりました。

使用上のガイドライン

セキュリティ アプライアンスは、そのルーティング テーブル情報によって、（*tftp_pathname* 引数で指定された）目的の場所に到達する方法を認識する必要があります。この情報は、コンフィギュレーションに応じて **ip address** コマンドまたは **route** コマンドによって決定されます（RIP も使用されることがあります）。*tftp_pathname* には、サーバ上のファイル パスの最後の要素に加えて、任意のディレクトリ名を含むことができます。

pathname には、サーバ上のファイル パスの最後の要素に加えて、任意のディレクトリ名を含むことができます。ただし、パス名にスペースを含めることはできません。ディレクトリ名にスペースが含まれている場合は、**copy tftp flash** コマンドを使用する代わりに、TFTP サーバのディレクトリを設定してください。

例

次の例では、ファイルをディスクから TFTP サーバにコピーする方法を示します。

```
hostname(config)# copy disk0:my_context/my_context.cfg
tftp://10.7.0.80/my_context/my_context.cfg
```

次に、ファイルをディスク上のある場所からディスク上の別の場所にコピーする方法を示します。宛先ファイルの名前は、コピー元のファイルの名前にすることも、別の名前することもできます。

```
hostname(config)# copy disk0:my_context.cfg disk0:my_context/my_context.cfg
```

次に、イメージまたは ASDM ファイルをディスクからフラッシュ パーティションにコピーする方法を示します。

```
hostname(config)# copy tftp://10.7.0.80/asa700.bin disk0:asa700.bin
hostname(config)# copy tftp://10.7.0.80/asdm700.bin disk0:asdm700.bin
```

次に、ファイルをディスクからスタートアップ コンフィギュレーションまたは実行コンフィギュレーションにコピーする方法を示します。

```
hostname(config)# copy disk:my_context/my_context.cfg startup-config
hostname(config)# copy disk:my_context/my_context.cfg running-config
```

関連コマンド

コマンド	説明
copy capture	キャプチャ ファイルを TFTP サーバにコピーします。

copy capture

キャプチャ ファイルを TFTP サーバにコピーするには、**copy capture** コマンドをグローバル コンフィギュレーション モードで使用します。

copy [*/options*] **capture:** *buffer_name* **url:**//*pathname*

シンタックスの説明

/options	copy コマンドで使用するオプション。 • **noconfirm** 確認プロンプトなしでファイルをコピーします。 • **pcap** キャプチャを転送する形式を指定します。
buffer_name	キャプチャを識別するための一意の名前。
url	コンテキスト コンフィギュレーションの URL を設定します。すべてのリモート URL は、管理コンテキストからアクセスできる必要があります。次の URL シンタックスを参照してください。 • ***disk0:/*[*path/*]*filename*** このオプションは ASA プラットフォームだけで使用でき、内部フラッシュ カードを示します。***disk0*** ではなく ***flash*** を使用することもできます。これらは、エイリアス関係にあります。 • ***disk1:/*[*path/*]*filename*** このオプションは ASA プラットフォームだけで使用でき、外部フラッシュ カードを示します。 • ***flash:/*[*path/*]*filename*** このオプションは、内部フラッシュ カードを示します。ASA プラットフォームの場合、***flash*** は ***disk0*** のエイリアスです。 • ***ftp://***[*user*[**:***password*]**@**]*server*[*:port*]**/**[*path/*]*filename*[***;type=****xx*] ***type*** には、次のいずれかのキーワードを指定できます。 － ***ap***：ASCII パッシブ モード － ***an***：ASCII 通常モード － ***ip***：（デフォルト）バイナリ パッシブ モード － ***in***：バイナリ通常モード • ***http***[*s*]***://***[*user*[**:***password*]**@**]*server*[*:port*]**/**[*path/*]*filename* • ***tftp://***[*user*[**:***password*]**@**]*server*[*:port*]**/**[*path/*]*filename*[***;int=****interface_name*] サーバ アドレスへのルートを上書きする場合は、インターフェイス名を指定します。
pathname	サーバ上のファイル パスの最後の要素を示すパス名。
pcap	（オプション）事前に設定した TFTP サーバのデフォルトを指定します。

デフォルト

このコマンドにデフォルト設定はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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	透過	シングル	マルチ コンテキスト	システム
特権モード	•	•	•	•	•

コマンド履歴

リリース	変更
7.0(1)	セキュリティ アプライアンスでこのコマンドがサポートされるようになりました。

使用上のガイドライン

セキュリティ アプライアンスは、そのルーティング テーブル情報によって、（*tftp_pathname* 引数で指定された）目的の場所に到達する方法を認識する必要があります。この情報は、コンフィギュレーションに応じて **ip address** コマンド、**route** コマンド、RIP、または OSPF によって決定されます。*tftp_pathname* には、サーバ上のファイル パスの最後の要素に加えて、任意のディレクトリ名を含むことができます。

pathname には、サーバ上のファイル パスの最後の要素に加えて、任意のディレクトリ名を含むことができます。ただし、パス名にスペースを含めることはできません。ディレクトリ名にスペースが含まれている場合は、**copy tftp flash** コマンドを使用する代わりに、TFTP サーバのディレクトリを設定してください。HTTP または TFTP を使用して、セキュリティ アプライアンスからイメージを取得できます。

例

次の例では、フルパスを指定せずに **copy capture** コマンドを入力した場合に表示されるプロンプトを示します。

```
hostname(config)# copy /pcap capture:abc tftp
Address or name of remote host [171.68.11.129]?
Source file name [username/cdisk]?
copying capture to tftp://171.68.11.129/username/cdisk:
[yes|no|again]? y
!!!!!!!!!!!!!
```

次のようにフルパスを指定できます。

```
hostname(config)# copy pcap/capture:abc tftp:171.68.11.129/tftpboot/abc.cap
```

TFTP サーバを設定している場合は、次のようにファイルの位置や名前を省略できます。

```
hostname(config)# tftp-server outside 171.68.11.129 tftp/cdisk
hostname(config)# copy pcap capture:abc tftp:/tftp/abc.cap
```

次の例では、事前に設定した TFTP サーバのデフォルト値を **copy capture** コマンドで使用する方法を示します。

```
hostname(config)# copy /pcap capture:abc tftp
```

関連コマンド

コマンド	説明
capture	パケット キャプチャ機能を有効にして、パケットのスニッフィングやネットワーク障害を検出できるようにします。
clear capture	キャプチャ バッファをクリアします。
show capture	オプションが何も指定されていない場合は、キャプチャのコンフィギュレーションを表示します。

crashinfo console disable

フラッシュに対するクラッシュ書き込みの読み取り、書き込み、および設定を行うには、**crashinfo console disable** コマンドを使用します。

crashinfo console disable

[no] crashinfo console disable

シンタックスの説明

disable	クラッシュが発生した場合にコンソール出力を抑制します。

デフォルト

このコマンドにデフォルト設定はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(4)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、crashinfo がコンソールに出力されないようにすることができます。crashinfo には、装置に接続されたすべてのユーザに対して表示されるのにふさわしくない機密情報が含まれている場合があります。このコマンドとともに、crashinfo がフラッシュに書き込まれていることも確認する必要があります。これは装置のリブート後に確認できます。このコマンドは、crashinfo および checkheaps の出力に影響を与えます。この出力はフラッシュに保存され、トラブルシューティングに十分に役立ちます。

例

```
hostname(config)# crashinfo console disable
```

関連コマンド

コマンド	説明
clear configure fips	NVRAM に格納されている、システムまたはモジュールの FIPS コンフィギュレーション情報を消去します。
fips enable	システムまたはモジュールに対して FIPS 準拠を強制するためのポリシーチェックをイネーブルまたはディセーブルにします。
fips self-test poweron	パワーオン セルフテストを実行します。
show crashinfo console	フラッシュに対するクラッシュ書き込みの読み取り、書き込み、および設定を行います。
show running-config fips	セキュリティ アプライアンス上で実行されている FIPS コンフィギュレーションを表示します。

crashinfo force

セキュリティ アプライアンスを強制的にクラッシュさせるには、***crashinfo force*** コマンドを特権 EXEC モードで使用します。

crashinfo force [**page-fault | watchdog**]

シンタックスの説明

page-fault	（オプション）ページ フォールトを利用して、セキュリティ アプライアンスを強制的にクラッシュさせます。
watchdog	（オプション）ウォッチドッグを利用して、セキュリティ アプライアンスを強制的にクラッシュさせます。

デフォルト

デフォルトでは、セキュリティ アプライアンスはフラッシュ メモリにクラッシュ情報ファイルを保存します。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

crashinfo force コマンドを使用して、クラッシュ出力の生成をテストできます。クラッシュ出力では、本物のクラッシュと **crashinfo force page-fault** コマンドまたは **crashinfo force watchdog** コマンドによって発生したクラッシュは区別できません。これは、コマンドによって実際にクラッシュが発生しているためです。セキュリティ アプライアンスは、クラッシュのダンプが完了するとリロードします。

注意　実稼働環境では **crashinfo force** コマンドを使用しないでください。**crashinfo force** コマンドはセキュリティ アプライアンスをクラッシュさせて、強制的にリロードを実行します。

例

次の例では、**crashinfo force page-fault** コマンドを入力したときに表示される警告を示します。

```
hostname# crashinfo force page-fault
WARNING: This command will force the XXX to crash and reboot.
    Do you wish to proceed? [confirm]:
```

キーボードの Return キーまたは Enter キーを押して復帰改行を入力するか、**Y** キーまたは **y** キーを押すと、セキュリティ アプライアンスがクラッシュしてリロードが実行されます。これらの応答は、いずれも操作に同意したものと解釈されます。その他の文字はすべて **no** と解釈され、セキュリティ アプライアンスはコマンドライン プロンプトに戻ります。

関連コマンド

clear crashinfo	クラッシュ情報ファイルの内容を消去します。
crashinfo save disable	フラッシュ メモリへのクラッシュ情報の書き込みをディセーブルにします。
crashinfo test	フラッシュ メモリ内のファイルにクラッシュ情報を保存する、セキュリティ アプライアンスの機能をテストします。
show crashinfo	クラッシュ情報ファイルの内容を表示します。

crashinfo save disable

フラッシュ メモリへのクラッシュ情報の書き込みをディセーブルにするには、***crashinfo save*** コマンドをグローバル コンフィギュレーション モードで使用します。

crashinfo save disable

no crashinfo save disable

シンタックスの説明

このコマンドには、デフォルトの引数もキーワードもありません。

デフォルト

デフォルトでは、セキュリティ アプライアンスはフラッシュ メモリにクラッシュ情報ファイルを保存します。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	***crashinfo save enable*** コマンドは廃止され、有効なオプションではなくなりました。代わりに、***no crashinfo save disable*** コマンドを使用します。

使用上のガイドライン

クラッシュ情報は、まずフラッシュ メモリに書き込まれ、次にコンソールに書き込まれます。

（注） セキュリティ　アプライアンスが起動中にクラッシュした場合、クラッシュ情報ファイルは保存されません。クラッシュ情報をフラッシュ メモリに保存するには、セキュリティ アプライアンスは完全に初期化されて、動作を開始している必要があります。

クラッシュ情報のフラッシュ メモリへの保存をもう一度イネーブルにするには、**no crashinfo save disable** コマンドを使用します。

例

```
hostname(config)# crashinfo save disable
```

関連コマンド

clear crashinfo	クラッシュ ファイルの内容を消去します。
crashinfo force	セキュリティ アプライアンスを強制的にクラッシュさせます。
crashinfo test	フラッシュ メモリ内のファイルにクラッシュ情報を保存する、セキュリティ アプライアンスの機能をテストします。
show crashinfo	クラッシュ ファイルの内容を表示します。

crashinfo test

セキュリティ アプライアンスの機能をテストして、フラッシュ メモリ内のファイルにクラッシュ情報を保存するには、***crashinfo test*** コマンドをグローバル コンフィギュレーション モードで使用します。

crashinfo test

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

フラッシュ メモリ内に以前のクラッシュ情報ファイルがすでに存在する場合、そのファイルは上書きされます。

（注）　**crashinfo test** コマンドを入力してもセキュリティ アプライアンスはクラッシュしません。

例

次の例では、クラッシュ情報ファイル テストの出力を示します。

```
hostname(config)# crashinfo test
```

関連コマンド

clear crashinfo	クラッシュ ファイルの内容を削除します。
crashinfo force	セキュリティ アプライアンスを強制的にクラッシュさせます。
crashinfo save disable	フラッシュ メモリへのクラッシュ情報の書き込みをディセーブルにします。
show crashinfo	クラッシュ ファイルの内容を表示します。

crl

CRL コンフィギュレーション オプションを指定するには、**crl** コマンドを暗号 CA トラストポイント コンフィギュレーション モードで使用します。

crl {**required** | **optional** | **nocheck**}

シンタックスの説明

required	必須の CRL は、検証されるピア証明書に対して使用できる必要があります。
optional	必須の CRL が使用できない場合にも、セキュリティ アプライアンスはピア証明書を受け入れることができます。
nocheck	CRL チェックを実行しないようにセキュリティ アプライアンスに指示します。

デフォルト

デフォルト値は、**nocheck** です。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 CA トラストポイント コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、トラストポイント central の暗号 CA トラストポイント コンフィギュレーション モードに入り、CRL がトラストポイント central の検証されるピア証明書に対して使用できることを要求します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl required
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
clear configure crypto ca trustpoint	すべてのトラストポイントを削除します。
crypto ca trustpoint	トラストポイント サブモードに入ります。
crl configure	crl コンフィギュレーション モードに入ります。

crl configure

CRL 設定コンフィギュレーション モードに入るには、**crl configure** コマンドを暗号 CA トラストポイント コンフィギュレーション モードで使用します。

crl configure

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 CA トラストポイント コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、トラストポイント central 内の crl コンフィギュレーション モードに入ります。

```
hostname<config># crypto ca trustpoint central
hostname<ca-trustpoint># crl configure
hostname<ca-crl>#
```

関連コマンド

コマンド	説明
clear configure crypto ca trustpoint	すべてのトラストポイントを削除します。
crypto ca trustpoint	トラストポイント サブモードに入ります。

crypto ca authenticate

トラストポイントに関連付けられた CA 証明書をインストールおよび認証するには、**crypto ca authenticate** コマンドをグローバル コンフィギュレーション モードで使用します。CA 証明書を削除するには、このコマンドの **no** 形式を使用します。

crypto ca authenticate *trustpoint* [**fingerprint** *hexvalue*] [**nointeractive**]

no crypto ca authenticate *trustpoint*

シンタックスの説明

fingerprint	セキュリティ アプライアンスが CA 証明書の認証に使用する、英数字で構成されたハッシュ値を指定します。フィンガープリントが提供されている場合、セキュリティ アプライアンスは CA 証明書の計算されたフィンガープリントと比較し、2 つの値が一致した場合のみその証明書を受け入れます。フィンガープリントがない場合、セキュリティ アプライアンスは計算されたフィンガープリントを表示し、証明書を受け入れるかどうか尋ねます。
hexvalue	フィンガープリントの 16 進値を指定します。
nointeractive	Device Manager 専用の非対話型モードを使用して、このトラストポイントの CA 証明書を取得します。そのとき、フィンガープリントがない場合、セキュリティ アプライアンスは確認せずに証明書を受け入れます。
trustpoint	CA 証明書を取得するトラストポイントを指定します。名前の最大長は 128 文字です。

デフォルト

このコマンドには、デフォルトの動作も値もありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

使用上のガイドライン

トラストポイントが SCEP 登録用に設定されている場合、CA 証明書は SCEP 経由でダウンロードされます。トラストポイントが SCEP 登録用に設定されていない場合、セキュリティ アプライアンスは Base-64 形式の CA 証明書を端末に貼り付けるように要求します。

このコマンドの呼び出しは、実行コンフィギュレーションの一部になりません。

例

次の例では、セキュリティ アプライアンスが CA の証明書を要求します。CA は証明書を送信し、セキュリティ アプライアンスは、管理者に CA 証明書のフィンガープリントをチェックして CA 証明書を確認するように要求します。セキュリティ アプライアンスの管理者は、表示されたフィンガープリントの値を既知の正しい値と照合する必要があります。セキュリティ アプライアンスによって表示されたフィンガープリントが正しい値と一致した場合は、その証明書を有効であるとして受け入れる必要があります。

```
hostname(config)# crypto ca authenticate myca
Certificate has the following attributes:
Fingerprint: 0123 4567 89AB CDEF 0123
Do you accept this certificate? [yes/no] y#
hostname(config)#
```

次の例では、トラストポイント tp9 が端末ベース（手動）の登録用に設定されます。この場合、セキュリティ アプライアンスは管理者に CA 証明書を端末に貼り付けるように要求します。証明書のフィンガープリントを表示した後、セキュリティ アプライアンスは、管理者に証明書が保持されることを確認するように要求します。

```
hostname(config)# crypto ca authenticate tp9
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

MIIDjjCCAvegAwIBAgIQejIaQ3SJRIBMHcvDdgOsKTANBgkqhkiG9w0BAQUFADBA
MQswCQYDVQQGEwJVUzELMAkGA1UECBMCTUExETAPBgNVBAcTCEZyYW5rbGluMREw
DwYDVQQDEwhCcmlhbnNDQTAeFw0wMjEwMTcxODE5MTJaFw0wNjEwMjQxOTU3MDha
MEAxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJNQTERMA8GA1UEBxMIRnJhbmtsaW4x
ETAPBgNVBAMTCEJyaWFuc0NBMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCd
jXEPvNnkZD1bKzahbTHuRot1T8KRUbCP5aWKfqViKJENzI2GnAheArazsAcc4Eaz
LDnpuyyqa0j5LA3MI577MoN1/nll018fbpqOf9eVDPJDkYTvtZ/X3vJgnEjTOWyz
T0pXxhdU1b/jgqVE74OvKBzU7A2yoQ2hMYzwVbGkewIDAQABo4IBhzCCAYMwEwYJ
KwYBBAGCNxQCBAYeBABDAEEwCwYDVR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8w
HQYDVR0OBBYEFBHr3holowFDmniI3FBwKpSEucdtMIIBGwYDVR0fBIIBEjCCAQ4w
gcaggcOggcCGgb1sZGFwOi8vL0NOPUJyaWFuc0NBLENOPWJyaWFuLXcyay1zdnIs
Q049Q0RQLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENO
PUNvbmZpZ3VyYXRpb24sREM9YnJpYW5wZGMsREM9YmRzLERDPWNvbT9jZXJ0aWZp
Y2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Y2xhc3M9Y1JMRGlzdHJpYnV0
aW9uUG9pbnQwQ6BBoD+GPWh0dHA6Ly9icmlhbi13Mmstc3ZyLmJyaWFucGRjLmJk
cy5jb20vQ2VydEVucm9sbC9Ccmlhbnl0NDQS5jcmwwEAYJKwYBBAGCNxUBBAMCAQEw
DQYJKoZIhvcNAQEFBQADgYEAdLhc4Za3AbMjRq66xH1qJWxKUzd4nE9wOrhGgA1r
j4B/Hv2K1gUie34xGqu9OpwqvJgp/vCU12Ciykb1YdSDy/PxN4KtR9Xd1JDQMbu5
f20AYqCG5vpPWavCgmgTLcdwKa3ps1YSWGkhWmScHHSiGg1a3tevYVwhHNPA4mWo
7sQ=

Certificate has the following attributes:
Fingerprint: 21B598D5 4A81F3E5 0B24D12E 3F89C2E4
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ca enroll	CA への登録を開始します。
crypto ca import certificate	手動登録要求への応答として CA から受信した証明書をインストールします。また、PKS12 データをトラストポイントにインポートします。
crypto ca trustpoint	指定したトラストポイントのトラストポイント サブモードに入ります。

crypto ca certificate chain

指定したトラストポイントの証明書チェーン コンフィギュレーション モードに入るには、**crypto ca certificate chain** コマンドをグローバル コンフィギュレーション モードで使用します。グローバル コンフィギュレーション モードに戻るには、このコマンドの **no** 形式を使用するか、**exit** コマンドを使用します。

crypto ca certificate chain *trustpoint*

シンタックスの説明

trustpoint	証明書チェーンを設定するトラストポイントを指定します。

デフォルト

このコマンドにデフォルト値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、トラストポイント central の CA 証明書チェーン サブモードに入ります。

```
hostname<config># crypto ca certificate chain central
hostname<config-cert-chain>#
```

関連コマンド

コマンド	説明
clear configure crypto ca trustpoint	すべてのトラストポイントを削除します。

crypto ca certificate map

CA 証明書マップ モードに入るには、**crypto ca configuration map** コマンドをグローバル コンフィギュレーション モードで使用します。このコマンドを実行すると、CA 証明書マップ モードに入ります。証明書マッピング規則の優先順位付きリストを管理するには、このコマンドのグループを使用します。マッピング規則の順序はシーケンス番号によって決まります。

暗号 CA 証明書マップ規則を削除するには、このコマンドの **no** 形式を使用します。

crypto ca certificate map *sequence-number*

no crypto ca certificate map [*sequence-number*]

シンタックスの説明

sequence-number	作成する証明書マップ規則の番号を指定します。範囲は 1 ～ 65535 です。トンネルグループを証明書マップ規則にマッピングする tunnel-group-map を作成するときに、この番号を使用できます。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを発行すると、セキュリティ アプライアンスは CA 証明書マップ コンフィギュレーション モードになります。このモードでは、証明書の発行者名およびサブジェクト認定者名（DN）に基づいて規則を設定できます。これらの規則の一般的な形式は次のとおりです。

DN match-criteria match-value

DN は、*subject-name* または *issuer-name* のいずれかです。DN は、ITU-T X.509 標準で定義されています。証明書フィールドのリストについては、関連コマンドを参照してください。

match-criteria は、次の表現または演算子で構成されます。

attr *tag*	比較を通常名（CN）などの特定の DN アトリビュートに制限します。
co	含む
eq	等しい
nc	含まない
ne	等しくない

DN の一致表現では大文字と小文字が区別されません。

例

次の例では、シーケンス番号 1（規則番号 1）の CA 証明書マップ モードに入り、subject-name の通常名（CN）アトリビュートが Pat と一致する必要があることを指定します。

```
hostname(config)# crypto ca certificate map 1
hostname(ca-certificate-map)# subject-name attr cn eq pat
hostname(ca-certificate-map)#
```

次の例では、シーケンス番号 1 の CA 証明書マップ モードに入り、subject-name 内のどこかに値 cisco が含まれることを指定します。

```
hostname(config)# crypto ca certificate map 1
hostname(ca-certificate-map)# subject-name co cisco
hostname(ca-certificate-map)#
```

関連コマンド

コマンド	説明
issuer-name	規則エントリが IPSec ピア証明書の発行者 DN に適用されることを指定します。
subject-name（crypto ca certificate map）	規則エントリが IPSec ピア証明書のサブジェクト DN に適用されることを指定します。
tunnel-group-map enable	**crypto ca certificate map** コマンドで作成された証明書マップ エントリをトンネルグループに関連付けます。

crypto ca crl request

指定したトラストポイントのコンフィギュレーション パラメータに基づいて CRL を要求するには、**crypto ca crl request** コマンドを暗号 CA トラストポイント コンフィギュレーション モードで使用します。

crypto ca crl request *trustpoint*

シンタックスの説明

trustpoint	トラストポイントを指定します。最大文字数は 128 です。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 CA トラストポイント コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドの呼び出しは、実行コンフィギュレーションの一部になりません。

例

次の例では、central という名前のトラストポイントに基づいて CRL を要求します。

```
hostname(config)# crypto ca crl request central
hostname(config)#
```

関連コマンド

コマンド	説明
crl configure	crl 設定モードに入ります。

crypto ca enroll

CA との登録プロセスを開始するには、**crypto ca enroll** コマンドをグローバル コンフィギュレーション モードで使用します。このコマンドが正常に実行されるには、トラストポイントが正しく設定されている必要があります。

crypto ca enroll *trustpoint* [**noconfirm**]

シンタックスの説明

noconfirm	（オプション）すべてのプロンプトを表示しないようにします。要求されている場合がある登録オプションは、トラストポイントに事前設定されている必要があります。このオプションは、スクリプト、ASDM、または他の非対話型で使用するためのものです。
trustpoint	登録に使用するトラストポイントの名前を指定します。最大文字数は 128 です。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

トラストポイントが SCEP 登録用に設定されている場合、セキュリティ アプライアンスはただちに CLI プロンプトを表示し、コンソールへのステータス メッセージを非同期的に表示します。トラストポイントが手動登録用に設定されている場合、セキュリティ アプライアンスは Base-64 符号化 PKCS10 認証要求をコンソールに書き込んでから、CLI プロンプトを表示します。

このコマンドは、参照されるトラストポイントの設定された状態に応じて異なる対話型のプロンプトを生成します。

例

次の例では、SCEP 登録を使用して、トラストポイント tp1 で識別証明書を登録します。セキュリティ アプライアンスは、トラストポイント コンフィギュレーションで保存されていない情報を要求します。

```
hostname(config)# crypto ca enroll tp1
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
% password to the CA Administrator in order to revoke your certificate.
% For security reasons your password will not be saved in the configuration.
% Please make a note of it.
Password:
Re-enter password:
% The fully-qualified domain name in the certificate will be: xyz.example.com
% The subject name in the certificate will be: xyz.example.com
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA [yes/no]: yes
% Certificate request sent to Certificate authority.
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the fingerprint.

hostname(config)#
```

次のコマンドは、CA 証明書の手動登録を示しています。

```
hostname(config)# crypto ca enroll tp1
% Start certificate enrollment ..
% The fully-qualified domain name in the certificate will be: xyz.example.com
% The subject name in the certificate will be: wb-2600-3.example.com
if serial number not set in trustpoint, prompt:
% Include the router serial number in the subject name? [yes/no]: no
If ip-address not configured in trustpoint:
% Include an IP address in the subject name? [no]: yes
Enter Interface name or IP Address[]: 1.2.3.4
Display Certificate Request to terminal? [yes/no]: y
Certificate Request follows:
MIIBFTCBwAIBADA6MTgwFAYJKoZIhvcNAQkIEwcxLjIuMy40MCAGCSqGSIb3DQEJ
AhYTd2ItMjYwMC0zLmNpc2NvLmNvbTBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQDT
IdvHa4D5wXZ+40sKQV7Uek1E+CC6hm/LRN3p5ULW1KF6bxhA3Q5CQfh4jDxobn+A
Y8GoeceulS2Zb+mvgNvjAgMBAAGgITAfBgkqhkiG9w0BCQ4xEjAQMA4GA1UdDwEB
/wQEAwIFoDANBgkqhkiG9w0BAQQFAANBACDhnrEGBVtltG7hp8x6Wz/dgY+ouWcA
lzy7QpdGhb1du2P81RYn+8pWRA43cikXMTeM4ykEkZhLjDUgv9t+R9c=

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]: no
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ca authenticate	このトラストポイントの CA 証明書を取得します。
crypto ca import pkcs12	手動登録要求への応答として CA から受信した証明書をインストールします。また、PKS12 データをトラストポイントにインポートします。
crypto ca trustpoint	指定したトラストポイントのトラストポイント サブモードに入ります。

crypto ca export

トラストポイント コンフィギュレーションに関連付けられたキーと証明書を PKCS12 形式でエクスポートするには、**crypto ca export** コマンドをグローバル コンフィギュレーション モードで使用します。

crypto ca export *trustpoint* ***pkcs12*** *passphrase*

シンタックスの説明

passphrase	エクスポートする PKCS12 ファイルの暗号化に使用するパスフレーズを指定します。
pkcs12	トラストポイント コンフィギュレーションのエクスポートに使用する公開キー暗号化標準を指定します。
trustpoint	証明書とキーをエクスポートするトラストポイントの名前を指定します。エクスポート時にトラストポイントが RSA キーを使用する場合、エクスポートされるキー ペアはトラストポイントと同じ名前を割り当てられます。

デフォルト

このコマンドにデフォルト値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドの呼び出しは、アクティブなコンフィギュレーションの一部になりません。PKCS12 データは端末に書き込まれます。

例

次の例では、xxyyzz をパスコードとして使用して、トラストポイント central の PKCS12 データをエクスポートします。

```
hostname (config)# crypto ca export central pkcs12 xxyyzz

Exported pkcs12 follows:

[ PKCS12 data omitted ]

---End - This line not part of the pkcs12---

hostname (config)#
```

関連コマンド

コマンド	説明
crypto ca import pkcs12	手動登録要求への応答として CA から受信した証明書をインストールします。また、PKS12 データをトラストポイントにインポートします。
crypto ca authenticate	このトラストポイントの CA 証明書を取得します。
crypto ca enroll	CA への登録を開始します。
crypto ca trustpoint	指定したトラストポイントのトラストポイント サブモードに入ります。

crypto ca import

手動登録要求への応答で CA から受信した証明書をインストール、または PKCS12 データを使用してトラストポイントの証明書とキー ペアをインポートするには、**crypto ca import** コマンドをグローバル コンフィギュレーション モードで使用します。セキュリティ アプライアンスは、Base-64 形式で端末にテキストを貼り付けるように要求します。

crypto ca import *trustpoint* **certificate** [**nointeractive**]

crypto ca import *trustpoint* **pkcs12** *passphrase* [**nointeractive**]

シンタックスの説明

trustpoint	インポート アクションを関連付けるトラストポイントを指定します。最大文字数は 128 です。PKCS12 データをインポートし、トラストポイントが RSA キーを使用する場合、インポートされるキー ペアはトラストポイントと同じ名前を割り当てられます。
certificate	セキュリティ アプライアンスに、トラストポイントによって示される CA から証明書をインポートするように指示します。
pkcs12	セキュリティ アプライアンスに、PKCS12 形式を使用してトラストポイントの証明書とキー ペアをインポートするように指示します。
passphrase	PKCS12 データの暗号解除に使用するパスフレーズを指定します。
nointeractive	（オプション）非対話型モードを使用して証明書をインポートします。プロンプトをすべて表示しません。このオプションは、スクリプト、ASDM、または他の非対話型で使用するためのものです。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次の例では、トラストポイント Main の証明書を手動でインポートします。

```
hostname (config)# crypto ca import Main certificate
% The fully-qualified domain name in the certificate will be:
securityappliance.example.com

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself
[ certificate data omitted ]
quit
INFO: Certificate successfully imported
hostname (config)#
```

次の例では、PKCS12 データをトラストポイント central に手動でインポートします。

```
hostname (config)# crypto ca import central pkcs12

Enter the base 64 encoded pkcs12.
End with a blank line or the word "quit" on a line by itself:
[ PKCS12 data omitted ]
quit
INFO: Import PKCS12 operation completed successfully
hostname (config)#
```

関連コマンド

コマンド	説明
crypto ca export	トラストポイントの証明書とキー ペアを PKCS12 形式でエクスポートします。
crypto ca authenticate	トラストポイントの CA 証明書を取得します。
crypto ca enroll	CA への登録を開始します。
crypto ca trustpoint	指定したトラストポイントのトラストポイント サブモードに入ります。

crypto ca trustpoint

指定したトラストポイントのトラストポイント サブモードに入るには、**crypto ca trustpoint** コマンドをグローバル コンフィギュレーション モードで使用します。指定したトラストポイ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。このコマンドはトラストポイント情報を管理します。トラストポイントは、CA によって発行された証明書に基づいて CA の識別情報を表し、また、装置の識別情報を表すことがあります。トラストポイント サブモード内のコマンドは、CA 固有のコンフィギュレーション パラメータを制御します。このパラメータでは、セキュリティ アプライアンスが CA 証明書を取得する方法、セキュリティ アプライアンスが CA から証明書を取得する方法、および CA によって発行されるユーザ証明書の認証ポリシーを指定します。

crypto ca trustpoint *trustpoint-name*

no crypto ca trustpoint *trustpoint-name* [**noconfirm/**

シンタックスの説明

noconfirm	対話型のプロンプトをすべて表示しません。
trustpoint- name	管理するトラストポイントの名前を指定します。名前の最大長は 128 文字です。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

CA を宣言するには、**crypto ca trustpoint** コマンドを使用します。このコマンドを発行すると、暗号 CA トラストポイント コンフィギュレーション モードに入ります。

このマニュアルにアルファベット順に記載されている次のコマンドを使用して、トラストポイントの特性を指定できます。

- **crl required | optional | nocheck**：CRL コンフィギュレーション オプションを指定します。
- **crl configure**：CRL コンフィギュレーション サブモードに入ります（**crl** を参照）。
- **default enrollment**：すべての登録パラメータをシステム デフォルト値に戻します。このコマンドの呼び出しは、アクティブなコンフィギュレーションの一部になりません。
- **enrollment retry period**：自動（SCEP）登録のリトライ期間を分単位で指定します。
- **enrollment retry count**：自動（SCEP）登録の許可されるリトライの最大回数を指定します。
- **enrollment terminal**：このトラストポイントを使用したカット アンド ペースト登録を指定します。

- **enrollment url** *url*：このトラストポイントを使用して登録する自動登録（SCEP）を指定し、登録 URL（*url*）を設定します。
- **fqdn** *fqdn*：登録中に、指定した完全修飾認定者名（FQDN）を証明書のサブジェクト代替名の拡張に含めるかどうかを CA に確認します。
- **email** *address*：登録中に、指定した電子メール アドレスを証明書のサブジェクト代替名の拡張に含めるかどうかを CA に確認します。
- **subject-name** *X.500 name*：登録中に、指定したサブジェクト DN を証明書に含めるかどうかを CA に確認します。
- **serial-number**：登録中に、セキュリティ アプライアンスのシリアル番号を証明書に含めるかどうかを CA に確認します。
- **ip-addr** *ip-address*：登録中に、セキュリティ アプライアンスの IP アドレスを証明書に含めるかどうかを CA に確認します。
- **password** *string*：登録中に CA に登録されるチャレンジ フレーズを指定します。CA は、通常、このフレーズを使用して、その後の失効要求を認証します。
- **keypair** *name*：公開キーを認証するキー ペアを指定します。
- **id-cert-issuer**：このトラストポイントに関連付けられた CA によって発行されるピア証明書をシステムが受け入れるかどうかを指定します。
- **accept-subordinates**：トラストポイントに関連付けられた CA に従属する CA 証明書が、装置にインストールされていない場合にフェーズ 1 の IKE 交換中に提供されたときに受け入れるかどうかを指定します。
- **support-user-cert-validation**：イネーブルにした場合、トラストポイントがリモート証明書を発行した CA に対して認証されていれば、リモート ユーザ証明書を検証するコンフィギュレーション設定はこのトラストポイントから取得できます。このオプションは、サブコマンド **crl required | optional | nocheck** および CRL サブモードのすべての設定に関連付けられたコンフィギュレーション データに適用されます。
- **exit**：サブモードを終了します。

例

次の例では、central という名前のトラストポイントを管理するための CA トラストポイント モードに入ります。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
clear configure crypto ca trustpoint	すべてのトラストポイントを削除します。
crypto ca authenticate	このトラストポイントの CA 証明書を取得します。
crypto ca certificate map	暗号 CA 証明書マップ モードに入ります。証明書ベースの ACL を定義します。
crypto ca crl request	指定したトラストポイントのコンフィギュレーション パラメータに基づいて、CRL を要求します。
crypto ca import	手動登録要求への応答として CA から受信した証明書をインストールします。また、PKS12 データをトラストポイントにインポートします。

crypto dynamic-map match address

このコマンドの詳細については、crypto map match address コマンドを参照してください。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **match address** *acl_name*

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **match address** *acl_name*

シンタックスの説明

acl-name	ダイナミック暗号マップ エントリに一致させるアクセスリストを指定します。
dynamic-map-name	ダイナミック暗号マップ セットの名前を指定します。
dynamic-seq-num	ダイナミック暗号マップ エントリに対応するシーケンス番号を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

例

次の例では、aclist1 という名前のアクセスリストのアドレスに一致させる crypto dynamic-map コマンドの使用方法を示します。

```
hostname(config)# crypto dynamic-map mymap 10 match address aclist1
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	すべてのダイナミック暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto dynamic-map	すべてのダイナミック暗号マップのすべてのコンフィギュレーションを表示します。

crypto dynamic-map set nat-t-disable

接続の NAT-T をこの暗号マップ エントリに基づいてディセーブルにするには、**crypto dynamic-map set nat-t-disable** コマンドをグローバル コンフィギュレーション モードで使用します。この暗号マップ エントリの NAT-T をイネーブルにするには、このコマンドの **no** 形式を使用します。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set nat-t-disable**

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set nat-t-disable**

シンタックスの説明

dynamic-map-name	ダイナミック暗号マップ セットの名前を指定します。
dynamic-seq-num	ダイナミック暗号マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルト設定はオフです。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

NAT-T をグローバルにイネーブルにするには、**isakmp nat-traversal** コマンドを使用します。その後、**crypto dynamic-map set nat-t-disable** コマンドを使用して、特定の暗号マップ エントリの NAT-T をディセーブルにできます。

例

次のコマンドは、mymap という名前のダイナミック暗号マップの NAT-T をディセーブルにします。

```
hostname(config)# crypto dynamic-map mymap 10 set nat-t-disable
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	すべてのダイナミック暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto dynamic-map	すべてのダイナミック暗号マップのすべてのコンフィギュレーションを表示します。

crypto dynamic-map set peer

このコマンドの詳細については、**crypto map set peer** コマンドを参照してください。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set peer** *ip_address* | *hostname*

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set peer** *ip_address* | *hostname*

シンタックスの説明

dynamic-map-name	ダイナミック暗号マップ セットの名前を指定します。
dynamic-seq-num	ダイナミック暗号マップ エントリに対応するシーケンス番号を指定します。
ip_address	**name** コマンドで定義されているように、ダイナミック暗号マップ エントリのピアを IP アドレスで指定します。
hostname	**name** コマンドで定義されているように、ダイナミック暗号マップ エントリのピアをホスト名で指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

例

次の例では、mymap という名前のダイナミック マップのピアを IP アドレス 10.0.0.1 に設定します。

```
hostname(config)# crypto dynamic-map mymap 10 set peer 10.0.0.1
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	すべてのダイナミック暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto dynamic-map	すべてのダイナミック暗号マップのすべてのコンフィギュレーションを表示します。

crypto dynamic-map set pfs

このコマンドの詳細については、**crypto map set pfs** コマンドを参照してください。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set pfs [group1 | group2 | group5 | group 7]**

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set pfs [group1 | group2 | group5 | group 7]**

シンタックスの説明

dynamic-map-name	ダイナミック暗号マップ セットの名前を指定します。
dynamic-seq-num	ダイナミック暗号マップ エントリに対応するシーケンス番号を指定します。
group1	IPSec で新しい Diffie-Hellman 交換を実行するときに、768 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group2	IPSec で新しい Diffie-Hellman 交換を実行するときに、1024 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group5	IPSec で新しい Diffie-Hellman 交換を実行するときに、1536 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group7	IPSec が、たとえば movianVPN クライアントで、楕円曲線フィールドのサイズが 163 ビットである group7（ECC）を使用するように指定します。
set pfs	このダイナミック暗号マップ エントリ用の新しいセキュリティ アソシエーションを要求するときに、PFS（perfect forward secrecy; 完全転送秘密）を要求するように IPSec を設定します。また、新しいセキュリティ アソシエーションの要求を受信したときに PFS を要求するように IPSec を設定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが変更され、Diffie-Hellman group 7 が追加されました。

使用上のガイドライン

crypto dynamic-map コマンド（**match address**、**set peer**、**set pfs** など）については、**crypto map** コマンドの項で説明します。ピアがネゴシエーションを開始するときに、ローカル コンフィギュレーションで PFS が指定されている場合、ピアは PFS 交換を実行する必要があります。実行しない場合は、ネゴシエーションに失敗します。ローカル コンフィギュレーションでグループが指定されていない場合、セキュリティ アプライアンスはデフォルトの group2 が指定されているものと見なします。ローカル コンフィギュレーションで PFS が指定されていない場合は、ピアからの PFS のオファーがすべて受け入れられます。

セキュリティ アプライアンスは、Cisco VPN Client と対話するときに PFS 値を使用しません。その代わり、フェーズ 1 でネゴシエートされた値を使用します。

例

次の例では、ダイナミック暗号マップ mymap 10 用の新しいセキュリティ アソシエーションをネゴシエートするときに、必ず PFS を使用することを指定します。指定されたグループはグループ 2 です。

```
hostname(config)# crypto dynamic-map mymap 10 set pfs group2
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	すべてのダイナミック暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto dynamic-map	すべてのダイナミック暗号マップのすべてのコンフィギュレーションを表示します。

crypto dynamic-map set reverse route

このコマンドの詳細については、crypto map set reverse-route コマンドを参照してください。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set reverse route**

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set reverse route**

シンタックスの説明

dynamic-map-name	暗号マップ セットの名前を指定します。
dynamic-seq-num	暗号マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトでは、このコマンドの値はオフになっています。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

次のコマンドは、mymap という名前のダイナミック暗号マップの RRI をイネーブルにします。

```
hostname(config)# crypto dynamic-map mymap 10 set reverse route
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	すべてのダイナミック暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto dynamic-map	すべてのダイナミック暗号マップのすべてのコンフィギュレーションを表示します。

crypto dynamic-map set security-association lifetime

このコマンドの詳細については、**crypto map set security-association lifetime** コマンドを参照してください。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set security-association lifetime seconds** *seconds* | **kilobytes** *kilobytes*

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set security-association lifetime seconds** *seconds* | **kilobytes** *kilobytes*

シンタックスの説明

dynamic-map-name	ダイナミック暗号マップ セットの名前を指定します。
dynamic-seq-num	ダイナミック暗号マップ エントリに対応するシーケンス番号を指定します。
kilobytes	所定のセキュリティ アソシエーションの有効期限が切れるまでに、そのセキュリティ アソシエーションを使用してピア間を通過できるトラフィックの量を KB 単位で指定します。デフォルトは 4,608,000 KB です。
seconds	セキュリティ アソシエーションの有効期限が切れるまでの存続時間（秒数）を指定します。デフォルトは 28,800 秒（8 時間）です。

デフォルト

デフォルトの KB 数は 4,608,000 で、デフォルトの秒数は 28,800 です。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

例

次のコマンドは、ダイナミック暗号マップ mymap のセキュリティ アソシエーションのライフタイムを秒単位で指定します。

```
hostname(config)# crypto dynamic-map mymap 10 set security-association lifetime
seconds 1400
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	すべてのダイナミック暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto dynamic-map	すべてのダイナミック暗号マップのすべてのコンフィギュレーションを表示します。

crypto dynamic-map set transform-set

このコマンドの詳細については、**crypto map set transform-set** コマンドを参照してください。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set transform-set** *transform-set-name1* [*… transform-set-name9*]

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set transform-set** *transform-set-name1* [*… transform-set-name9*]

シンタックスの説明

dynamic-map-name	ダイナミック暗号マップ セットの名前を指定します。
dynamic-seq-num	ダイナミック暗号マップ エントリに対応するシーケンス番号を指定します。
transform-set-name1 *transform-set-name9*	ダイナミック暗号マップ エントリで使用するトランスフォーム セット（**crypto ipsec** コマンドを使用して定義されたトランスフォーム セットの名前）を指定します。

（注）　**crypto map set transform-set** コマンドは、ダイナミック暗号マップ エントリを使用する場合に必須となるコマンドです。このエントリで必要なものは、トランスフォーム セットだけです。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

例

次のコマンドは、ダイナミック暗号マップ mymap に 2 つのトランスフォーム セット（tfset1 および tfset2）を指定しています。

```
hostname(config)# crypto dynamic-map mymap 10 set transform-set tfset1 tfset2
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	すべてのダイナミック暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto dynamic-map	すべてのダイナミック暗号マップのすべてのコンフィギュレーションを表示します。

crypto map set security-association lifetime

特定の暗号マップ エントリについて、IPSec セキュリティ アソシエーションをネゴシエートするときに使用されるグローバル ライフタイム値を上書きするには、グローバル コンフィギュレーション モードで **crypto map set security-association lifetime** コマンドを使用します。暗号マップ エントリのライフタイム値をグローバル値にリセットするには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set security-association lifetime {seconds** *seconds* | **kilobytes** *kilobytes*}

no crypto map *map-name seq-num* **set security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes*}

シンタックスの説明

kilobytes	所定のセキュリティ アソシエーションの有効期限が切れるまでに、そのセキュリティ アソシエーションを使用してピア間を通過できるトラフィックの量を KB 単位で指定します。 デフォルトは 4,608,000 KB です。
map-name	暗号マップ セットの名前を指定します。
seconds	セキュリティ アソシエーションの有効期限が切れるまでの存続時間（秒数）を指定します。デフォルトは 28,800 秒（8 時間）です。
seq-num	暗号マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトの KB 数は 4,608,000 で、デフォルトの秒数は 28,800 です。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

暗号マップのセキュリティ アソシエーションは、グローバル ライフタイム値に基づいてネゴシエートされます。

IPSec セキュリティ アソシエーションでは、共有秘密鍵を使用します。これらの鍵とセキュリティ アソシエーションは、両方同時にタイムアウトします。

個々の暗号マップ エントリでライフタイム値が設定されている場合は、セキュリティ アソシエーションのネゴシエート中に新しいセキュリティ アソシエーションを要求するとき、セキュリティ アプライアンスは、ピアへの要求の中でこの暗号マップ ライフタイム値を利用します。この値を、新しいセキュリティ アソシエーションのライフタイムとして使用します。セキュリティ アプライアンスは、ピアからネゴシエーション要求を受信すると、ピアが指定するライフタイム値またはローカルに設定済みのライフタイム値のうち、小さい方を新しいセキュリティ アソシエーションのライフタイムとして使用します。

ライフタイムには、期間を指定するものとトラフィック量を指定するものの 2 つがあります。セッション キーとセキュリティ アソシエーションは、いずれかのライフタイムに最初に到達した時点で期限切れになります。1 つのコマンドで両方を指定できます。

（注）　セキュリティ アプライアンスでは、暗号マップ、ダイナミック マップ、および ipsec 設定をその場で変更できます。これを行う場合は、変更によって影響を受ける接続だけがセキュリティ アプライアンスによって停止させられます。特に、アクセスリスト内のエントリを削除することによって、暗号マップに関連付けられている既存のアクセスリストを変更する場合は、関連する接続だけが停止させられます。アクセスリスト内の他のエントリに基づく接続は、影響を受けません。

期間ライフタイムを変更するには、**crypto map set security-association lifetime seconds** コマンドを使用します。期間ライフタイムを使用する場合は、指定した秒数が経過した時点でキーおよびセキュリティ アソシエーションがタイムアウトします。

例

グローバル コンフィギュレーション モードで次のコマンドを入力すると、暗号マップ mymap のセキュリティ アソシエーション ライフタイムが秒単位および KB 単位で指定されます。

```
hostname(config)# crypto map mymap 10 set security-association lifetime seconds 1400
kilobytes 3000000
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべての暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。

crypto dynamic-map set transform-set

このコマンドの詳細については、**crypto map set transform-set** コマンドを参照してください。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set transform-set** *transform-set-name1* [*… transform-set-name9*]

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set transform-set** *transform-set-name1* [*… transform-set-name9*]

シンタックスの説明

dynamic-map-name	ダイナミック暗号マップ セットの名前を指定します。
dynamic-seq-num	ダイナミック暗号マップ エントリに対応するシーケンス番号を指定します。
transform-set-name1 *transform-set-name9*	ダイナミック暗号マップ エントリで使用するトランスフォーム セット（**crypto ipsec** コマンドを使用して定義されたトランスフォーム セットの名前）を指定します。

（注）　**crypto map set transform-set** コマンドは、ダイナミック暗号マップ エントリを使用する場合に必須となるコマンドです。このエントリで必要なものは、トランスフォーム セットだけです。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

例

次のコマンドは、ダイナミック暗号マップ mymap に 2 つのトランスフォーム セット（tfset1 および tfset2）を指定しています。

```
hostname(config)# crypto dynamic-map mymap 10 set transform-set tfset1 tfset2
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	すべてのダイナミック暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto dynamic-map	すべてのダイナミック暗号マップのすべてのコンフィギュレーションを表示します。

crypto ipsec df-bit

IPSec パケットの DF ビット ポリシーを設定するには、**crypto ipsec df-bit** コマンドをグローバル コンフィギュレーション モードで使用します。

crypto ipsec df-bit [**clear-df** | **copy-df** | **set-df**] *interface*

シンタックスの説明

clear-df	（オプション）外部 IP ヘッダーは DF ビットを消去されること、およびセキュリティ アプライアンスはパケットをフラグメント化して IPSec カプセル化を追加する場合があることを指定します。
copy-df	（オプション）セキュリティ アプライアンスが外部 DF ビット設定を元のパケット内で探すことを指定します。
set-df	（オプション）外部 IP ヘッダーに DF ビットを設定することを指定します。ただし、元のパケットで DF ビットが消去されている場合、セキュリティ アプライアンスはパケットをフラグメント化することがあります。
interface	インターフェイス名を指定します。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。設定を指定せずにこのコマンドをイネーブルにした場合、セキュリティ アプライアンスはデフォルトとして ***copy-df*** 設定を使用します。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

IPSec トンネル機能がある DF ビットを使用すると、セキュリティ アプライアンスがカプセル化されたヘッダーから Don’t Fragment（DF）ビットを消去、設定、またはコピーできるかどうかを指定できます。IP ヘッダー内の DF ビットにより、装置がパケットをフラグメント化できるかどうかが決定されます。

カプセル化されたヘッダー内の DF ビットを指定するようにセキュリティ アプライアンスを設定するには、**crypto *ipsec df-bit*** コマンドをグローバル コンフィギュレーション モードで使用します。

トンネル モードの IPSec トラフィックをカプセル化する場合は、DF ビットの ***clear-df*** 設定を使用します。この設定を使用すると、装置は使用可能な MTU のサイズよりも大きなパケットを送信できます。また、この設定は、使用可能な MTU のサイズが不明な場合にも適しています。

例

グローバル コンフィギュレーション モードで入力した次の例では、IPSec DF ポリシーを **clear-df** に設定するよう指定します。

```
hostname(config)# crypto ipsec df-bit clear-df inside
hostname(config)#
```

関連コマンド

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

crypto ipsec fragmentation

IPSec パケットのフラグメンテーション ポリシーを設定するには、**crypto ipsec fragmentation** コマンドをグローバル コンフィギュレーション モードで使用します。

crypto ipsec fragmentation {**after-encryption** | **before-encryption**} *interface*

シンタックスの説明

after-encryption	暗号化の後で MTU の最大サイズに近い IPSec パケットをフラグメント化するようにセキュリティ アプライアンスに指定します(事前フラグメント化をディセーブルにします)。
before-encryption	暗号化の前に MTU の最大サイズに近い IPSec パケットをフラグメント化するようにセキュリティ アプライアンスに指定します(事前フラグメント化をイネーブルにします)。
interface	インターフェイス名を指定します。

デフォルト

この機能はデフォルトでイネーブルになっています。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

暗号化するセキュリティ アプライアンスの発信リンクの MTU のサイズにパケットのサイズが近く、IPSec ヘッダーでカプセル化される場合、発信リンクの MTU を超える可能性があります。MTU のサイズを超えると暗号化の後にパケットがフラグメント化され、このため暗号解除装置がプロセス パスで再組み立てされます。IPSec VPN の事前フラグメント化では、暗号解除装置はプロセス パスではなく高性能な CEF パスで動作するため、パフォーマンスが向上します。

IPSec VPN の事前フラグメント化では、暗号化装置は、IPSec SA の一部として設定されたトランスフォーム セットで使用可能な情報から、カプセル化されたパケット サイズを事前に設定します。装置でパケットが出力インターフェイスの MTU を超えることが事前に設定されている場合、装置は暗号化する前にそのパケットをフラグメント化します。これにより、暗号解除前のプロセス レベルの再組み立てが回避され、暗号解除のパフォーマンスおよび全体的な IPsec トラフィックのスループットの向上に役立ちます。

例

グローバル コンフィギュレーション モードで入力した次の例では、IPSec パケットの事前フラグメント化を装置上でグローバルにイネーブルにします。

```
hostname(config)# crypto ipsec fragmentation before-encryption inside
hostname(config)#
```

グローバル コンフィギュレーション モードで入力した次の例では、IPSec パケットの事前フラグメント化をインターフェイス上でディセーブルにします。

```
hostname(config)# crypto ipsec fragmentation after-encryption inside
hostname(config)#
```

関連コマンド

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

crypto ipsec security-association lifetime

グローバル ライフタイム値を設定するには、**crypto ipsec security-association lifetime** コマンドをグローバル コンフィギュレーション モードで使用します。crypto ipsec エントリのライフタイム値をデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

crypto ipsec security-association lifetime {**seconds** *seconds* | **kilobytes** *kilobytes*}

no crypto ipsec security-association lifetime {**seconds** *seconds* | **kilobytes** *kilobytes*}

シンタックスの説明

kilobytes	所定のセキュリティ アソシエーションの有効期限が切れるまでに、そのセキュリティ アソシエーションを使用してピア間を通過できるトラフィックの量を KB 単位で指定します。範囲は 10 ～ 2,147,483,647 KB です。デフォルトは 4,608,000 KB です。
seconds	セキュリティ アソシエーションの有効期限が切れるまでの存続時間（秒数）を指定します。範囲は 120 ～ 214,783,647 秒です。デフォルトは 28,800 秒（8 時間）です。
token	ユーザ認証にトークン ベースのサーバを使用することを指定します。

デフォルト

デフォルトの KB 数は 4,608,000 で、デフォルトの秒数は 28,800 です。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが導入されました。

使用上のガイドライン

crypto ipsec security-association lifetime コマンドは、IPSec セキュリティ アソシエーションのネゴシエート時に使用されるグローバル ライフタイム値を変更します。

IPSec セキュリティ アソシエーションでは、共有秘密鍵を使用します。これらの鍵とセキュリティ アソシエーションは、両方同時にタイムアウトします。

個々の暗号マップ エントリでライフタイム値が設定されていない場合は、セキュリティ アソシエーションのネゴシエート中に新しいセキュリティ アソシエーションを要求するとき、セキュリティ アプライアンスは、ピアへの要求の中でグローバル ライフタイム値を指定します。この値を、新しいセキュリティ アソシエーションのライフタイムとして使用します。セキュリティ アプライアンスは、ピアからネゴシエーション要求を受信すると、ピアが指定するライフタイム値またはローカルに設定済みのライフタイム値のうち、小さい方を新しいセキュリティ アソシエーションのライフタイムとして使用します。

ライフタイムには、期間を指定するものとトラフィック量を指定するものの 2 つがあります。セキュリティ アソシエーションは、いずれかのライフタイムに最初に到達した時点で期限切れになります。

セキュリティ アプライアンスでは、暗号マップ、ダイナミック マップ、および ipsec 設定をその場で変更できます。これを行う場合は、変更によって影響を受ける接続だけがセキュリティ アプライアンスによって停止させられます。特に、アクセスリスト内のエントリを削除することによって、暗号マップに関連付けられている既存のアクセスリストを変更する場合は、関連する接続だけが停止させられます。アクセスリスト内の他のエントリに基づく接続は、影響を受けません。

グローバル期間ライフタイムを変更するには、**crypto ipsec security-association lifetime seconds** コマンドを使用します。期間ライフタイムを使用する場合は、指定した秒数が経過した時点でセキュリティ アソシエーションがタイムアウトします。

グローバル トラフィック量ライフタイムを変更するには、**crypto ipsec security-association lifetime kilobytes** コマンドを使用します。トラフィック量ライフタイムを使用する場合は、指定した量のトラフィック（KB 単位）がセキュリティ アソシエーション キーによって保護された時点で、セキュリティ アソシエーションがタイムアウトします。

ライフタイムを短くするほど、攻撃者がキー再現攻撃を成功させることが困難になります。攻撃者にとっては、解析の対象となる、同じキーで暗号化されたデータの量が少なくなるためです。ただし、ライフタイムを短くするほど、新しいセキュリティ アソシエーションの確立にかかる CPU 処理時間が長くなります。

セキュリティ アソシエーション（およびそれに対応するキー）は、指定した秒数または指定したトラフィック量（KB 単位）のうち、どちらかを超えた時点で有効期限が切れます。

例

次の例では、セキュリティ アソシエーションのグローバル期間ライフタイムを指定します。

```
hostname(config)# crypto ipsec-security association lifetime seconds 240
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべての IPSec コンフィギュレーション（たとえば、グローバル ライフタイムやトランスフォーム セット）を消去します。
show running-config crypto map	すべての暗号マップのすべてのコンフィギュレーションを表示します。

crypto ipsec transform-set

トランスフォーム セットを定義するには、**crypto ipsec transform-set** コマンドをグローバル コンフィギュレーション モードで使用します。このコマンドを使用すると、トランスフォーム セットで使用される IPSec 暗号化およびハッシュ アルゴリズムを指定できます。トランスフォーム セットを削除するには、このコマンドの **no** 形式を使用します。

crypto ipsec *map-name seq-num* **transform-set** *transform-set-name transform1 [transform2]*

no crypto ipsec *map-name seq-num* **transform-set** *transform-set-name*

シンタックスの説明

esp-aes	このトランスフォームによって保護される IPSec メッセージが、AES を使用して 128 ビット キーで暗号化されます。
esp-aes-192	このトランスフォームによって保護される IPSec メッセージが、AES を使用して 192 ビット キーで暗号化されます。
esp-aes-256	このトランスフォームによって保護される IPSec メッセージが、AES を使用して 256 ビット キーで暗号化されます。
esp-des	このトランスフォームによって保護される IPSec メッセージが、56 ビット DES-CBC を使用して暗号化されます。
esp-3des	このトランスフォームによって保護される IPSec メッセージが、Triple DES アルゴリズムを使用して暗号化されます。
esp-none	IPSec メッセージが HMAC 認証を使用しません。
esp-null	IPSec メッセージが IPSec セキュリティ プロトコル（ESP）だけを使用して暗号化されることはありません。
esp-md5-hmac	このトランスフォームによって保護される IPSec メッセージが、ハッシュ アルゴリズムとして MD5/HMAC-128 を使用します。
esp-sha-hmac	このトランスフォームによって保護される IPSec メッセージが、ハッシュ アルゴリズムとして SHA/HMAC-160 を使用します。
map-name	暗号マップ セットの名前を指定します。
seq-num	暗号マップ エントリに割り当てる番号を指定します。
transform1, transform2	トランスフォームを 2 つまで指定します。トランスフォームは、IPSec のセキュリティ プロトコルとアルゴリズムを定義するものです。各トランスフォームは、IPSec セキュリティ プロトコル（ESP）および使用するアルゴリズムを表します（シンタックスの表に定義されている [**esp-aes** | **esp-aes-192** | **esp-aes-256** | **esp-des** | **esp-3des** | **esp-null**] または [**esp-md5-hmac** | **esp-sha-hmac**] のいずれか）。
transform-set-name	作成または修正するトランスフォーム セットの名前を指定します。
token	ユーザ認証にトークン ベースのサーバを使用することを指定します。

デフォルト

デフォルトの暗号化アルゴリズムは、esp-3des（Triple DES）です。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが導入されました。

使用上のガイドライン

トランスフォーム セットは、IPSec セキュリティ プロトコルを 1 つまたは 2 つ指定し、そのセキュリティ プロトコルで使用するアルゴリズムを指定します。特定のデータ フローを保護する場合、ピアは、IPSec セキュリティ アソシエーションのネゴシエート中に特定のトランスフォーム セットの使用に同意します。

IPSec メッセージを保護するには、128 ビット キー、192 ビット キー、または 256 ビット キーの AES を使用するトランスフォーム セットを使用します。

AES によって提供されるキーのサイズは非常に大きいため、ISAKMP ネゴシエーションでは、Diffie-Hellman グループ 1 およびグループ 2 ではなくグループ 5 を使用する必要があります。そのためには、**isakmp policy priority group 5** コマンドを使用します。

トランスフォーム セットを複数設定して、暗号マップ エントリでそれらのトランスフォーム セットを 1 つまたはそれ以上指定することもできます。IPSec セキュリティ アソシエーションのネゴシエーション内の暗号マップ エントリで定義したトランスフォーム セットは、その暗号マップ エントリのアクセスリストで指定されているデータ フローを保護します。ネゴシエート中、2 つのピアは、両方のピアで一致しているトランスフォーム セットがあるかどうかを検索します。セキュリティ アプライアンスは、そのようなトランスフォーム セットを検出すると、両方のピアの IPSec セキュリティ アソシエーションの一部として、保護対象のトラフィックに適用します。

各トランスフォーム セットは、暗号化または認証に使用するアルゴリズムを表します。IPSec セキュリティ アソシエーションのネゴシエート中に特定のトランスフォーム セットを使用するときは、トランスフォーム セット全体（プロトコル、アルゴリズム、およびその他の設定値の組み合せ）が、リモート ピアのトランスフォーム セットと一致する必要があります。

トランスフォーム セットで、ESP 暗号化トランスフォームのみ、または ESP 暗号化トランスフォームと ESP 認証トランスフォームの両方を指定できます。

指定できるトランスフォームの組み合せとしては、たとえば次のものがあります。

- **esp-des**
- **esp-des** と **esp-md5-hmac**

既存のトランスフォーム セットに対して、**crypto ipsec transform-set** コマンドで 1 つまたはそれ以上のトランスフォームを指定すると、指定したトランスフォームによってそのトランスフォーム セットのトランスフォームが置き換えられます。

例

次の例では、2 つのトランスフォーム セットを設定します。1 つは t1 という名前で、暗号化に DES を使用し、ハッシュ アルゴリズムとして SHA/HMAC-160 を使用します。もう 1 つは standard という名前で、暗号化に AES 192 を使用し、ハッシュ アルゴリズムとして MD5/HMAC-128 を使用します。

```
hostname(config)# crypto ipsec transform-set t1 esp-des esp-sha-hmac
hostname(config)# crypto ipsec transform-set standard esp-aes-192 esp-md5-hmac
hostname(config)
```

関連コマンド

コマンド	説明
clear configure crypto	すべての ipsec コンフィギュレーション（たとえば、グローバル ライフタイムやトランスフォーム セット）を消去します。
show running-config crypto map	すべての暗号マップのすべてのコンフィギュレーションを表示します。

crypto ipsec transform-set mode transport

トランスフォーム セットの IPSec トランスポート モードを指定するには、**crypto ipsec transport-set mode transport** コマンドをグローバル コンフィギュレーション モードで使用します。トランスフォーム セットから IPSec トランスポート モードを削除するには、このコマンドの **no** 形式を使用します。

crypto ipsec transform-set *transform-set-name* **mode transport**

no crypto ipsec transform-set *transform-set-name* **mode transport**

シンタックスの説明

mode transport	トンネル モード要求に加えて、トランスポート モード要求を受け付けるためのトランスフォーム セットを指定します。
transform-set-name	作成または修正するトランスフォーム セットの名前を指定します。
token	ユーザ認証にトークン ベースのサーバを使用することを指定します。

デフォルト

デフォルトはトンネル モードです。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

このコマンドは、トランスフォーム セットに対して IPSec トランスポート モードを指定します。デフォルトはトンネル モードです。

トンネル モードはトランスフォーム セットに対して自動的にイネーブルになります。

例

次の例では、暗号化に Triple DES を使用し、ハッシュ アルゴリズムに MD5/HMAC-128 を使用する transet5 という名前のトランスフォーム セットを設定してから、トランスフォーム セット transet5 に IPSec トランスポート モードを指定します。

```
hostname(config)# crypto ipsec transform-set transet5 esp-3des esp-md5-hmac
hostname(config)# crypto ipsec transform-set transet5 mode transport
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto	すべての ipsec コンフィギュレーション（たとえば、グローバル ライフタイムやトランスフォーム セット）を消去します。
clear configure crypto map	すべての暗号マップを消去します。
show running-config crypto map	すべての暗号マップのすべてのコンフィギュレーションを表示します。

crypto key generate dsa

識別証明書用の DSA キー ペアを生成するには、**crypto key generate dsa** コマンドをグローバル コンフィギュレーション モードで使用します。

crypto key generate dsa {**label** *key-pair-label*} [**modulus** *size*] [**noconfirm**]

シンタックスの説明

label *key-pair-label*	キー ペアに関連付ける名前を指定します。最大ラベル長は 128 文字です。DSA にはラベルが必要です。
modulus *size*	キー ペアのモジュール サイズ 512、768、または 1024 を指定します。デフォルトのモジュール サイズは 1024 です。
noconfirm	対話型のプロンプトをすべて表示しません。

デフォルト

デフォルトの係数サイズは 1024 です。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

SSL、SSH、および IPSec 接続をサポートする DSA キー ペアを生成するには、**crypto key generate dsa** コマンドを使用します。生成されたキー ペアは、コマンド シンタックスの一部として指定したラベルで識別します。ラベルを指定しない場合、セキュリティ アプライアンスはエラー メッセージを表示します。

（注）　DSA キーを生成するとき、遅延が発生する場合があります。Cisco PIX 515E Firewall では、この遅延が最大数分にわたることがあります。

例

グローバル コンフィギュレーション モードで入力した次の例では、mypubkey というラベルの DSA キー ペアを生成します。

```
hostname(config)# crypto key generate dsa label mypubkey
INFO: The name for the keys will be: mypubkey
hostname(config)#
```

グローバル コンフィギュレーション モードで入力した次の例では、誤って mypubkey というラベルの重複した DSA キー ペアを生成しようとしています。

```
hostname(config)# crypto key generate dsa label mypubkey
WARNING: You already have dSA keys defined named mypubkey
Do you really want to replace them? [yes/no] no
ERROR: Failed to create new DSA keys named mypubkey
hostname(config)#
```

関連コマンド

コマンド	説明
crypto key zeroize	DSA キー ペアを削除します。
show crypto key mypubkey	DSA キー ペアを表示します。

crypto key generate rsa

識別証明書用の RSA キー ペアを生成するには、**crypto key generate rsa** コマンドをグローバル コンフィギュレーション モードで使用します。

crypto key generate rsa [**usage-keys | general-keys**] [**label** *key-pair-label*] [**modulus** *size*] [**noconfirm**]

シンタックスの説明

general-keys	一組の汎用キーを生成します。これはデフォルトのキー ペア タイプです。
label *key-pair-label*	キー ペアに関連付ける名前を指定します。このキー ペアのラベルは一意である必要があります。同じラベルで別のキー ペアを作成しようとすると、セキュリティ アプライアンスは警告メッセージを表示します。キーの生成時にラベルを指定しない場合、キー ペアはスタティックに <Default-RSA-Key> という名前が付けられます。
modulus *size*	キー ペアのモジュール サイズ 512、768、1024、または 2048 を指定します。デフォルトのモジュール サイズは 1024 です。
noconfirm	対話型のプロンプトをすべて表示しません。
usage-keys	シグニチャ用と暗号化用の 2 つのキー ペアを生成します。これは、対応する識別用に 2 通の証明書が必要なことを意味します。

デフォルト

デフォルトのキー ペア タイプは **general key** です。デフォルトの係数サイズは 1024 です。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

SSL、SSH、および IPSec 接続をサポートする RSA キー ペアを生成するには、**crypto key generate rsa** コマンドを使用します。生成されたキー ペアは、コマンド シンタックスの一部として指定できるラベルで識別します。キー ペアを参照しないトラストポイントは、デフォルトの <Default-RSA-Key> を使用できます。SSH 接続では常にこのキーが使用されます。SSL は独自の証明書やキーをダイナミックに生成するため、トラストポイントに設定されていない限り、このことは SSL に影響を与えません。

例

グローバル コンフィギュレーション モードで入力した次の例では、mypubkey というラベルの RSA キー ペアを生成します。

```
hostname(config)# crypto key generate rsa label mypubkey
INFO: The name for the keys will be: mypubkey
Keypair generation process
hostname(config)#
```

グローバル コンフィギュレーション モードで入力した次の例では、誤って mypubkey というラベルの重複した RSA キー ペアを生成しようとしています。

```
hostname(config)# crypto key generate rsa label mypubkey
WARNING: You already have RSA keys defined named mypubkey
Do you really want to replace them? [yes/no] no
ERROR: Failed to create new RSA keys named mypubkey
hostname(config)#
```

グローバル コンフィギュレーション モードで入力した次の例では、デフォルト ラベルの RSA キー ペアを生成します。

```
hostname(config)# crypto key generate rsa
INFO: The name for the keys will be: <Default-RSA-Key>
Keypair generation process begin. Please wait...
hostname(config)#
```

関連コマンド

コマンド	説明
crypto key zeroize	RSA キー ペアを削除します。
show crypto key mypubkey	RSA キー ペアを表示します。

crypto key zeroize

指定したタイプ（rsa または dsa）のキー ペアを削除するには、**crypto key zeroize** コマンドをグローバル コンフィギュレーション モードで使用します。

crypto key zeroize {**rsa** | **dsa**} [**label** *key-pair-label*] [**default**] [**noconfirm**]

シンタックスの説明

default	ラベルがない RSA キー ペアを削除します。このキーワードは、RSA キー ペアに限り有効です。
dsa	キー タイプとして DSA を指定します。
label *key-pair-label*	指定したタイプ（rsa または dsa）のキー ペアを削除します。ラベルを指定しない場合、セキュリティ アプライアンスは指定したタイプのキー ペアをすべて削除します。
noconfirm	対話型のプロンプトをすべて表示しません。
rsa	キー タイプとして RSA 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。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

例

グローバル コンフィギュレーション モードで入力した次の例では、すべての RSA キー ペアを削除します。

```
hostname(config)# crypto key zeroize rsa
WARNING: All RSA keys will be removed.
WARNING: All router certs issued using these keys will also be removed.

Do you really want to remove these keys? [yes/no] y
hostname(config)#
```

関連コマンド

コマンド	説明
crypto key generate dsa	識別証明書用の DSA キー ペアを生成します。
crypto key generate rsa	識別証明書用の RSA キー ペアを生成します。

crypto map interface

以前に定義した暗号マップ セットをインターフェイスに適用するには、**crypto map interface** コマンドをグローバル コンフィギュレーション モードで使用します。インターフェイスから暗号マップ セットを削除するには、このコマンドの **no** 形式を使用します。

crypto map *map-name* **interface** *interface-name*

no crypto map *map-name* **interface** *interface-name*

シンタックスの説明

interface-name	VPN ピアでトンネルの確立に使用するセキュリティ アプライアンスのインターフェイスを指定します。ISAKMP をイネーブルにしていて、認証局（CA）を使用して証明書を取得する場合には、CA 証明書内で指定されているアドレスを持つインターフェイスにする必要があります。
map-name	暗号マップ セットの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

このコマンドは、暗号マップ セットをアクティブなセキュリティ アプライアンスのインターフェイスに割り当てるために使用します。セキュリティ アプライアンスでは、任意のアクティブ インターフェイスを IPSec の終端にできます。インターフェイスで IPSec サービスを提供するには、そのインターフェイスにまず暗号マップ セットを割り当てる必要があります。

インターフェイスに割り当てることができる暗号マップ セットは 1 つだけです。同じ *map-name* で *seq-num* が異なる暗号マップ エントリが複数ある場合、それらのエントリは同じセットの一部であり、インターフェイスにすべて適用されます。セキュリティ アプライアンスは、*seq-num* が最も小さい暗号マップ エントリを最初に評価します。

（注） セキュリティ アプライアンスでは、暗号マップ、ダイナミック マップ、および ipsec 設定をその場で変更できます。これを行う場合は、変更によって影響を受ける接続だけがセキュリティ アプライアンスによって停止させられます。特に、アクセスリスト内のエントリを削除することによって、暗号マップに関連付けられている既存のアクセスリストを変更する場合は、関連する接続だけが停止させられます。アクセスリスト内の他のエントリに基づく接続は、影響を受けません。

（注）　すべてのスタティック暗号マップは、アクセスリスト、トランスフォーム セット、および IPsec ピアの 3 つの部分を定義する必要があります。これらの 1 つが欠けている場合、暗号マップは不完全で、セキュリティ アプライアンスは次のエントリに進みます。ただし、暗号マップがアクセスリストでは一致するが、他の 2 つの要件のいずれかまたは両方で一致しない場合、このセキュリティ アプライアンスはトラフィックをドロップします。

すべての暗号マップが完全であることを確認するには、**show running-config crypto map** コマンドを使用します。不完全な暗号マップを修正するには、暗号マップを削除し、欠けているエントリを追加して再び適用します。

例

グローバル コンフィギュレーション モードで入力した次の例では、mymap という名前の暗号マップ セットを外部インターフェイスに割り当てます。トラフィックがこの外部インターフェイスを通過するときは、トラフィックがセキュリティ アプライアンスによって mymap セット内のすべての暗号マップ エントリと対照され、評価されます。発信トラフィックが mymap 暗号マップ エントリの 1 つのアクセスリストと一致する場合、セキュリティ アプライアンスはその暗号マップ エントリのコンフィギュレーションを使用して、セキュリティ アソシエーションを形成します。

```
hostname(config)# crypto map mymap interface outside
```

次の例は、必要な最小限の暗号マップ コンフィギュレーションを示しています。

```
hostname(config)# crypto map mymap 10 ipsec-isakmp
hostname(config)# crypto map mymap 10 match address 101
hostname(config)# crypto map mymap set transform-set my_t_set1
hostname(config)# crypto map mymap set peer 10.0.0.1
```

関連コマンド

コマンド	説明
clear configure crypto map	すべての暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。

crypto map ipsec-isakmp dynamic

所定の暗号マップ エントリが既存のダイナミック暗号マップを参照することを要求するには、**crypto map ipsec-isakmp dynamic** コマンドをグローバル コンフィギュレーション モードで使用します。相互参照を削除するには、このコマンドの **no** 形式を使用します。

ダイナミック暗号マップ エントリを作成するには、**crypto dynamic-map** コマンドを使用します。ダイナミック暗号マップ セットを作成したら、**crypto map ipsec-isakmp dynamic** コマンドを使用して、ダイナミック暗号マップ セットをスタティック暗号マップに追加します。

crypto map *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name*

no crypto map *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name*

シンタックスの説明

dynamic-map-name	既存のダイナミック暗号マップを参照する暗号マップ エントリの名前を指定します。
ipsec-isakmp	IKE がこの暗号マップ エントリの IPSec セキュリティ アソシエーションを確立することを指定します。
map-name	暗号マップ セットの名前を指定します。
seq-num	暗号マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0	このコマンドが **ipsec-manual** キーワードを削除するように変更されました。

使用上のガイドライン

暗号マップ エントリを作成したら、**crypto map interface** コマンドを使用して、ダイナミック暗号マップ セットをインターフェイスに割り当てることができます。

ダイナミック暗号マップを使用することで、保護の対象となるトラフィックのフィルタリングと分類、そのトラフィックに適用するポリシーの定義という 2 つの機能を利用できます。最初の機能はインターフェイス上のトラフィック フローが対象となり、2 番目の機能は（IKE を通じた）そのトラフィックのためのネゴシエーションが対象となります。

IPSec ダイナミック暗号マップは次の 4 つを指定します。

- 保護するトラフィック
- セキュリティ アソシエーションを確立する IPSec ピア
- 保護対象のトラフィックとともに使用するトランスフォーム セット
- キーおよびセキュリティ アソシエーションの使用方法または管理方法

暗号マップ セットは、それぞれ異なるシーケンス番号（seq-num）を持ち、マップ名が共通している暗号マップ エントリの集合です。たとえば、所定のインターフェイスを介して、あるトラフィックには所定のセキュリティを適用してピアに転送し、その他のトラフィックには別の IPSec セキュリティを適用して同じまたは別個のピアに転送するとします。このような構成をセットアップするには、2 つの暗号マップ エントリを作成します。マップ名は同じ名前にし、シーケンス番号をそれぞれ別の番号にします。

シーケンス番号引数として割り当てる番号は、任意に決定しないようにしてください。この番号は、暗号マップ セットに含まれている複数の暗号マップ エントリにランクを付けます。シーケンス番号の小さい暗号マップ エントリが番号の大きいエントリよりも先に評価されます。つまり、番号の小さいマップ エントリは優先順位が高くなります。

（注）　暗号マップをダイナミック暗号マップにリンクする場合は、ダイナミック暗号マップを指定する必要があります。指定すると、**crypto dynamic-map** コマンドを使用して以前に定義した既存のダイナミック暗号マップに暗号マップがリンクされます。暗号マップ エントリが変換された後に加えた変更は、有効になりません。たとえば、set peer 設定への変更は有効になりません。ただし、セキュリティ アプライアンスは起動中に変更を保存します。ダイナミック暗号マップを暗号マップに変換して戻す場合、変更は有効で、**show running-config crypto map** コマンドの出力に表示されます。セキュリティ アプライアンスは、リブートされるまでこれらの設定を維持します。

例

グローバル コンフィギュレーション モードで入力した次のコマンドでは、暗号マップ mymap を test という名前のダイナミック暗号マップを参照するように設定します。

```
hostname(config)# crypto map mymap ipsec-isakmp dynamic test
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべての暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。

crypto map match address

アクセスリストを暗号マップ エントリに割り当てるには、**crypto map match address** コマンドをグローバル コンフィギュレーション モードで使用します。暗号マップ エントリからアクセスリ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。

crypto map *map-name seq-num* **match address** *acl_name*

no crypto map *map-name seq-num* **match address** *acl_name*

シンタックスの説明

acl_name	暗号化アクセスリストの名前を指定します。この名前は、一致対象となる名前付き暗号化アクセスリストの名前引数と一致している必要があります。
map-name	暗号マップ セットの名前を指定します。
seq-num	暗号マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

このコマンドは、すべてのスタティック暗号マップに対して指定必須となるコマンドです。**crypto dynamic-map** コマンドでダイナミック暗号マップを定義する場合は、このコマンドは必須ではありませんが、使用することを強く推奨します。

アクセスリストを定義するには、**access-list** コマンドを使用します。

セキュリティ アプライアンスはアクセスリストを利用して、保護を必要としないトラフィックと IPSec 暗号で保護するトラフィックを区別します。また、許可 ACE に一致する発信パケットを保護し、許可 ACE に一致する着信パケットが保護されるようにします。

セキュリティ アプライアンスが deny 文へのパケットと一致する場合、暗号マップ内の残りのアクセス コントロール エントリ（ACE）に対するパケットの評価を省略し、順番に次の暗号マップ内の ACE に対するパケットの評価を再開します。*Cascading ACL* は、ACL 内の残りの ACE の評価をバイパスする拒否 ACE の使用および暗号マップ セット内の次の暗号マップに割り当てられた ACL に対するトラフィックの評価の再開に関係します。各暗号マップを別の IPSec 設定に関連付けることができるため、拒否 ACE を使用して対応する暗号マップの詳細な評価から特別なトラフィックを除外し、特別なトラフィックを別の暗号マップの permit 文と一致させて別のセキュリティを提供または要求できます。

（注）　暗号化用のアクセスリストは、インターフェイスを通過するトラフィックを許可するかどうかを判定しません。このような判定には、**access-group** コマンドで作成する、インターフェイスに直接適用されるアクセスリストが使用されます。

（注）　透過モードでは、宛先アドレスはセキュリティ アプライアンスの IP アドレス、管理アドレスである必要があります。透過モードでは、セキュリティ アプライアンスへのトンネルだけが許可されます。

関連コマンド

コマンド	説明
clear configure crypto map	すべての暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。

crypto map set connection-type

この暗号マップ エントリのバックアップ サイトツーサイト機能の接続タイプを指定するには、**crypto map set connection-type** コマンドをグローバル コンフィギュレーション モードで使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set connection-type {answer-only | originate-only | bidirectional}**

no crypto map *map-name seq-num* **set connection-type {answer-only | originate-only | bidirectional}**

シンタックスの説明

answer-only	このピアが、この暗号マップ エントリに基づいてサイトツーサイト接続の着信 IKE 接続に応答のみできることを指定します。接続要求を発信することはできません。
bidirectional	このピアが、この暗号マップ エントリに基づいて接続を受け入れ、発信できることを指定します。これはすべてのサイトツーサイト接続のデフォルトの接続タイプです。
map-*name*	暗号マップ セットの名前を指定します。
originate-only	このピアが、この暗号マップ エントリに基づいて接続の発信のみできることを指定します。着信接続を受け入れることはできません。
seq-num	暗号マップ エントリに割り当てる番号を指定します。
set connection-type	この暗号マップ エントリのバックアップ サイトツーサイト機能の接続タイプを指定します。answer-only、originate-only、および bidirectional の 3 タイプの接続があります。

デフォルト

デフォルト設定は bidirectional です。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

* 透過ファイアウォール モードでは、このコマンドは表示されますが、インターフェイスに対応付けられた暗号マップに含まれる暗号マップ エントリでは、answer-only 値は answer-only 以外の値に設定できません。

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで入力した次の例では、暗号マップ mymap を設定し、接続タイプを bidirectional に設定します。

```
hostname(config)# crypto map mymap 10 set connection-type bidirectional
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべての暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。

crypto map set inheritance

この暗号マップ エントリ用に生成されるセキュリティ アソシエーションの精度（シングルまたはマルチ）を設定するには、**set inheritance** コマンドをグローバル コンフィギュレーション モードで使用します。この暗号マップ エントリの継承の設定を削除するには、このコマンドの no 形式を使用します。

crypto map *map-name seq-num* **set inheritance {data| rule}**

no crypto map *map-name seq-num* **set inheritance {data | rule}**

シンタックスの説明

data	規則で指定されているアドレス範囲内のすべてのアドレス ペアに 1 つのトンネルを指定します。
map-name	暗号マップ セットの名前を指定します。
rule	この暗号マップに関連付けられている各 ACL エントリに 1 つのトンネルを指定します。これはデフォルトの値です。
seq-num	暗号マップ エントリに割り当てる番号を指定します。
set inheritance	継承のタイプ **data** *または* **rule** を指定します。継承では、各セキュリティ ポリシー データベース（SPD）規則に対して 1 つのセキュリティ アソシエーション（SA）を生成したり、範囲内の各アドレス ペアに対して複数のセキュリティ SA を生成したりすることができます。

デフォルト

デフォルト値は、***rule*** です。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、セキュリティ アプライアンスがトンネルに応答しているときではなく、トンネルを開始しているときのみ動作します。データ設定を使用すると、多数の IPSec SA が作成される場合があります。それによりメモリが消費され、全体的なトンネルが少なくなります。データ設定は、セキュリティ依存型のアプリケーションに対してのみ使用する必要があります。

例

グローバル コンフィギュレーション モードで入力した次の例では、暗号マップ mymap を設定し、継承タイプを data に設定します。

```
hostname(config)# crypto map mymap 10 set inheritance data
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべての暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。

crypto map set nat-t-disable

接続の NAT-T をこの暗号マップ エントリに基づいてディセーブルにするには、**crypto map set nat-t-disable** コマンドをグローバル コンフィギュレーション モードで使用します。この暗号マップ エントリの NAT-T をイネーブルにするには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* ***set nat-t-disable***

no crypto map *map-name seq-num* ***set nat-t-disable***

シンタックスの説明

map-name	暗号マップ セットの名前を指定します。
seq-num	暗号マップ エントリに割り当てる番号を指定します。

デフォルト

このコマンドのデフォルト設定はオンではありません（したがって、NAT-T はデフォルトでイネーブルです）。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

NAT-T をグローバルにイネーブルにするには、**isakmp nat-traversal** コマンドを使用します。その後、**crypto map set nat-t-disable** コマンドを使用して、特定の暗号マップ エントリの NAT-T をディセーブルにできます。

例

グローバル コンフィギュレーション モードで入力した次のコマンドは、mymap という名前の暗号マップ エントリの NAT-T をディセーブルにします。

```
hostname(config)# crypto map mymap 10 set nat-t-disable
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべての暗号マップのすべてのコンフィギュレーションを消去します。
isakmp nat-traversal	すべての接続の NAT-T をイネーブルにします。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。

crypto map set peer

暗号マップ エントリの IPSec ピアを指定するには、**crypto map set peer** コマンドをグローバル コンフィギュレーション モードで使用します。暗号マップ エントリから IPSec ピアを削除するには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set peer** {*ip_address* | *hostname*} {*...ip_address* | *hostname10*}

no crypto map *map-name seq-num* **set peer** {*ip_address* | *hostname*} {*...ip_address* | *hostname10*}

シンタックスの説明

hostname	ピアをセキュリティ アプライアンスの **name** コマンドで定義したホスト名で指定します。
ip_address	ピアを IP アドレスで指定します。
map-name	暗号マップ セットの名前を指定します。
peer	暗号マップ エントリの IPSec ピアをホスト名または IP アドレスで指定します。
seq-num	暗号マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0	このコマンドが、最大 10 のピア アドレスを許容するように変更されました。

使用上のガイドライン

このコマンドは、すべてのスタティック暗号マップに対して指定必須となるコマンドです。**crypto dynamic-map** コマンドでダイナミック暗号マップ エントリを定義する場合には、このコマンドは必須ではなく、ほとんど使用しません。これは、ピアが通常は未知のものであるためです。

LAN-to-LAN 接続では、複数のピアを originate-only 接続タイプでのみ使用できます。複数のピアを設定することは、フォールバック リストを指定することと同じです。トンネルごとに、セキュリティ アプライアンスはリストの最初のピアとネゴシエートしようとします。ピアが応答しない場合、セキュリティ アプライアンスはピアが応答するか、リストにピアがなくなるまでリストを検索します。バックアップ LAN-to-LAN 機能を使用している場合（つまり暗号マップが originate-only タイプの場合）にのみ複数のピアを設定できます。

例

グローバル コンフィギュレーション モードで入力した次の例は、IKE を使用してセキュリティ アソシエーションを確立する暗号マップ コンフィギュレーションを示します。この例では、ピア 10.0.0.1 またはピア 10.0.0.2 に対するセキュリティ アソシエーションをセットアップできます。

```
hostname(config)# crypto map mymap 10 ipsec-isakmp
hostname(config)# crypto map mymap 10 match address 101
hostname(config)# crypto map mymap 10 set transform-set my_t_set1
hostname(config)# crypto map mymap 10 set peer 10.0.0.1 10.0.0.2
```

関連コマンド

コマンド	説明
clear configure crypto map	すべての暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。

crypto map set pfs

この暗号マップ エントリ用の新しいセキュリティ アソシエーションを要求するときに、完全転送秘密（PFS）を要求するように IPSec を設定、または新しいセキュリティ アソシエーションの要求を受信したときに IPSec が PFS を要求するように設定するには、**crypto map set pfs** コマンドをグローバル コンフィギュレーション モードで使用します。IPSec が PFS を要求しないことを指定するには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set pfs [group1 | group2 | group5 | group7]**

no crypto map *map-name seq-num* **set pfs [group1 | group2 | group5 | group7]**

シンタックスの説明

group1	IPSec で新しい Diffie-Hellman 交換を実行するときに、768 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group2	IPSec で新しい Diffie-Hellman 交換を実行するときに、1024 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group5	IPSec で新しい Diffie-Hellman 交換を実行するときに、1536 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group7	IPSec が、たとえば movianVPN クライアントで、楕円曲線フィールドのサイズが 163 ビットである group7（ECC）を使用するように指定します。
map-name	暗号マップ セットの名前を指定します。
seq-num	暗号マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトでは、PFS は設定されません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0	このコマンドが変更され、Diffie-Hellman group 7 が追加されました。

使用上のガイドライン

PFS を使用すると、新しいセキュリティ アソシエーションをネゴシエートするたびに新しい Diffie-Hellman 交換が発生します。この交換によって、処理にかかる時間が長くなります。PFS を使用すると、セキュリティがいっそう向上します。1 つのキーが攻撃者によってクラックされた場合でも、信頼性が損なわれるのはそのキーで送信されたデータだけになるためです。

このコマンドを使用すると、暗号マップ エントリ用の新しいセキュリティ アソシエーションを要求するとき、ネゴシエート中に IPSec が PFS を要求します。**set pfs** 文でグループが指定されていない場合、セキュリティ アプライアンスはデフォルト（group2）を送信します。

ピアがネゴシエーションを開始するときに、ローカル コンフィギュレーションで PFS が指定されている場合、ピアは PFS 交換を実行する必要があります。実行しない場合は、ネゴシエーションに失敗します。ローカル コンフィギュレーションでグループが指定されていない場合、セキュリティ アプライアンスはデフォルトの group2 が指定されているものと見なします。ローカル コンフィギュレーションで group2、group5、または group7 が指定されている場合は、そのグループがピアのオファーに含まれている必要があります。含まれていない場合は、ネゴシエーションに失敗します。

ネゴシエーションが成功するには、両端に PFS が設定されている必要があります。設定されている場合、グループは完全に一致する必要があります。セキュリティ アプライアンスは、ピアからの PFS のオファーをすべて受け入れません。

1536 ビットの Diffie-Hellman プライム モジュラス グループ group5 は、group1 や group2 よりも強固なセキュリティを提供します。ただし、他のグループの場合よりも多くの処理時間が必要になります。

楕円曲線フィールドのサイズが 163 ビットである Diffie-Hellman Group 7 では、IPSec SA キーが生成されます。このオプションは、任意の暗号化アルゴリズムとともに使用できます。これは、movianVPN クライアントで使用するためのオプションですが、Group 7（ECC）をサポートしている任意のピアで使用できます。

セキュリティ アプライアンスは、Cisco VPN Client と対話するときに PFS 値を使用しません。その代わり、フェーズ 1 でネゴシエートされた値を使用します。

例

グローバル コンフィギュレーション モードで入力した次の例では、暗号マップ「mymap 10」用の新しいセキュリティ アソシエーションをネゴシエートするときに、必ず PFS を使用することを指定します。

```
hostname(config)# crypto map mymap 10 ipsec-isakmp
hostname(config)# crypto map mymap 10 set pfs group2
```

関連コマンド

コマンド	説明
clear isakmp sa	アクティブな IKE セキュリティ アソシエーションを削除します。
clear configure crypto map	すべての暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。
tunnel-group	トンネルグループとそのパラメータを設定します。

crypto map set phase1 mode

メインまたはアグレッシブへの接続を開始する場合にフェーズ 1 の IKE モードを指定するには、**crypto map set phase1mode** コマンドをグローバル コンフィギュレーション モードで使用します。フェーズ 1 IKE ネゴシエーションの設定を削除するには、このコマンドの **no** 形式を使用します。アグレッシブ モードの Diffie-Hellman グループを含めることはオプションです。含めない場合、セキュリティ アプライアンスは group 2 を使用します。

crypto map *map-name seq-num* **set phase1mode {main | aggressive [group1 | group2 | group5 | group7]}**

no crypto map *map-name seq-num* **set phase1mode {main | aggressive [group1 | group2 | group5 | group7]}**

シンタックスの説明

aggressive	フェーズ 1 IKE ネゴシエーションにアグレッシブ モードを指定します。
group1	IPSec で新しい Diffie-Hellman 交換を実行するときに、768 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group2	IPSec で新しい Diffie-Hellman 交換を実行するときに、1024 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group5	IPSec で新しい Diffie-Hellman 交換を実行するときに、1536 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group7	IPSec が、たとえば movianVPN クライアントで、楕円曲線フィールドのサイズが 163 ビットである group7（ECC）を使用するように指定します。
main	フェーズ 1 IKE ネゴシエーションにメイン モードを指定します。
map-name	暗号マップ セットの名前を指定します。
seq-num	暗号マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトのフェーズ 1 のモードは、**main** です。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、発信側モードでのみ動作します。応答側モードでは動作しません。

例

グローバル コンフィギュレーション モードで入力した次の例では、暗号マップ mymap を設定し、group2 を使用してフェーズ 1 のモードをアグレッシブに設定します。

```
hostname(config)# crypto map mymap 10 set phase1mode aggressive group2
hostname(config)#
```

関連コマンド

コマンド	説明
clear isakmp sa	アクティブな IKE セキュリティ アソシエーションを削除します。
clear configure crypto map	すべての暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。

crypto map set reverse-route

この暗号マップ エントリに基づいて任意の接続の RRI をイネーブルにするには、**crypto map set reverse-route** コマンドをグローバル コンフィギュレーション モードで使用します。この暗号マップ エントリに基づいた任意の接続の逆ルート注入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。

crypto map *map-name seq-num* ***set reverse-route***

no crypto map *map-name seq-num* ***set reverse-route***

シンタックスの説明

map-name	暗号マップ セットの名前を指定します。
seq-num	暗号マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトでは、このコマンドの設定はオフになっています。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスは、ルーティング テーブルにスタティック ルートを自動的に追加し、OSPF を使用してそれらのルートをプライベート ネットワークまたは境界ルータに通知できます。

例

グローバル コンフィギュレーション モードで入力した次の例では、mymap という名前の暗号マップの RRI をイネーブルにします。

```
hostname(config)# crypto map mymap 10 set reverse-route
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべての暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。

crypto map set security-association lifetime

特定の暗号マップ エントリについて、IPSec セキュリティ アソシエーションをネゴシエートするときに使用されるグローバル ライフタイム値を上書きするには、グローバル コンフィギュレーション モードで **crypto map set security-association lifetime** コマンドを使用します。暗号マップ エントリのライフタイム値をグローバル値にリセットするには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set security-association lifetime {seconds** *seconds* | **kilobytes** *kilobytes*}

no crypto map *map-name seq-num* **set security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes*}

シンタックスの説明

kilobytes	所定のセキュリティ アソシエーションの有効期限が切れるまでに、そのセキュリティ アソシエーションを使用してピア間を通過できるトラフィックの量を KB 単位で指定します。 デフォルトは 4,608,000 KB です。
map-name	暗号マップ セットの名前を指定します。
seconds	セキュリティ アソシエーションの有効期限が切れるまでの存続時間（秒数）を指定します。デフォルトは 28,800 秒（8 時間）です。
seq-num	暗号マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトの KB 数は 4,608,000 で、デフォルトの秒数は 28,800 です。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

暗号マップのセキュリティ アソシエーションは、グローバル ライフタイム値に基づいてネゴシエートされます。

IPSec セキュリティ アソシエーションでは、共有秘密鍵を使用します。これらの鍵とセキュリティ アソシエーションは、両方同時にタイムアウトします。

個々の暗号マップ エントリでライフタイム値が設定されている場合は、セキュリティ アソシエーションのネゴシエート中に新しいセキュリティ アソシエーションを要求するとき、セキュリティ アプライアンスは、ピアへの要求の中でこの暗号マップ ライフタイム値を利用します。この値を、新しいセキュリティ アソシエーションのライフタイムとして使用します。セキュリティ アプライアンスは、ピアからネゴシエーション要求を受信すると、ピアが指定するライフタイム値またはローカルに設定済みのライフタイム値のうち、小さい方を新しいセキュリティ アソシエーションのライフタイムとして使用します。

ライフタイムには、期間を指定するものとトラフィック量を指定するものの 2 つがあります。セッション キーとセキュリティ アソシエーションは、いずれかのライフタイムに最初に到達した時点で期限切れになります。1 つのコマンドで両方を指定できます。

（注）　セキュリティ アプライアンスでは、暗号マップ、ダイナミック マップ、および ipsec 設定をその場で変更できます。これを行う場合は、変更によって影響を受ける接続だけがセキュリティ アプライアンスによって停止させられます。特に、アクセスリスト内のエントリを削除することによって、暗号マップに関連付けられている既存のアクセスリストを変更する場合は、関連する接続だけが停止させられます。アクセスリスト内の他のエントリに基づく接続は、影響を受けません。

期間ライフタイムを変更するには、**crypto map set security-association lifetime seconds** コマンドを使用します。期間ライフタイムを使用する場合は、指定した秒数が経過した時点でキーおよびセキュリティ アソシエーションがタイムアウトします。

例

グローバル コンフィギュレーション モードで次のコマンドを入力すると、暗号マップ mymap のセキュリティ アソシエーション ライフタイムが秒単位および KB 単位で指定されます。

```
hostname(config)# crypto map mymap 10 set security-association lifetime seconds 1400
kilobytes 3000000
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべての暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。

crypto map set transform-set

暗号マップ エントリで使用するトランスフォーム セットを指定するには、**crypto map set transform-set** コマンドをグローバル コンフィギュレーション モードで使用します。暗号マップ エントリから指定したトランスフォーム セットを削除するには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set transform-set** *transform-set-name1* [*… transform-set-name9*]

no crypto map *map-name seq-num* **set transform-set** *transform-set-name1* [*… transform-set-name9*]

シンタックスの説明

map-name	暗号マップ セットの名前を指定します。
seq-num	暗号マップ エントリに割り当てる番号を指定します。
transform-set-name1 *transform-set-name9*	暗号マップに使用する、**crypto ipsec transform-set** コマンドを使用して定義したトランスフォーム セットの名前を指定します。ipsec-isakmp 暗号マップ エントリまたはダイナミック暗号マップ エントリの場合には、トランスフォーム セットを 9 つまで指定できます。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

このコマンドは、すべての暗号マップ エントリに対して指定必須となるコマンドです。

ローカル セキュリティ アプライアンスがネゴシエーションを開始する場合、トランスフォーム セットは **crypto map** コマンド文に指定した順序でピアに提示されます。ピアがネゴシエーションを開始する場合、ローカル セキュリティ アプライアンスは、暗号マップ エントリで指定されているトランスフォーム セットのいずれかに最初に一致したトランスフォーム セットを受け入れます。

両方のピアで最初に一致したトランスフォーム セットが、セキュリティ アソシエーションに使用されます。一致するトランスフォーム セットが検出されない場合、IPSec はセキュリティ アソシエーションを確立しません。トラフィックを保護するセキュリティ アソシエーションが存在しないため、トラフィックはドロップされます。

トランスフォーム セットのリストを変更する場合は、新しいトランスフォーム セット リストを再指定して、古いリストを置き換えます。この変更が適用されるのは、このトランスフォーム セットを参照している **crypto map** コマンド文だけです。

crypto map コマンド文の中で指定するトランスフォーム セットは、**crypto ipsec transform-set** コマンドを使用して事前に定義しておく必要があります。

例

グローバル コンフィギュレーション モードで入力した次の例では、暗号マップ mymap に 2 つのトランスフォーム セット（tfset1 および tfset2）を指定します。

```
hostname(config)# crypto map mymap 10 set transform-set tfset1 tfset2
hostname(config)#
```

グローバル コンフィギュレーション モードで入力した次の例は、セキュリティ アプライアンスが IKE を使用してセキュリティ アソシエーションを確立する場合に必要となる、最小限の暗号マップ コンフィギュレーションを示しています。

```
hostname(config)# crypto map mymap 10 ipsec-isakmp
hostname(config)# crypto map mymap 10 match address 101
hostname(config)# crypto map mymap set transform-set my_t_set1
hostname(config)# crypto map mymap set peer 10.0.0.1
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべての暗号マップのすべてのコンフィギュレーションを消去します。
crypto ipsec transform-set	トランスフォーム セットを設定します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。

crypto map set trustpoint

暗号マップ エントリのフェーズ 1 ネゴシエーション中に、認証用に送信する証明書を指定するトラストポイントを指定するには、**crypto map set trustpoint** コマンドをグローバル コンフィギュレーション モードで使用します。暗号マップ エントリからトラストポイ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。

crypto map *map-name seq-num* **set trustpoint** *trustpoint-name* **[chain]**

nocrypto map *map-name seq-num* **set trustpoint** *trustpoint-name* **[chain]**

シンタックスの説明

chain	（オプション）証明書チェーンを送信します。CA 証明書チェーンには、ルート証明書から識別証明書まで、証明書の階層内のすべての CA 証明書が含まれています。デフォルト値はディセーブル（チェーンなし）です。
map-name	暗号マップ セットの名前を指定します。
seq-num	暗号マップ エントリに割り当てる番号を指定します。
trustpoint- name	フェーズ 1 ネゴシエーション中に送信する証明書を指定します。デフォルトは none です。

デフォルト

デフォルト値は none です。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

この暗号マップ コマンドは、接続の開始に限り有効です。応答側の情報については、**tunnel-group** コマンドを参照してください。

例

グローバル コンフィギュレーション モードで入力した次の例では、暗号マップ mymap に tpoint1 という名前のトラストポイントを指定し、証明書のチェーンを指定します。

```
hostname(config)# crypto map mymap 10 set trustpoint tpoint1 chain
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべての暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。
tunnel-group	トンネルグループを設定します。