CHAPTER 5

G ～ L のコマンド

gateway

特定のゲートウェイを管理しているコール エージェントのグループを指定するには、MGCP マップ コンフィギュレーション モードで **gateway** コマンドを使用します。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。

gateway *ip_address* [*group_id*]

シンタックスの説明

gateway	特定のゲートウェイを管理しているコール エージェントのグループを指定します。
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
MGCP 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

gateway コマンドは、特定のゲートウェイを管理しているコール エージェントのグループを指定するために使用します。*ip_address* オプションを使用して、ゲートウェイの IP アドレスを指定します。*group_id* オプションは 0 ～ 4294967295 の数字です。この数字は、ゲートウェイを管理しているコール エージェントの *group_id* に対応している必要があります。1 つのゲートウェイは 1 つのグループだけに所属できます。

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_policy
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。

global

NAT 用のマッピング アドレスのプールを作成するには、グローバル コンフィギュレーション モードで **global** コマンドを使用します。アドレスのプールを削除するには、このコマンドの **no** 形式を使用します。

global (*mapped_ifc) nat_id* {*mapped_ip*[**-***mapped_ip*] [**netmask** *mask*] | **interface**}

no global (*mapped_ifc) nat_id* {*mapped_ip*[-*mapped_ip*] [**netmask** *mask*] | **interface**}

シンタックスの説明

interface	インターフェイスの IP アドレスを、マッピング アドレスとして使用します。このキーワードを使用するのは、インターフェイス アドレスを使用しようとする場合に、アドレスが DHCP を使用して動的に割り当てられているときです。
mapped_ifc	マッピング IP アドレス ネットワークに接続されているインターフェイスの名前を指定します。
mapped_ip[**-***mapped_ip*]	マッピングされているインターフェイスの終了時に実際のアドレスを変換する場合の変換先マッピング アドレス（複数可）を指定します。単一のアドレスを指定する場合は、PAT を設定します。アドレスの範囲を指定する場合は、ダイナミック NAT を設定します。 外部ネットワークがインターネットに接続されている場合は、各グローバル IP アドレスが Network Information Center（NIC）に登録されている必要があります。
nat_id	NAT ID の整数を指定します。この ID は、変換対象の実際のアドレスにマッピング プールを関連付けるときに **nat** コマンドによって参照されます。 通常の NAT の場合、この整数の範囲は 1 ～ 2147483647 となります。ポリシー NAT（**nat id access-list**）の場合、整数の範囲は 1 ～ 65535 となります。 **global** コマンドで NAT ID に 0 を指定しないでください。0 は、**global** コマンドを使用しないアイデンティティ NAT および NAT 免除用に予約されています。
netmask *mask*	（オプション）*mapped_ip* のネットワーク マスクを指定します。このマスクは、*mapped_ip* と組み合せた場合、ネットワークを指定しません。この場合は、*mapped_ip* をホストに割り当てるときに mapped_ip に割り当てたサブネット マスクを指定します。アドレスの範囲を設定する場合は、*mapped_ip-mapped_ip* を指定する必要があります。 マスクを指定しない場合は、アドレス クラスのデフォルト マスクが使用されます。

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。

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

ダイナミック NAT および PAT の場合は、最初に、変換対象となるインターフェイス上の実際のアドレスを指定する **nat** コマンドを設定します。次に、別のインターフェイスの終了時にマッピング アドレスを指定するための **global** コマンドを別途設定します（PAT の場合、マッピング アドレスは 1 つです）。各 **nat** コマンドは、各コマンドに割り当てられた番号である NAT ID の比較によって、**global** コマンドと一致します。

ダイナミック NAT および PAT の詳細については、**nat** コマンドを参照してください。

NAT コンフィギュレーションを変更する場合、既存の変換がタイムアウトするのを待たずに新しい NAT 情報を使用するときは、**clear xlate** コマンドを使用して変換テーブルを消去してもかまいません。ただし、変換テーブルを消去すると現在の接続がすべて切断されます。

例

たとえば、内部インターフェイス上の 10.1.1.0/24 ネットワークを変換するには、次のコマンドを入力します。

```
hostname(config)# nat (inside) 1 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.1-209.165.201.30
```

ダイナミック NAT 用のアドレス プールを、NAT プールを使い果たしたときのための PAT アドレスとともに指定するには、次のコマンドを入力します。

```
hostname(config)# nat (inside) 1 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.5
hostname(config)# global (outside) 1 209.165.201.10-209.165.201.20
```

ルーティングの簡略化などのために、セキュリティの低い DMZ（非武装地帯）のネットワーク アドレスを変換して内部ネットワーク（10.1.1.0）と同じネットワーク上に表示するには、次のコマンドを入力します。

```
hostname(config)# nat (dmz) 1 10.1.2.0 255.255.255.0 outside dns
hostname(config)# global (inside) 1 10.1.1.45
```

ポリシー NAT を使用して、1 つの実際のアドレスに 2 つの異なる宛先アドレスを指定するには、次のコマンドを入力します。

```
hostname(config)# access-list NET1 permit ip 10.1.2.0 255.255.255.0 209.165.201.0
255.255.255.224
hostname(config)# access-list NET2 permit ip 10.1.2.0 255.255.255.0 209.165.200.224
255.255.255.224
hostname(config)# nat (inside) 1 access-list NET1 tcp 0 2000 udp 10000
hostname(config)# global (outside) 1 209.165.202.129
hostname(config)# nat (inside) 2 access-list NET2 tcp 1000 500 udp 2000
hostname(config)# global (outside) 2 209.165.202.130
```

ポリシー NAT を使用して、それぞれが異なるポートを使用する、1 つの実際のアドレスと宛先アドレスのペアを指定するには、次のコマンドを入力します。

```
hostname(config)# access-list WEB permit tcp 10.1.2.0 255.255.255.0 209.165.201.11
255.255.255.255 eq 80
hostname(config)# access-list TELNET permit tcp 10.1.2.0 255.255.255.0 209.165.201.11
255.255.255.255 eq 23
hostname(config)# nat (inside) 1 access-list WEB
hostname(config)# global (outside) 1 209.165.202.129
hostname(config)# nat (inside) 2 access-list TELNET
hostname(config)# global (outside) 2 209.165.202.130
```

関連コマンド

コマンド	説明
clear configure global	**global** コマンドをコンフィギュレーションから削除します。
nat	変換対象となる実際のアドレスを指定します。
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。
static	1 対 1 の変換を設定します。

group-delimiter

グループ名の解析をイネーブルにし、トンネルのネゴシエーション中に受信したユーザ名からグループ名を解析するときに使用するデリミタを指定するには、グローバル コンフィギュレーション モードで **group-delimiter** コマンドを使用します。このグループ名の解析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。

group-delimiter *delimiter*

no group-delimiter

シンタックスの説明

delimiter	グループ名のデリミタとして使用する文字を指定します。 有効値は、**@**、**#**、および **!** 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

デフォルトでは、デリミタは指定されておらず、グループ名の解析はディセーブルになっています。

例

次の例は、グループ デリミタを番号記号（#）に変更するための **group-delimiter** コマンドを示しています。

```
hostname(config)# group-delimiter #
```

関連コマンド

コマンド	説明
show running-config group-delimiter	現在の group-delimiter の値を表示します。
strip-group	strip-group の処理をイネーブルまたはディセーブルにします。

group-lock

リモート ユーザがトンネルグループだけからアクセスできるようにするには、グループポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **group-lock** コマンドを発行します。

group-lock アトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、値を別のグループポリシーから継承できます。group-lock をディセーブルにするには、**group-lock none** コマンドを使用します。

group-lock はユーザを制限するときに、VPN Client に設定されているグループが、ユーザの割り当て先のトンネルグループと同じかどうかを確認します。同じでない場合、セキュリティ アプライアンスは、ユーザが接続できないようにします。group-lock を設定しない場合、セキュリティ アプライアンスは割り当てグループを考慮せずにユーザを認証します。

group-lock {value *tunnel-grp-name* **| none}**

no group-lock

シンタックスの説明

none	group-lock をヌル値に設定して、group-lock の制限を拒否します。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 group-lock の値を継承しないようにします。
value *tunnel-grp-name*	接続しようとするユーザにセキュリティ アプライアンスが要求する既存の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
グループポリシー	•	—	•	—	—
ユーザ名	•	—	•	—	—

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

次の例は、FirstGroup というグループポリシーにグループ ロックを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# group-lock value tunnel group name
```

group-object

ネットワーク オブジェクト グループを追加するには、プロトコル、ネットワーク、サービス、および icmp-type コンフィギュレーション モードで **group-object** コマンドを使用します。ネットワーク オブジェクト グループを削除するには、このコマンドの **no** 形式を使用します。

group-object *obj_grp_id*

no group-object *obj_grp_id*

シンタックスの説明

obj_grp_id	オブジェクト グループ（1 ～ 64 文字）を指定します。アルファベット、数字、アンダースコア（_）、ハイフン（-）、およびピリオド（.）を任意に組み合せることができます。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
プロトコル、ネットワーク、サービス、および icmp-type 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

group-object コマンドは、**object-group** コマンドと組み合せることで、自身がオブジェクト グループであるオブジェクトを定義します。このコマンドは、プロトコル、ネットワーク、サービス、および icmp-type コンフィギュレーション モードで使用されます。このサブコマンドを使用すると、同じタイプのオブジェクトを論理的にグループ化することや、構造化コンフィギュレーションの階層型オブジェクト グループを構築することができます。

グループ オブジェクトに限り、オブジェクトをオブジェクト グループ内で重複させることができます。たとえば、オブジェクト 1 がグループ A とグループ B の両方にある場合、A と B を両方含むグループ C を定義できます。ただし、グループ オブジェクトに含めることによってグループ階層が循環型になる場合は、含めることができません。たとえば、グループ A をグループ B に含め、同時にグループ B をグループ A に含めることはできません。

階層型オブジェクト グループの最大許容レベルは 10 です。

例

次の例は、ホストを重複させる必要がなくなるように、ネットワーク コンフィギュレーション モードで **group-object** コマンドを使用する方法を示しています。

```
hostname(config)# object-group network host_grp_1
hostname(config-network)# network-object host 192.168.1.1
hostname(config-network)# network-object host 192.168.1.2
hostname(config-network)# exit
hostname(config)# object-group network host_grp_2
hostname(config-network)# network-object host 172.23.56.1
hostname(config-network)# network-object host 172.23.56.2
hostname(config-network)# exit
hostname(config)# object-group network all_hosts
hostname(config-network)# group-object host_grp_1
hostname(config-network)# group-object host_grp_2
hostname(config-network)# exit
hostname(config)# access-list grp_1 permit tcp object-group host_grp_1 any eq ftp
hostname(config)# access-list grp_2 permit tcp object-group host_grp_2 any eq smtp
hostname(config)# access-list all permit tcp object-group all-hosts any eq w
```

関連コマンド

コマンド	説明
clear configure object-group	すべての **object-group** コマンドをコンフィギュレーションから削除します。
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。

group-policy

グループポリシーを作成または編集するには、グローバル コンフィギュレーション モードで **group-policy** コマンドを使用します。グループポリシーをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

group-policy *name* {**internal [from** *group-policy_name*] | **external server-group** *server_group* **password** *server_password*}

no group-policy *name*

シンタックスの説明

external server-group *server_group*	グループポリシーを外部として指定し、セキュリティ アプライアンスがアトリビュートをクエリーするための AAA サーバ グループを指定します。
from *group-policy_name*	この内部グループポリシーのアトリビュートを、既存のグループポリシーの値に初期化します。
internal	グループポリシーを内部として指定します。
name	グループポリシーの名前を指定します。
password *server_password*	外部 AAA サーバ グループからアトリビュートを取得するときに使用するパスワードを指定します。

デフォルト

デフォルトの動作や値はありません。使用上のガイドラインを参照してください。

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

「DefaultGroupPolicy」というデフォルトのグループポリシーは、常にセキュリティ アプライアンス上に存在します。ただし、このデフォルトのグループポリシーを有効にするには、このポリシーを使用するようにセキュリティ アプライアンスを設定する必要があります。設定方法については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

DefaultGroupPolicy には、次の AVP が含まれています。

アトリビュート	デフォルト値
wins-server	none
dns-server	none
vpn-access-hours	unrestricted
vpn-simultaneous-logins	3

アトリビュート	デフォルト値
vpn-idle-timeout	30 minutes
vpn-session-timeout	none
vpn-filter	none
vpn-tunnel-protocol	IPSec WebVPN
ip-comp	disable
re-xauth	disable
group-lock	none
pfs	disable
client-access-rules	none
banner	none
password-storage	disabled
ipsec-udp	disabled
ipsec-udp-port	10000
backup-servers	keep-client-config
split-tunnel-policy	tunnelall
split-tunnel-network-list	none
default-domain	none
split-dns	none
client-firewall	none
secure-unit-authentication	disabled
user-authentication	disabled
user-authentication-idle-timeout	none
ip-phone-bypass	disabled
leap-bypass	disabled
nem	disabled

例

次の例は、「FirstGroup」という内部グループポリシーを作成する方法を示しています。

```
hostname(config)# group-policy FirstGroup internal
```

次の例は、「ExternalGroup」という外部グループポリシー、「BostonAAA」という AAA サーバ グループ、および「12345678」というパスワードを作成する方法を示しています。

```
hostname(config)# group-policy ExternalGroup external server-group BostonAAA password
12345678
```

関連コマンド

コマンド	説明
clear configure 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コンフィギュレーションを削除します。
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。

group-policy attributes

グループポリシー アトリビュート モードに入るには、グローバル コンフィギュレーション モードで **group-policy attributes** コマンドを使用します。グループポリシーからすべてのアトリビュートを削除するには、このコマンドの **no** 形式を使用します。アトリビュート モードでは、指定したグループポリシーの AVP を設定できます。

group-policy *name* **attributes**

no group-policy *name* **attributes**

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

アトリビュート モードのコマンドのシンタックスには、共通する次の特性があります。

- **no** 形式は、アトリビュートを実行コンフィギュレーションから削除し、値を別のグループポリシーから継承できるようにします。
- **none** キーワードは、実行コンフィギュレーションのアトリビュートをヌル値に設定して、値を継承できないようにします。
- ブール アトリビュートには、イネーブルまたはディセーブルになっている設定のための明示的なシンタックスがあります。

例

次の例は、「FirstGroup」というグループポリシーのグループポリシー アトリビュート モードに入る方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)#
```

関連コマンド

コマンド	説明
clear configure 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コンフィギュレーションを削除します。
group-policy	グループポリシーを作成、編集、または削除します。
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。

gtp-map

GTP のパラメータの定義に使用する特定のマップを指定するには、グローバル コンフィギュレーション モードで **gtp-map** コマンドを使用します。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。

gtp-map *map_name*

no gtp-map *map_name*

（注） GTP 検査には、特別なライセンスが必要です。セキュリティ アプライアンス上で **gtp-map** コマンドを入力する場合、必要なライセンスを持っていないときは、セキュリティ アプライアンス上にエラー メッセージが表示されます。

シンタックスの説明

map_name	GTP マップの名前。

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

GPRS は、既存の GSM ネットワークを統合するために設計されたデータ ネットワーク アーキテクチャです。モバイル ユーザに対して、企業ネットワークとインターネットにアクセスするためのパケット スイッチ データ サービスを中断なく提供します。GTP の概要や、セキュリティ アプライアンスがワイヤレス ネットワーク上でセキュアなアクセスを保証する仕組みについては、『*Cisco Security Appliance Command Line Configuration Guide*』の「Applying Application Layer Protocol Inspection」の章を参照してください。

gtp-map コマンドを使用して、GTP のパラメータの定義に使用する特定のマップを指定します。このコマンドを入力すると、システムがコンフィギュレーション モードに入って、個々のマップを定義するためのさまざまなコマンドを入力できるようになります。GTP マップを定義したら、**inspect gtp** コマンドを使用してマップをイネーブルにします。**class-map**、**policy-map**、および **service-policy** の各コマンドを使用して、トラフィックのクラスを定義し、**inspect** コマンドをクラスに適用し、ポリシーを 1 つまたはそれ以上のインターフェイスに適用します。

表 5-1　GTP マップ コンフィギュレーションのコマンド

コマンド	説明
description	GTP コンフィギュレーション マップの説明を指定します。
drop	ドロップするメッセージ ID、APN、または GTP バージョンを指定します。
help	GTP マップ コンフィギュレーションのコマンドのヘルプを表示します。
mcc	3 桁の Mobile Country Code（000 ～ 999）を指定します。1 桁または 2 桁の値を入力した場合は、先頭に 00 または 0 が付加されます。
message-length	メッセージの最小長と最大長を指定します。
permit errors	エラーのあるパケットまたは GTP バージョンの異なるパケットを許可します。
request-queue	キューに入れることができる要求の最大数を指定します。
timeout (gtp-map)	GSN、PDP コンテキスト、要求、シグナリング接続、およびトンネルのアイドル タイムアウトを指定します。
tunnel-limit	使用可能なトンネルの最大数を指定します。

例

次の例は、**gtp-map** コマンドを使用して、GTP のパラメータの定義に使用する特定のマップ（gtp-policy）を指定する方法を示しています。

```
hostname(config)# gtp-map qtp-policy
hostname(config-gtpmap)#
```

次の例は、アクセスリストを使用して GTP トラフィックを識別し、GTP マップを定義し、ポリシーを定義して、そのポリシーを外部インターフェイスに適用する方法を示しています。

```
hostname(config)# access-list gtp-acl permit udp any any eq 3386
hostname(config)# access-list gtp-acl permit udp any any eq 2123
hostname(config)# class-map gtp-traffic
hostname(config-cmap)# match access-list gtp-acl
hostname(config-cmap)# exit
hostname(config)# gtp-map gtp-policy
hostname(config-gtpmap)# request-queue 300
hostname(config-gtpmap)# permit mcc 111 mnc 222
hostname(config-gtpmap)# message-length min 20 max 300
hostname(config-gtpmap)# drop message 20
hostname(config-gtpmap)# tunnel-limit 10000
hostname(config)# policy-map inspection_policy
hostname(config-pmap)# class gtp-traffic
hostname(config-pmap-c)# inspect gtp gtp-policy
hostname(config)# service-policy inspection_policy outside
```

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。
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。
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。

help

指定したコマンドのヘルプ情報を表示するには、ユーザ EXEC モードで **help** コマンドを使用します。

help {*command* | **?**}

シンタックスの説明

command	CLI ヘルプの表示対象となるコマンドを指定します。
?	現在の特権レベルとモードで利用できるコマンドをすべて表示します。

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
ユーザ 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

help コマンドは、すべてのコマンドについてヘルプ情報を表示します。個々のコマンドについてのヘルプは、***help*** コマンドの後にコマンド名を入力することで、表示できます。コマンド名を指定しないで ***?*** を代わりに入力を入力すると、現在の特権レベルとモードで使用可能なコマンドがすべて表示されます。

pager コマンドがイネーブルになっている場合は、24 行が表示されたときに、表示が一時停止して次のプロンプトが表示されます。

```
<--- More --->
```

More プロンプトは UNIX の **more** コマンドと同様のシンタックスを使用します。このシンタックスを次に示します。

- 次のテキスト画面を表示するには、**Space** キーを押す。
- 次の行を表示するには、**Enter** キーを押す。
- コマンド ラインに戻るには、**q** キーを押す。

例

次の例は、***rename*** コマンドのヘルプを表示する方法を示しています。

```
hostname# help rename

USAGE:

        rename /noconfirm [{disk0:|disk1:|flash:}] <source path> [{disk0:|disk1:
|flash:}] <destination path>

DESCRIPTION:

rename          Rename a file

SYNTAX:

/noconfirm                      No confirmation
{disk0:|disk1:|flash:} Optional parameter that specifies the filesystem
<source path>           Source file path
<destination path>      Destination file path

hostname#
```

次の例は、コマンド名と疑問符を入力してヘルプを表示する方法を示しています。

```
hostname(config)# enable ?
usage: enable password <pwd> [encrypted]
```

コア コマンド（**show**、**no**、**clear** 以外のコマンド）についてのヘルプは、コマンド プロンプトで **?** を入力します。

```
hostname(config)# ?
aaa             Enable, disable, or view TACACS+ or RADIUS
                user authentication, authorization and accounting
…
```

関連コマンド

コマンド	説明
show version	オペレーティング システム ソフトウェアに関する情報を表示します。

homepage

この WebVPN ユーザまたはグループポリシーに対して、ログイン後すぐに表示する Web ページの URL を指定するには、WebVPN モードで **homepage** コマンドを使用します。WebVPN モードには、グループポリシー モードまたはユーザ名モードから入ります。設定済みのホーム ページ（**homepage none** コマンドを発行して作成されたヌル値を含む）を削除するには、このコマンドの **no** 形式を使用します。**no** オプションを使用すると、値を別のグループポリシーから継承できます。ホーム ページを継承しないようにするには、**homepage none** コマンドを使用します。

homepage {value *url-string* **| none}**

no homepage

シンタックスの説明

none	WebVPN ホーム ページを使用しないことを指定します。ヌル値を設定して、ホーム ページを拒否します。ホーム ページを継承しないようにします。
value *url-string*	ホーム ページの URL を指定します。文字列は、http:// または https:// で始まる必要があります。

デフォルト

デフォルトのホーム ページはありません。

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
WebVPN 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。

例

次の例は、FirstGroup というグループポリシーのホーム ページとして www.example.com を指定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# homepage value http://www.example.com
```

関連コマンド

コマンド	説明
webvpn	グループポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。WebVPN モードに入って、グループポリシーまたはユーザ名に適用するパラメータを設定できるようにします。

hostname

セキュリティ アプライアンスのホスト名を設定するには、グローバル コンフィギュレーション モードで **hostname** コマンドを使用します。デフォルトのホスト名に戻すには、このコマンドの **no** 形式を使用します。ホスト名はコマンドライン プロンプトとして表示されます。複数のデバイスに対してセッションを確立している場合は、ホスト名を見ることでコマンドの入力場所を把握できます。

hostname *name*

no hostname [*name*]

シンタックスの説明

name	最大 63 文字のホスト名を指定します。ホスト名の先頭と末尾はアルファベットまたは数字にする必要があります。それ以外の部分に使用できる文字はアルファベット、数字、またはハイフンのみです。

デフォルト

デフォルトのホスト名はプラットフォームによって異なります。

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
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)	アルファベット以外の文字（ハイフンを除く）が使用不可になりました。

使用上のガイドライン

マルチ コンテキスト モードの場合、システム実行スペースに設定したホスト名は、すべてのコンテキストのコマンドライン プロンプトに表示されます。

コンテキスト内にオプションで設定したホスト名は、コマンドラインに表示されませんが、**banner** コマンドの **$(hostname)** トークンに使用できます。

例

次の例では、ホスト名を firewall1 に設定します。

```
hostname(config)# hostname firewall1
firewall1(config)#
```

関連コマンド

コマンド	説明
banner	ログイン バナー、「今日のお知らせ」バナー、またはイネーブル バナーを設定します。
domain-name	デフォルトのドメイン名を設定します。

html-content-filter

このユーザまたはグループポリシーに対して、WebVPN セッションの Java、ActiveX、イメージ、スクリプト、クッキーをフィルタリングするには、WebVPN モードで **html-content-filter** コマンドを使用します。WebVPN モードには、グループポリシー モードまたはユーザ名モードから入ります。コンテンツ フィルタを削除するには、このコマンドの **no** 形式を使用します。すべてのコンテンツ フィルタ（**html-content-filter none** コマンドを発行して作成されたヌル値を含む）を削除するには、引数を指定しないでこのコマンドの **no** 形式を使用します。**no** オプションを使用すると、値を別のグループポリシーから継承できます。html コンテンツ フィルタを継承しないようにするには、**html-content-filter none** コマンドを使用します。

html-content-filter {**java** | **images** | **scripts** | **cookies** | **none**}

no html-content-filter [**java** | **images** | **scripts** | **cookies** | **none**]

シンタックスの説明

cookies	イメージからクッキーを削除して、限定的な広告フィルタリングとプライバシーを実現します。
images	イメージへの参照を削除します（<IMG> タグを削除します）。
java	Java と ActiveX への参照を削除します（<EMBED>、<APPLET>、および <OBJECT> タグを削除します）。
none	フィルタリングを実行しないことを指定します。ヌル値を設定して、フィルタリングを拒否します。フィルタリングの値を継承しないようにします。
scripts	スクリプトへの参照を削除します（<SCRIPT> タグを削除します）。

デフォルト

フィルタリングは行われません。

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
WebVPN 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

コマンドを 2 回使用すると、先行する設定値が上書きされます。

例

次の例は、FirstGroup というグループポリシーに対して、JAVA、ActiveX、クッキー、およびイメージのフィルタリングを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# html-content-filter java cookies images
```

関連コマンド

コマンド	説明
webvpn (group-policy, username)	グループポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。WebVPN モードに入って、グループポリシーまたはユーザ名に適用するパラメータを設定できるようにします。
webvpn	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。WebVPN のグローバル コンフィギュレーション値を設定できます。

http

セキュリティ アプライアンスの内部にある HTTP サーバにアクセスできるホストを指定するには、グローバル コンフィギュレーション モードで **http** コマンドを使用します。1 つまたは複数のホ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。このアトリビュートをコンフィギュレーションから削除するには、引数を指定しないでこのコマンドの **no** 形式を使用します。

http *ip_address subnet_mask interface_name*

no http

シンタックスの説明

interface_name	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 インターフェイスの名前を指定します。
ip_address	HTTP サーバにアクセスできるホストの IP アドレスを指定します。
subnet_mask	HTTP サーバにアクセスできるホストのサブネット マスクを指定します。

デフォルト

HTTP サーバにアクセスできるホストは指定されていません。

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

次の例は、IP アドレス 10.10.99.1 およびサブネット マスク 255.255.255.255 のホストが外部インターフェイス経由で HTTP サーバにアクセスできるようにする方法を示しています。

```
hostname(config)# http 10.10.99.1 255.255.255.255 outside
```

次の例は、すべてのホストが外部インターフェイス経由で HTTP サーバにアクセスできるようにする方法を示しています。

```
hostname(config)# http 0.0.0.0 0.0.0.0 outside
```

関連コマンド

コマンド	説明
clear configure http	HTTP コンフィギュレーションを削除します。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ホストを削除します。
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。

http authentication-certificate

HTTPS 接続を確立しようとするユーザに、証明書による認証を要求するには、グローバル コンフィギュレーション モードで **http authentication-certificate** コマンドを使用します。アトリビュートをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。コンフィギュレーションからすべての **http authentication-certificate** コマンドを削除するには、引数を指定しないで **no** 形式を使用します。

セキュリティ アプライアンスは、PKI トラスト ポイントに対して証明書を検証します。証明書が検証に合格しなかった場合、セキュリティ アプライアンスは SSL 接続を閉じます。

http authentication-certificate *interface*

no http authentication-certificate [*interface*]

シンタックスの説明

interface	証明書認証を要求するセキュリティ アプライアンス上のインターフェイスを指定します。

デフォルト

HTTP 証明書認証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

証明書認証はインターフェイスごとに設定できます。その結果、信頼できるインターフェイスまたは内部インターフェイス上の接続については証明書の提示が不要になります。コマンドを複数回使用すれば、複数のインターフェイス上で証明書認証をイネーブルにできます。

URL は検証後に判明します。そのため、検証は WebVPN と ASDM アクセスの両方に影響します。

ASDM は、この値のほかに、独自の認証方式を使用します。つまり、証明書認証とユーザ名 / パスワード認証の両方が設定されている場合は、両方の認証を要求し、証明書認証がディセーブルの場合は、ユーザ名 / パスワード認証のみを要求します。

例

次の例は、outside と external というインターフェイスに接続しようとするクライアントに証明書認証を要求する方法を示しています。

```
hostname(config)# http authentication-certificate inside
hostname(config)# http authentication-certificate external
```

関連コマンド

コマンド	説明
clear configure http	HTTP コンフィギュレーションを削除します。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ホストを削除します。
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 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。

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するには、グローバル コンフィギュレーション モードで **http redirect** コマンドを使用します。指定した http redirect コマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。すべての http redirect コマンドをコンフィギュレーションから削除するには、引数を指定しないでこのコマンドの **no** 形式を使用します。

http redirect *interface* [*port*]

no http redirect [*interface*]

シンタックスの説明

interface	セキュリティ アプライアンスが HTTP 要求を HTTPS にリダイレクトする対象となるインターフェイスを指定します。
port	セキュリティ アプライアンスが HTTP 要求をリスンするポートを指定します。HTTP 要求は後で HTTPS にリダイレクトされます。デフォルトでは、ポート 80 上でリスンします。

デフォルト

HTTP リダイレクト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　インターフェイスが、HTTP を許可するアクセスリストを要求します。要求がない場合、セキュリティ アプライアンスは、ポート 80 または HTTP 用に設定した他のポートすべてをリスンしません。

例　次の例は、デフォルト ポート 80 のままで、内部インターフェイスの HTTP リダイレクトを設定する方法を示しています。

```
hostname(config)# http redirect inside
```

関連コマンド

コマンド	説明
clear configure http	HTTP コンフィギュレーションを削除します。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ホストを削除します。
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 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。

http server enable

セキュリティ アプライアンスの HTTP サーバをイネーブルにするには、グローバル コンフィギュレーション モードで **http server enable** コマンドを使用します。HTTP サーバ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。

http server enable

no http server enable

デフォルト

HTTP サーバ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
既存	このコマンドは既存のものです。

例

次の例は、HTTP サーバをイネーブルにする方法を示しています。

```
hostname(config)# http server enable
```

関連コマンド

コマンド	説明
clear configure http	HTTP コンフィギュレーションを削除します。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ホストを削除します。
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。
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。

http-map

高度な HTTP 検査のパラメータを適用するための HTTP マップを作成するには、グローバル コンフィギュレーション モードで **http-map** コマンドを使用します。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。

http-map *map_name*

no http-map *map_name*

シンタックスの説明

map_name	HTTP マップの名前。

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)	このコマンドは 7.0(1) で導入されました。

使用上のガイドライン

アプリケーション ファイアウォールとしても知られる高度な HTTP 検査機能は、HTTP メッセージが RFC 2616 に準拠していること、RFC で定義およびサポートされている拡張方式を使用していること、および他のさまざまな基準を満たしていることを確認します。この機能を使用すると、攻撃者が HTTP メッセージを使用してネットワーク セキュリティ ポリシーを回避することを防止できます。

（注） HTTP マップを使用して HTTP 検査をイネーブルにすると、デフォルトでは、アクション reset および log を使用した厳密な HTTP 検査がイネーブルになります。検査に合格しない場合に実行されるアクションは変更できますが、HTTP マップがイネーブルのままである限り、厳密な検査をディセーブルにすることはできません。

多くの場合、基準と、その基準が満たされないときのセキュリティ アプライアンスの応答を設定できます。HTTP メッセージに適用できる基準には、次のものがあります。

- リスト（設定可能）に挙げられているメソッドを含んでいない。
- メッセージ本文のサイズが、制限値（設定可能）以下である。
- 要求と応答のメッセージ ヘッダーのサイズが、制限値（設定可能）以下である。
- URI の長さが制限値（設定可能）以下である。
- メッセージ本文の content-type が、ヘッダーと一致している。

- 応答メッセージの content-type が、要求メッセージの accept-type フィールドと一致している。
- メッセージの content-type が、事前定義済みの内部リストに挙げられている。
- メッセージが、RFC による HTTP 形式の基準を満たしている。
- 選択したサポート可能アプリケーションが存在している（または、存在していない）。
- 選択した符号化タイプが存在している（または、存在していない）。

（注） 基準を満たさないメッセージに対して指定できるアクションは、**allow**、**reset**、**drop** などのさまざまなコンフィギュレーション コマンドを使用して設定します。これらのアクションに加えて、イベントをログに記録するかどうかも指定できます。

表 5-2 は、HTTP マップ コンフィギュレーション モードで使用可能なコンフィギュレーション コマンドを要約しています。エントリをクリックするとコマンドのページが開き、各コマンドの詳細なシンタックスが表示されます。

表 5-2　HTTP マップ コンフィギュレーションのコマンド

コマンド	説明
content-length	HTTP コンテンツの長さに基づいた検査をイネーブルにします。
content-type-verification	HTTP コンテンツのタイプに基づいた検査をイネーブルにします。
max-header-length	HTTP ヘッダーの長さに基づいた検査をイネーブルにします。
max-uri-length	URI の長さに基づいた検査をイネーブルにします。
port-misuse	ポート不正使用アプリケーション検査をイネーブルにします。
request-method	HTTP 要求方式に基づいた検査をイネーブルにします。
strict-http	厳密な HTTP 検査をイネーブルにします。
transfer-encoding	転送符号化タイプに基づいた検査をイネーブルにします。

例

次の出力例は、HTTP トラフィックを識別し、HTTP マップを定義し、ポリシーを定義して、そのポリシーを外部インターフェイスに適用する方法を示しています。

```
hostname(config)# class-map http-port
hostname(config-cmap)# match port tcp eq 80
hostname(config-cmap)# exit
hostname(config)# http-map inbound_http
hostname(config-http-map)# content-length min 100 max 2000 action reset log
hostname(config-http-map)# content-type-verification match-req-rsp reset log
hostname(config-http-map)# max-header-length request bytes 100 action log reset
hostname(config-http-map)# max-uri-length 100 action reset log
hostname(config-http-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class http-port
hostname(config-pmap-c)# inspect http inbound_http
hostname(config-pmap-c)# exit
hostname(config-pmap)# exit
hostname(config)# service-policy inbound_policy interface outside
```

この例では、次のコンテンツを含んでいるトラフィックをセキュリティ アプライアンスが検出したときに、接続をリセットして syslog エントリを作成します。

- 100 バイト未満または 2,000 バイトを超えるメッセージ
- サポートされていないコンテンツ タイプ
- 100 バイトを超える HTTP ヘッダー
- 100 バイトを超える URI

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 appfw	HTTP アプリケーション検査に関する詳細情報を表示します。
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。
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。

http-proxy

HTTP プロキシ サーバを設定するには、WebVPN モードで **http-proxy** コマンドを使用します。HTTP プロキシ サーバをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

このプロキシ サーバは、セキュリティ アプライアンスが HTTP 要求に使用する外部プロキシ サーバです。

http-proxy *address* [*port*]

no http-proxy

シンタックスの説明

address	外部 HTTP プロキシ サーバの IP アドレスを指定します。
port	HTTP プロキシ サーバが使用するポートを指定します。デフォルト ポートは 80 です。値を指定しない場合、セキュリティ アプライアンスはこのポートを使用します。

デフォルト

HTTP プロキシ サーバは、デフォルトでは設定されていません。

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
Webvpn	•	—	•	—	—

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

次の例は、ポート 80 を使用する IP アドレス 10.10.10.7 の HTTP プロキシ サーバを設定する方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# http-proxy 10.10.10.7
```

https-proxy

HTTPS プロキシ サーバを設定するには、WebVPN モードで **https-proxy** コマンドを使用します。HTTPS プロキシ サーバをコンフィギュレーションから削除するには、このコマンドの no 形式を使用します。

このプロキシ サーバは、セキュリティ アプライアンスが HTTPS 要求に使用する外部プロキシ サーバです。

https-proxy *address* [*port*]

no https-proxy

シンタックスの説明

address	外部 HTTPS プロキシ サーバの IP アドレスを指定します。
port	HTTPS プロキシ サーバが使用するポートを指定します。デフォルト ポートは 443 です。値を指定しない場合、セキュリティ アプライアンスはこのポートを使用します。

デフォルト

HTTPS プロキシ サーバは、デフォルトでは設定されていません。

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
Webvpn	•	—	•	—	—

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

次の例は、ポート 443 を使用する IP アドレス 10.10.10.1 の HTTPS プロキシ サーバを設定する方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# https-proxy 10.10.10.1 443
```

hw-module module recover

TFTP サーバからインテリジェント SSM（たとえば、AIP SSM）にリカバリ ソフトウェア イメージをロードする場合や、TFTP サーバにアクセスするためのネットワーク設定値を設定する場合は、特権 EXEC モードで **hw-module module recover** コマンドを使用します。SSM でローカル イメージをロードできないような場合は、このコマンドを使用して SSM を回復することが必要となる場合があります。このコマンドは、インターフェイスの SSM（4GE SSM など）に対しては使用できません。

hw-module module 1 recover {***boot*** | ***stop*** | ***configure*** [***url*** *tfp_url* | ***ip*** *port_ip_address* | ***gateway*** *gateway_ip_address* | ***vlan*** *vlan_id*]}

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。
boot	この SSM のリカバリを開始し、***configure*** 設定に応じてリカバリ イメージをダウンロードします。その後、SSM が新しいイメージからリブートされます。
configure	リカバリ イメージをダウンロードするためのネットワーク パラメータを設定します。***configure*** キーワードの後ろにネットワーク パラメータを入力しない場合は、情報を入力するよう求められます。
gateway *gateway_ip_address*	（オプション）SSM 管理インターフェイスを通じて TFTP サーバにアクセスするためのゲートウェイ IP アドレス。
ip *port_ip_address*	（オプション）SSM 管理インターフェイスの IP アドレス。
stop	リカバリ アクションを停止し、リカバリ イメージのダウンロードを停止します。SSM　は元のイメージからブートします。このコマンドは、**hw-module module boot** コマンドを使用してリカバリを開始してから 30 ～ 45 秒以内に入力する必要があります。この期間を過ぎてから **stop** コマンドを発行すると、SSM が応答しなくなるなど、予期しない結果が生じる場合があります。
url *tfp_url*	（オプション）TFTP サーバ上のイメージの URL。この形式は次のとおりです。 ***tftp://****server*/[*path*/]*filename*
vlan *vlan_id*	（オプション）管理インターフェイスの VLAN ID 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
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できるのは、SSM が Up、Down、Unresponsive、または Recovery 状態にある場合のみです。状態については、**show module** コマンドを参照してください。

例　次の例では、TFTP サーバからイメージをダウンロードするように SSM を設定します。

```
hostname# hw-module module 1 recover configure
Image URL [tftp://127.0.0.1/myimage]: tftp://10.1.1.1/ids-newimg
Port IP Address [127.0.0.2]: 10.1.2.10
Port Mask [255.255.255.254]: 255.255.255.0
Gateway IP Address [1.1.2.10]: 10.1.2.254
VLAN ID [0]: 100
```

次の例では、SSM を回復します。

```
hostname# hw-module module 1 recover boot
The module in slot 1 will be recovered.  This may
erase all configuration and all data on that device and
attempt to download a new image for it.
Recover module in slot 1? [confirm]
```

関連コマンド

コマンド	説明
debug module-boot	SSM のブート プロセスに関するデバッグ メッセージを表示します。
hw-module module reset	SSM をシャットダウンして、ハードウェア リセットを実行します。
hw-module module reload	インテリジェント SSM ソフトウェアをリロードします。
hw-module module shutdown	SSM ソフトウェアをシャットダウンして、コンフィギュレーション データを失わずに電源をオフにできる状態にします。
show module	SSM の情報を表示します。

hw-module module reload

インテリジェント SSM ソフトウェア（たとえば、AIP SSM）をリロードするには、特権 EXEC モードで **hw-module module reload** コマンドを使用します。このコマンドは、インターフェイスの SSM（4GE SSM など）に対しては使用できません。

hw-module module 1 ***reload***

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。

使用上のガイドライン

このコマンドが有効となるのは、SSM の状態が Up の場合のみです。状態については、**show module** コマンドを参照してください。

このコマンドは、同じくハードウェア リセットを実行する **hw-module module reset** コマンドとは異なります。

例

次の例では、スロット 1 の SSM をリロードします。

```
hostname# hw-module module 1 reload
Reload module in slot 1? [confirm] y
Reload issued for module in slot 1
%XXX-5-505002: Module in slot 1 is reloading.  Please wait...
%XXX-5-505006: Module in slot 1 is Up.
```

関連コマンド

コマンド	説明
debug module-boot	SSM のブート プロセスに関するデバッグ メッセージを表示します。
hw-module module recover	リカバリ イメージを TFTP サーバからロードして、インテリジェント SSM を回復します。
hw-module module reset	SSM をシャットダウンして、ハードウェア リセットを実行します。
hw-module module shutdown	SSM ソフトウェアをシャットダウンして、コンフィギュレーション データを失わずに電源をオフにできる状態にします。
show module	SSM の情報を表示します。

hw-module module reset

SSM ハードウェアをシャットダウンし、リセットするには、特権 EXEC モードで **hw-module module reset** コマンドを使用します。

hw-module module 1 ***reset***

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。

使用上のガイドライン

このコマンドが有効となるのは、SSM の状態が Up、Down、Unresponsive、または Recover の場合のみです。状態については、**show module** コマンドを参照してください。

SSM が Up 状態にある場合、**hw-module module reset** コマンドを使用すると、リセットする前にソフトウェアをシャットダウンするよう求められます。

インテリジェント SSM（たとえば、AIP SSM）を回復するには、**hw-module module recover** コマンドを使用します。SSM が Recover 状態にあるときに **hw-module module reset** を入力しても、SSM はリカバリ プロセスを中断しません。**hw-module module reset** コマンドは、SSM のハードウェア リセットを実行します。ハードウェア リセット後に、SSM のリカバリが続行されます。SSM がハングした場合は、リカバリ中でも SSM をリセットできます。ハードウェア リセットにより、問題が解決する場合があります。

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

例

次の例では、Up 状態にあるスロット 1 の SSM をリセットします。

```
hostname# hw-module module 1 reset
The module in slot 1 should be shut down before
resetting it or loss of configuration may occur.
Reset module in slot 1? [confirm] y
Reset issued for module in slot 1
%XXX-5-505001: Module in slot 1 is shutting down.  Please wait...
%XXX-5-505004: Module in slot 1 shutdown is complete.
%XXX-5-505003: Module in slot 1 is resetting.  Please wait...
%XXX-5-505006: Module in slot 1 is Up.
```

関連コマンド

コマンド	説明
debug module-boot	SSM のブート プロセスに関するデバッグ メッセージを表示します。
hw-module module recover	リカバリ イメージを TFTP サーバからロードして、インテリジェント SSM を回復します。
hw-module module reload	インテリジェント SSM ソフトウェアをリロードします。
hw-module module shutdown	SSM ソフトウェアをシャットダウンして、コンフィギュレーション データを失わずに電源をオフにできる状態にします。
show module	SSM の情報を表示します。

hw-module module shutdown

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

hw-module module 1 shutdown

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。

使用上のガイドライン

SSM ソフトウェアをシャットダウンすると、コンフィギュレーション データを失わずに SSM の電源を安全にオフにできる状態になります。

このコマンドが有効となるのは、SSM の状態が Up または Unresponsive の場合のみです。状態については、**show module** コマンドを参照してください。

例

次の例では、スロット 1 の SSM をシャットダウンします。

```
hostname# hw-module module 1 shutdown
Shutdown module in slot 1? [confirm] y
Shutdown issued for module in slot 1
hostname#
%XXX-5-505001: Module in slot 1 is shutting down.  Please wait...
%XXX-5-505004: Module in slot 1 shutdown is complete.
```

関連コマンド

コマンド	説明
debug module-boot	SSM のブート プロセスに関するデバッグ メッセージを表示します。
hw-module module recover	リカバリ イメージを TFTP サーバからロードして、インテリジェント SSM を回復します。
hw-module module reload	インテリジェント SSM ソフトウェアをリロードします。
hw-module module reset	SSM をシャットダウンして、ハードウェア リセットを実行します。
show module	SSM の情報を表示します。

icmp

セキュリティ アプライアンス インターフェイスで終端する ICMP トラフィックに対してアクセス規則を設定するには、**icmp** コマンドを使用します。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。

icmp {**permit** | **deny**} *ip_address net_mask* [*icmp_type*] *if_name*

no icmp {**permit** | **deny**} *ip_address net_mask* [*icmp_type*] *if_name*

シンタックスの説明

deny	条件に合致している場合、アクセスを拒否します。
icmp_type	（オプション）ICMP メッセージ タイプ（表 5-3 を参照）。
if_name	インターフェイス名。
ip_address	ICMP メッセージをインターフェイスに送信するホストの IP アドレス。
net_mask	*ip_address* に適用されるマスク。
permit	条件に合致している場合、アクセスを許可します。

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、セキュリティ アプライアンス インターフェイスへのICMP トラフィックをすべて許可します。ただし、デフォルトでは、セキュリティ アプライアンスはブロードキャスト アドレス宛ての ICMP エコー要求には応答しません。また、セキュリティ アプライアンスは、保護されたインターフェイス上の宛先に対する、外部インターフェイスで受信した ICMP メッセージを拒否します。

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)	このコマンドは既存のものです。

使用上のガイドライン

icmp コマンドは、すべてのセキュリティ アプライアンス インターフェイスで終端する ICMP トラフィックを制御します。ICMP コントロール リストが設定されていない場合、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（外部インターフェイスを含む）で終端する ICMP トラフィックをすべて受け入れます。ただし、デフォルトでは、セキュリティ アプライアンスはブロードキャスト アドレス宛ての ICMP エコー要求には応答しません。

icmp deny コマンドは、インターフェイスへの ping をディセーブルにし、**icmp permit** コマンドは、インターフェイスへの ping をイネーブルにします。ping をディセーブルにすると、セキュリティ アプライアンスがネットワーク上で検出できなくなります。これは、設定可能なプロキシ ping とも呼ばれます。

保護されたインターフェイス上の宛先に向けてセキュリティ アプライアンス*経由で*ルーティングされる ICMP トラフィックについては、**access-list extended** コマンドまたは **access-group** コマンドを使用します。

ICMP 到達不能メッセージ タイプ（タイプ 3）は、許可することを推奨します。ICMP 到達不能メッセージを拒否すると、Path MTU Discovery がディセーブルになるため、IPSec トラフィックと PPTP のトラフィックが停止される場合があります。Path MTU Discovery の詳細については、RFC 1195 と RFC 1435 を参照してください。

ICMP コントロール リストがインターフェイスに設定されている場合、セキュリティ アプライアンスは、指定された ICMP トラフィックと最初に一致したエントリを使用し、それ以外の当該インターフェイス上の ICMP トラフィックをすべて暗黙的に拒否します。つまり、最初に一致したエントリが許可エントリの場合、その ICMP パケットは処理が続けられます。最初に一致したエントリが拒否エントリの場合、またはエントリが一致しなかった場合は、セキュリティ アプライアンスがその ICMP パケットを廃棄し、syslog メッセージを生成します。例外は、ICMP コントロール リストが設定されていない場合で、その場合は、**permit** ステートメントがあるものとみなされます。

表 5-3 に、サポートされている ICMP タイプの値を示します。

表 5-3　ICMP タイプのリテラル

ICMP タイプ	リテラル
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-request
14	timestamp-reply
15	information-request
16	information-reply
17	mask-request
18	mask-reply
31	conversion-error
32	mobile-redirect

例

次の例では、外部インターフェイスで、すべての ping 要求を拒否し、すべての到達不能メッセージを許可します。

```
hostname(config)# icmp permit any unreachable outside
```

次の例では、ホスト 172.16.2.15 またはサブネット 172.22.1.0/16 上のホストに、外部インターフェイスへの ping を許可します。

```
hostname(config)# icmp permit host 172.16.2.15 echo-reply outside
hostname(config)# icmp permit 172.22.1.0 255.255.0.0 echo-reply outside
hostname(config)# icmp permit any unreachable outside
```

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。

icmp-object

icmp-type オブジェクト グループを追加するには、icmp-type コンフィギュレーション モードで **icmp-object** コマンドを使用します。ネットワーク オブジェクト グループを削除するには、このコマンドの **no** 形式を使用します。

icmp-object *icmp_type*

no group-object *icmp_type*

シンタックスの説明

icmp_type	icmp-type 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
Icmp-type　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

icmp-object コマンドは、**object-group** コマンドと組み合せることで、icmp-type オブジェクトを定義します。このコマンドは、icmp-type コンフィギュレーション モードで使用されます。

ICMP タイプの番号と名前には、次のものがあります。

番号	ICMP タイプの名前
0	**echo-reply**
3	**unreachable**
4	**source-quench**
5	**redirect**
6	**alternate-address**
8	**echo**

番号	ICMP タイプの名前
9	**router-advertisement**
10	**router-solicitation**
11	**time-exceeded**
12	**parameter-problem**
13	**timestamp-request**
14	**timestamp-reply**
15	**information-request**
16	**information-reply**
17	**address-mask-request**
18	**address-mask-reply**
31	**conversion-error**
32	**mobile-redirect**

例

次の例は、icmp-type コンフィギュレーション モードで **icmp-object** コマンドを使用する方法を示しています。

```
hostname(config)# object-group icmp-type icmp_allowed
hostname(config-icmp-type)# icmp-object echo
hostname(config-icmp-type)# icmp-object time-exceeded
hostname(config-icmp-type)# exit
```

関連コマンド

コマンド	説明
clear configure object-group	すべての **object-group** コマンドをコンフィギュレーションから削除します。
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。

id-cert-issuer

このトラストポイントに関連付けられている CA から発行されたピア証明書をシステムで受け入れるかどうかを示すには、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 **id-cert-issuer** コマンドを使用します。トラストポイントに関連付けられている CA から発行された証明書を拒否するには、このコマンドの **no** 形式を使用します。このコマンドは、広く使用されるルート CA を表すトラストポイントに対して有用です。

id-cert-issuer

no id-cert-issuer

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

デフォルト設定はイネーブルです（ID 証明書は受け入れられます）。

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
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

このコマンドは、広く使用されるルート CA の下位 CA から発行された証明書のみを受け入れるようにする場合に使用します。この機能を使用可能にしない場合は、セキュリティ アプライアンスが、この発行者によって署名された IKE ピア証明書をすべて拒否します。

例

次の例では、central トラストポイントの暗号 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、central トラストポイントの発行者によって署名された ID 証明書の受け入れを管理者に許可します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# id-cert-issuer
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント サブモードに入ります。
default enrollment	登録パラメータをデフォルトに戻します。
enrollment retry count	登録要求の送信を再試行する回数を指定します。
enrollment retry period	登録要求の送信を試行するまでの待機時間を、分単位で指定します。
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。

igmp

インターフェイス上で IGMP 処理を初期化するには、インターフェイス コンフィギュレーション モードで **igmp** コマンドを使用します。インターフェイス上で IGMP 処理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。

igmp

no igmp

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

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
インターフェイス 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

実行コンフィギュレーションに表示されるのは、このコマンドの **no** 形式のみです。

例

次の例では、選択したインターフェイス上で IGMP 処理をディセーブルにします。

```
hostname(config-if)# no igmp
```

関連コマンド

コマンド	説明
show igmp groups	セキュリティ アプライアンスに直接接続される受信者を保持していて、IGMP を通じてラーニングされたマルチキャスト グループを表示します。
show igmp interface	インターフェイスのマルチキャスト情報を表示します。

igmp access-group

インターフェイスを利用するサブネット上のホストが加入できるマルチキャスト グループを制御するには、インターフェイス コンフィギュレーション モードで **igmp access-group** コマンドを使用します。インターフェイス上でグループ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。

igmp access-group *acl*

no igmp access-group *acl*

シンタックスの説明

acl	IP アクセスリストの名前。標準アクセスリスト、拡張アクセスリスト、またはその両方を指定できます。ただし、拡張アクセスリストを指定した場合、一致するのは宛先アドレスのみです。そのため、送信元には **any** を指定する必要があります。

デフォルト

インターフェイス上ですべてのグループに加入できます。

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
インターフェイス 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、インターフェイス コンフィギュレーション モードに変更されました。以前のバージョンでは、マルチキャスト インターフェイス コンフィギュレーション モードに入る必要がありましたが、このモードは使用できなくなりました。

例

次の例では、アクセスリスト 1 で許可されたホストだけがグループに加入できるようにします。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp access-group 1
```

関連コマンド

コマンド	説明
show igmp interface	インターフェイスのマルチキャスト情報を表示します。

igmp forward interface

すべての IGMP ホスト レポートの転送をイネーブルにし、指定したインターフェイスでメッセージが受信される状態にするには、インターフェイス コンフィギュレーション モードで **igmp forward interface** コマンドを使用します。転送を解除するには、このコマンドの **no** 形式を使用します。

igmp forward interface *if-name*

no igmp forward interface *if-name*

シンタックスの説明

if-name	インターフェイスの論理名。

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
インターフェイス 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、インターフェイス コンフィギュレーション モードに変更されました。以前のバージョンでは、マルチキャスト インターフェイス コンフィギュレーション モードに入る必要がありましたが、このモードは使用できなくなりました。

使用上のガイドライン

このコマンドを入力インターフェイス上で入力します。このコマンドはスタブ マルチキャスト ルーティング用であるため、このコマンドに PIM を同時に設定することはできません。

例

次の例では、IGMP ホスト レポートを現在のインターフェイスから指定のインターフェイスに転送します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp forward interface outside
```

関連コマンド

コマンド	説明
show igmp interface	インターフェイスのマルチキャスト情報を表示します。

igmp join-group

インターフェイスを、指定したグループのローカルに接続されたメンバーとして設定するには、インターフェイス コンフィギュレーション モードで **igmp join-group** コマンドを使用します。グループのメンバーシップをキャンセルするには、このコマンドの **no** 形式を使用します。

igmp join-group *group-address*

no igmp join-group *group-address*

シンタックスの説明

group-address	マルチキャスト グループの 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
インターフェイス 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、インターフェイス コンフィギュレーション モードに変更されました。以前のバージョンでは、マルチキャスト インターフェイス コンフィギュレーション モードに入る必要がありましたが、このモードは使用できなくなりました。

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 インターフェイスをマルチキャスト グループのメンバーとして設定します。**igmp join-group** コマンドを使用すると、セキュリティ アプライアンスは、指定されたマルチキャスト グループ宛てのマルチキャスト パケットを受け入れて、転送します。

マルチキャスト グループのメンバーにしないで、セキュリティ アプライアンスがマルチキャスト トラフィックを転送するように設定するには、**igmp static-group** コマンドを使用します。

例

次の例では、選択したインターフェイスが IGMP グループ 255.2.2.2 に加入するように設定します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp join-group 225.2.2.2
```

関連コマンド

コマンド	説明
igmp static-group	インターフェイスを、指定したマルチキャスト グループのスタティックに接続されたメンバーとして設定します。

igmp limit

IGMP の状態の数をインターフェイスごとに制限するには、インターフェイス コンフィギュレーション モードで **igmp limit** コマンドを使用します。デフォルトの制限に戻すには、このコマンドの **no** 形式を使用します。

igmp limit *number*

no igmp limit [*number*]

シンタックスの説明

number	インターフェイス上で許可する IGMP の状態の数。有効値の範囲は 0 ～ 500 です。デフォルト値は 500 です。値を 0 に設定すると、ラーニングされたグループが追加されなくなります。ただし、メンバーシップを手動で定義することは引き続き可能です（**igmp join-group** コマンドと **igmp static-group** コマンドを使用します）。

デフォルト

デフォルトは 500 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
インターフェイス 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。このコマンドにより、**igmp max-groups** コマンドは置き換えられました。

例

次の例では、インターフェイス上で加入できるホストの数を 250 に制限します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp limit 250
```

関連コマンド

コマンド	説明
igmp	インターフェイス上で IGMP 処理を初期化します。
igmp join-group	インターフェイスを、指定したグループのローカルに接続されたメンバーとして設定します。
igmp static-group	インターフェイスを、指定したマルチキャスト グループのスタティックに接続されたメンバーとして設定します。

igmp query-interval

インターフェイスが IGMP ホスト クエリー メッセージを送信する頻度を設定するには、インターフェイス コンフィギュレーション モードで **igmp query-interval** コマンドを使用します。デフォルトの頻度に戻すには、このコマンドの **no** 形式を使用します。

igmp query-interval *seconds*

no igmp query-interval *seconds*

シンタックスの説明

seconds	IGMP ホスト クエリー メッセージを送信する頻度（秒単位）。有効となる値の範囲は、1 ～ 3,600 秒です。デフォルトは 125 秒です。

デフォルト

デフォルトのクエリー間隔は 125 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
インターフェイス 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、インターフェイス コンフィギュレーション モードに変更されました。以前のバージョンでは、マルチキャスト インターフェイス コンフィギュレーション モードに入る必要がありましたが、このモードは使用できなくなりました。

使用上のガイドライン

マルチキャスト ルータは、ホスト クエリー メッセージを送信して、インターフェイスに接続されたネットワーク上のメンバーを含むマルチキャスト グループを検出します。ホストは、特定のグループ宛てのマルチキャスト パケットを受信する必要があることを示す IGMP レポート メッセージを使用して応答します。ホスト クエリー メッセージは、アドレス 224.0.0.1 および TTL 値 1 の all-hosts マルチキャスト グループに宛先指定されます。

IGMP ホスト クエリー メッセージを送信するルータは、LAN の指定ルータのみです。

- IGMP バージョン 1 の場合、指定ルータは、LAN 上で動作するマルチキャスト ルーティング プロトコルに応じて選定されます。
- IGMP バージョン 2 の場合、指定ルータは、サブネット上で最も低い IP アドレスを持つマルチキャスト ルータになります。

ルータがタイムアウト期間（期間は **igmp query-timeout** コマンドで制御される）にクエリーを受信しなかった場合は、そのルータがクエリー発行者になります。

注意　この値を変更すると、マルチキャスト転送に重大な影響を及ぼす場合があります。

例

次の例では、IGMP クエリー間隔を 120 秒に変更します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp query-interval 120
```

関連コマンド

コマンド	説明
igmp query-max-response-time	IGMP クエリーでアドバタイズされる最長応答期間を設定します。
igmp query-timeout	前のクエリー発行者がクエリーを停止してから、ルータがインターフェイスのクエリー発行者を引き継ぐまでのタイムアウト期間を設定します。

igmp query-max-response-time

IGMP クエリーでアドバタイズされる最長応答期間を指定するには、インターフェイス コンフィギュレーション モードで **igmp query-max-response-time** コマンドを使用します。応答期間を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。

igmp query-max-response-time *seconds*

no igmp query-max-response-time [*seconds*]

シンタックスの説明

seconds	IGMP クエリーでアドバタイズされる最長応答期間（秒単位）。有効な値は 1 ～ 25 秒です。デフォルト値は 10 秒です。

デフォルト

10 秒。

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
インターフェイス 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、インターフェイス コンフィギュレーション モードに変更されました。以前のバージョンでは、マルチキャスト インターフェイス コンフィギュレーション モードに入る必要がありましたが、このモードは使用できなくなりました。

使用上のガイドライン

このコマンドが有効となるのは、IGMP バージョン 2 または 3 が動作している場合のみです。

このコマンドは、応答者が IGMP クエリー メッセージに応答できる期間を制御します。この期間を過ぎると、ルータがグループを削除します。

例

次の例では、最長クエリー応答期間を 8 秒に変更します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp query-max-response-time 8
```

関連コマンド

コマンド	説明
igmp query-interval	インターフェイスが IGMP ホスト クエリー メッセージを送信する頻度を設定します。
igmp query-timeout	前のクエリー発行者がクエリーを停止してから、ルータがインターフェイスのクエリー発行者を引き継ぐまでのタイムアウト期間を設定します。

igmp query-timeout

前のクエリー発行者がクエリーを停止してから、インターフェイスがクエリー発行者を引き継ぐまでのタイムアウト期間を設定するには、インターフェイス コンフィギュレーション モードで **igmp query-timeout** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

igmp query-timeout *seconds*

no igmp query-timeout [*seconds*]

シンタックスの説明

seconds	前のクエリー発行者がクエリーを停止してから、ルータがクエリー発行者を引き継ぐまで待機する秒数。有効な値は 60 ～ 300 秒です。デフォルト値は 255 秒です。

デフォルト

デフォルトのクエリー間隔は 255 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
インターフェイス 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

このコマンドには IGMP バージョン 2 または 3 が必要です。

例

次の例では、最後にクエリーを受信してから、インターフェイスのクエリー発行者を引き継ぐまで 200 秒待機するようルータを設定します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp query-timeout 200
```

関連コマンド

コマンド	説明
igmp query-interval	インターフェイスが IGMP ホスト クエリー メッセージを送信する頻度を設定します。
igmp query-max-response-time	IGMP クエリーでアドバタイズされる最長応答期間を設定します。

igmp static-group

インターフェイスを、指定したマルチキャスト グループのスタティックに接続されたメンバーとして設定するには、インターフェイス コンフィギュレーション モードで **igmp static-group** コマンドを使用します。スタティック グループ エントリを削除するには、このコマンドの **no** 形式を使用します。

igmp static-group *group*

no igmp static-group *group*

シンタックスの説明

group	IP マルチキャスト グループ 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
インターフェイス 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

igmp static-group コマンドを使用して設定すると、セキュリティ アプライアンス インターフェイスは、指定されたグループそのものを宛先とするマルチキャスト パケットを受け入れずに、転送します。指定されたマルチキャスト グループ宛てのマルチキャスト パケットを受け入れて、転送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、**igmp join-group** コマンドを使用します。**igmp join-group** コマンドに **igmp static-group** コマンドと同じグループ アドレスを設定した場合は、**igmp join-group** コマンドが優先され、グループはローカルに加入しているグループのように動作します。

例

次の例では、選択したインターフェイスをマルチキャスト グループ 239.100.100.101 に追加します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp static-group 239.100.100.101
```

関連コマンド

コマンド	説明
igmp join-group	インターフェイスを、指定したグループのローカルに接続されたメンバーとして設定します。

igmp version

インターフェイスが使用する IGMP のバージョンを設定するには、インターフェイス コンフィギュレーション モードで **igmp version** コマンドを使用します。バージョン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。

igmp version {*1* | *2*}

no igmp version [*1* | *2*]

シンタックスの説明

1	IGMP バージョン 1。
2	IGMP バージョン 2。

デフォルト

IGMP バージョン 2。

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
インターフェイス 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、インターフェイス コンフィギュレーション モードに変更されました。以前のバージョンでは、マルチキャスト インターフェイス コンフィギュレーション モードに入る必要がありましたが、このモードは使用できなくなりました。

使用上のガイドライン

サブネット上のルータはすべて、同じバージョンの IGMP をサポートする必要があります。ホストは任意の IGMP バージョン（1 または 2）を使用できます。また、セキュリティ アプライアンスは、ホストの存在を検出して、適切にクエリーします。

igmp query-max-response-time コマンドや **igmp query-timeout** コマンドなど、一部のコマンドでは IGMP バージョン 2 が必要です。

例

次の例では、選択したインターフェイスが IGMP バージョン 1 を使用するように設定します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp version 1
```

関連コマンド

コマンド	説明
igmp query-max-response-time	IGMP クエリーでアドバタイズされる最長応答期間を設定します。
igmp query-timeout	前のクエリー発行者がクエリーを停止してから、ルータがインターフェイスのクエリー発行者を引き継ぐまでのタイムアウト期間を設定します。

ignore lsa mospf

ルータが link-state advertisement（LSA; リンクステート アドバタイズメント）のタイプ 6 Multicast OSPF（MOSPF）パケットを受信した際に、syslog メッセージを送信しないようにするには、ルータ コンフィギュレーション モードで **ignore lsa mospf** コマンドを使用します。syslog メッセージを送信する設定に戻すには、このコマンドの **no** 形式を使用します。

ignore lsa mospf

no ignore lsa mospf

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
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

タイプ 6 MOSPF パケットはサポート対象外です。

例

次の例では、LSA タイプ 6 MOSPF パケットが無視されるようにします。

```
hostname(config-router)# ignore lsa mospf
```

関連コマンド

コマンド	説明
show running-config router ospf	OSPF ルータ コンフィギュレーションを表示します。

imap4s

IMAP4S コンフィギュレーション モードに入るには、グローバル コンフィギュレーション モードで **imap4s** コマンドを使用します。IMAP4S コマンド モードで入力したコマンドをすべて削除するには、このコマンドの **no** 形式を使用します。

IMAP4 は、インターネット サーバがユーザ宛ての電子メールを受信および保管するためのクライアント / サーバ プロトコルです。ユーザ（または電子メール クライアント）は、メールのヘッダーおよび送信者のみを表示して、メールをダウンロードするかどうかを決めることができます。また、サーバ上に複数のフォルダやメールボックスを作成して操作する、メッセージを削除する、または特定部分やメッセージ全体を検索することもできます。メールを操作する間、IMAP はサーバに継続的にアクセスする必要があります。IMAP4S を使用すると、SSL 接続上で電子メールを受信できます。

imap4s

no 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

次の例は、IMAP4S コンフィギュレーション モードに入る方法を示しています。

```
hostname(config)# imap4s
hostname(config-imap4s)#
```

関連コマンド

コマンド	説明
clear configure imap4s	IMAP4S コンフィギュレーションを削除します。
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。

inspect ctiqbe

CTIQBE プロトコル検査をイネーブルにするには、クラス コンフィギュレーション モードで **inspect ctiqbe** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシーマップ コンフィギュレーション モードからアクセスできます。検査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。

inspect ctiqbe

no inspect ctiqbe

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
クラス 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)	このコマンドは 7.0(1) で導入されました。このコマンドにより、既存の **fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

inspect ctiqbe コマンドは、NAT、PAT、および双方向 NAT をサポートする CTIQBE プロトコル検査をイネーブルにします。これにより、Cisco IP SoftPhone と他の Cisco TAPI/JTAPI アプリケーションが Cisco CallManager と正常に連携動作して、セキュリティ アプライアンスを通じてコール セットアップを実行できるようになります。

Telephony Application Programming Interface（TAPI）と Java Telephony Application Programming Interface（JTAPI）は、多くの Cisco VoIP アプリケーションで使用されます。Computer Telephony Interface Quick Buffer Encoding（CTIQBE）は、Cisco TAPI Service Provider（TSP）が Cisco CallManager と通信するために使用します。

次に、CTIQBE アプリケーション検査を使用するときに適用される制限を要約します。

- CTIQBE アプリケーション検査では、**alias** コマンドを使用したコンフィギュレーションはサポートされません。
- CTIQBE コールのステートフル フェールオーバーはサポートされません。
- **debug ctiqbe** コマンドを使用すると、メッセージ伝送が遅延する場合があります。その結果、リアルタイム環境ではパフォーマンスに影響が及ぶ場合があります。このデバッグまたはロギングをイネーブルにした結果、Cisco IP SoftPhone においてセキュリティ アプライアンスからのコール セットアップを完了できなくなったと思われる場合は、Cisco IP SoftPhone を実行するシステム上で Cisco TSP 設定のタイムアウト値を増やします。
- CTIQBE アプリケーション検査では、複数の TCP パケットにフラグメント化された CTIQBE メッセージはサポートされません。

次に、特定のシナリオで CTIQBE アプリケーション検査を使用する場合に特に考慮が必要な事項を要約します。

- 2 つの Cisco IP SoftPhone が別々の Cisco CallManager に登録されている場合、各 Cisco CallManager はセキュリティ アプライアンスの別々のインターフェイスに接続されているため、これら 2 つの電話間のコールは失敗します。
- Cisco CallManager が Cisco IP SoftPhone よりもセキュリティの高いインターフェイス上にあり、Cisco CallManager IP アドレスの NAT または外部 NAT が必要になる場合、Cisco IP SoftPhone では、Cisco CallManager IP アドレスを PC 上の Cisco TSP コンフィギュレーションで明示的に指定する必要があるため、マッピングはスタティックにする必要があります。
- PAT または外部 PAT を使用して、Cisco CallManager IP アドレスを変換する場合、Cisco IP SoftPhone の登録を成功させるには、その TCP ポート 2748 を PAT（インターフェイス）アドレスの**同じポート**にスタティックにマッピングする必要があります。CTIQBE リスニング ポート（TCP 2748）は固定されており、Cisco CallManager、Cisco IP SoftPhone、または Cisco TSP 上でユーザが設定変更することはできません。

シグナリング メッセージの検査

シグナリング メッセージを検査する場合、**inspect ctiqbe** コマンドでは、多くの場合、メディア エンドポイント（たとえば、IP 電話）の場所を判別する必要があります。

この情報は、メディア トラフィックのためのアクセス制御と NAT 状態を準備して、手作業での設定なしでメディア トラフィックを透過的にファイアウォールを通過させるために使用されます。

この場所を判別する場合、**inspect ctiqbe** コマンドは、トンネル デフォルト ゲートウェイのルートを使用し**ません**。トンネル デフォルト ゲートウェイのルートは、**route** *interface* **0 0** *metric* **tunneled** という形式のルートです。このルートは、IPSec トンネルから出力されるパケットのデフォルト ルートを上書きします。そのため、VPN トラフィックに対して **inspect ctiqbe** コマンドが必要となる場合は、トンネル デフォルト ゲートウェイのルートを設定しないでください。代わりに、他のスタティック ルーティングまたはダイナミック ルーティングを使用します。

例

次の例に示すように、CTIQBE 検査エンジンをイネーブルにします。この例では、デフォルト ポート（2748）上の CTIQBE トラフィックに一致するクラスマップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map ctiqbe-port
hostname(config-cmap)# match port tcp eq 2748
hostname(config-cmap)# exit
hostname(config)# policy-map ctiqbe_policy
hostname(config-pmap)# class ctiqbe-port
hostname(config-pmap-c)# inspect ctiqbe
hostname(config-pmap-c)# exit
hostname(config)# service-policy ctiqbe_policy interface outside
```

すべてのインターフェイスに対して CTIQBE 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

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。
show conn	さまざまな接続タイプの接続状態を表示します。
show ctiqbe	セキュリティ アプライアンスを越えて確立された CTIQBE セッションに関する情報を表示します。CTIQBE 検査エンジンによって割り当てられたメディア接続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。

inspect cuseeme

CU-SeeMe アプリケーション検査をイネーブルにする場合や、セキュリティ アプライアンスがリスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect cuseeme** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシーマップ コンフィギュレーション モードからアクセスできます。この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。

inspect cuseeme

no inspect cuseeme

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
クラス 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、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

inspect cuseeme コマンドを使用すると、CU-SeeMe アプリケーションに対してアプリケーション検査を実行できます。

port オプションを使用して、デフォルトのポート割り当てを 389 から変更します。*-port* オプションを使用して、ILS 検査を一定範囲のポート番号に適用します。

CU-SeeMe クライアントを使用すると、ユーザは別のユーザ（CU-SeeMe または他の H.323 クライアント）に直接接続して、両ユーザ間でオーディオ、ビデオ、およびデータのコラボレーションを行うことができます。CU-SeeMe クライアントは、CU-SeeMe クライアントおよび他のベンダーの H.323 準拠クライアントを両方含む混合クライアント環境で会議を行うことができます。

バックグラウンドでは、CU-SeeMe クライアントは、2 つの異なるモードで動作します。別の CU-SeeMe クライアントまたは CU-SeeMe Conference Server に接続された場合、クライアントは CU-SeeMe モードで情報を送信します。

異なるベンダーの H.323 準拠ビデオ会議クライアントに接続された場合、CU-SeeMe クライアントは H.323 モードで H.323 標準の形式を使用して通信します。

CU-SeeMe は、H.323 検査でサポートされるほか、UDP ポート 7648 上で動作する CU-SeeMe 制御ストリーム上で NAT を実行します。

例

次の例に示すように、CU-SeeMe 検査エンジンをイネーブルにします。この例では、デフォルト ポート（7648）上の CU-SeeMe トラフィックに一致するクラスマップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map cuseeme-port
hostname(config-cmap)# match port tcp eq 7648
hostname(config-cmap)# exit
hostname(config)# policy-map cuseeme_policy
hostname(config-pmap)# class cuseeme-port
hostname(config-pmap-c)# inspect cuseeme
hostname(config-pmap-c)# exit
hostname(config)# service-policy cuseeme_policy interface outside
```

すべてのインターフェイスに対して CU-SeeMe 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

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。
service-policy	1 つまたは複数のインターフェイスにポリシーマップを適用します。

inspect dns

DNS 検査をイネーブルにするには（以前にディセーブルにした場合）、クラス コンフィギュレーション モードで **inspect dns** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシーマップ コンフィギュレーション モードからアクセスできます。DNS パケットの最大長を指定するには、**inspect dns** コマンドを使用します。DNS 検査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。

inspect dns [***maximum-length*** *max_pkt_length*]

no inspect dns [***maximum-length*** *max_pkt_length*]

シンタックスの説明

maximum-length	（オプション）DNS パケットの最大長を指定します。デフォルトは 512 です。**inspect dns** コマンドを入力するときに **maximum-length** オプションを指定しない場合、DNS パケット サイズはチェックされません。
max_pkt_length	DNS パケットの最大長。これより長いパケットはドロップされます。

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。

DNS パケット サイズに関する **maximum-length** のデフォルトは 512 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
クラス 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、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

DNS guard は、DNS 応答がセキュリティ アプライアンスによって転送されると、DNS クエリーに関連付けられた DNS セッションをただちに停止します。DNS guard は、また、DNS 応答の ID が DNS クエリーの ID と一致していることを確認するために、メッセージ交換を監視します。

DNS 検査がイネーブルの場合（デフォルト）、セキュリティ アプライアンスは次の追加タスクを実行します。

- **alias**、**static**、および **nat** コマンドを使用して完成したコンフィギュレーションに基づいて、DNS レコードを変換する（DNS リライト）。変換が適用されるのは、DNS 応答の A レコードのみです。そのため、PTR レコードを要求する逆ルックアップは、DNS リライトの影響を受けません。

（注） DNS リライトは PAT には適用できません。これは、A レコードごとに複数の PAT 規則が適用可能であり、使用される PAT 規則があいまいになるためです。

- DNS メッセージの最大長を適用する（デフォルトは 512 バイト、最大長は 65,535 バイト）。必要に応じて再構成が実行され、パケット長が設定した最大長を超えていないことが確認されます。最大長を超えている場合、そのパケットはドロップされます。

（注）　**inspect dns** コマンドを入力するときに **maximum-length** オプションを指定しない場合、DNS パケット サイズはチェックされません。

- ドメイン名の長さとして 255 バイトを、ラベルの長さとして 63 バイトを適用する。
- DNS メッセージに圧縮ポインタが出現する場合、ポインタによって参照されるドメイン名の完全性を確認する。
- 圧縮ポインタのループが存在するかどうかを確認する。

複数の DNS セッションが同じ 2 つのホスト間で発生し、それらのセッションの 5 つのタプル（送信元 / 宛先 IP アドレス、送信元 / 宛先ポート、およびプロトコル）が同じものである場合、それらのセッションに対しては接続が 1 つのみ作成されます。DNS の ID は *app_id* によって追跡されます。また、各 app_id のアイドル タイマーは独立して動作します。

app_id の有効期限はそれぞれ独立して満了するため、正当な DNS 応答がセキュリティ アプライアンスを通過できるのは、限られた期間内のみであり、リソースの継続使用はできません。ただし、**show conn** コマンドを入力すると、DNS 接続のアイドル タイマーが新しい DNS セッションによってリセットされることが示されます。これは共有 DNS 接続の性質によるものであり、仕様です。

DNS リライトの動作

DNS 検査がイネーブルの場合、DNS リライトは、任意のインターフェイスから発信される DNS メッセージの NAT をフル サポートします。

内部ネットワーク上のクライアントが内部アドレスの DNS 解決を外部インターフェイス上の DNS サーバに要求した場合、DNS A レコードは正しく変換されます。DNS 検査エンジンがディセーブルの場合、A レコードは変換されません。

DNS リライトは、次の 2 つの機能を実行します。

- DNS クライアントがプライベート インターフェイス上にある場合、*DNS 応答* 内のパブリック アドレス（ルーティング可能なアドレスまたは「マッピングされた」アドレス）を、プライベート アドレス（「実際の」アドレス）に変換する。
- DNS クライアントがパブリック インターフェイス上にある場合、プライベート アドレスをパブリック アドレスに変換する。

DNS 検査がイネーブルであれば、**alias**、**static**、または **nat** コマンドを使用して DNS リライトを設定できます。これらのコマンドのシンタックスや機能の詳細については、該当するコマンドのページを参照してください。

例

次の例では、DNS パケットの最大長を 1,500 バイトに変更します。DNS 検査はデフォルトではイネーブルになっていますが、DNS トラフィックを識別するトラフィック マップを作成し、ポリシーマップを該当するインターフェイスに適用する必要があります。

```
hostname(config)# class-map dns-port
hostname(config-cmap)# match port udp eq 53
hostname(config-cmap)# exit
hostname(config)# policy-map sample_policy
hostname(config-pmap)# class dns-port
hostname(config-pmap-c)# inspect dns maximum-length 1500
hostname(config-pmap-c)# exit
hostname(config)# service-policy sample_policy interface outside
```

すべてのインターフェイスに対して DNS パケットの最大長を変更するには、**interface outside** の代わりに **global** パラメータを使用します。

次の例は、DNS をディセーブルにする方法を示しています。

```
hostname(config)# policy-map sample_policy
hostname(config-pmap)# class dns-port
hostname(config-pmap-c)# no inspect dns
hostname(config-pmap-c)# exit
hostname(config)# service-policy sample_policy interface outside
```

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 dns	DNS のデバッグ情報をイネーブルにします。
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。
service-policy	1 つまたは複数のインターフェイスにポリシーマップを適用します。

inspect esmtp

SMTP アプリケーション検査をイネーブルにする場合や、セキュリティ アプライアンスがリスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect esmtp** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシーマップ コンフィギュレーション モードからアクセスできます。この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。

inspect esmtp

no inspect esmtp

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
クラス 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、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

ESMTP アプリケーション検査では、SMTP ベースの攻撃からの保護を強化するため、セキュリティ アプライアンスを通過できる SMTP コマンドのタイプを制限し、モニタリング機能を追加しています。

ESMTP は SMTP プロトコルの機能拡張であり、あらゆる点で SMTP と類似しています。便宜上、このドキュメントでは、SMTP という用語は SMTP と ESMTP の両方を指します。拡張 SMTP のアプリケーション検査プロセスは、SMTP アプリケーション検査と類似しており、SMTP セッションのサポートを備えています。拡張 SMTP セッションで使用されるコマンドのほとんどは、SMTP セッションで使用されるものと同じですが、ESMTP セッションは、動作がはるかに高速で、配信通知ステータスなど、信頼性とセキュリティに関するオプションをより多く備えています。

inspect esmtp コマンドには、**fixup smtp** コマンドで提供されていた機能が含まれています。また、一部の拡張 SMTP コマンドに対する追加サポートも含まれています。拡張 SMTP アプリケーション検査では、8 つの拡張 SMTP コマンド（AUTH、EHLO、ETRN、HELP、SAML、SEND、SOML、および VRFY）に対するサポートが追加されています。7 つの RFC 821 コマンド（DATA、HELO、MAIL、NOOP、QUIT、RCPT、および RSET）に対するサポートを合わせると、セキュリティ アプライアンスは合計 15 の SMTP コマンドをサポートしています。

他の拡張 SMTP コマンド（ATRN、STARTLS、ONEX、VERB、CHUNKING など）やプライベート拡張はサポートされていません。サポート対象外のコマンドは、内部サーバにより拒否される X に変換されます。この結果は、「500 Command unknown: 'XXX'」のようなメッセージで表示されます。不完全なコマンドは、廃棄されます。

inspect smtp コマンドを入力した場合、セキュリティ アプライアンスはコマンドを **inspect esmtp** に自動的に変換します。このコンフィギュレーションは、**show running-config** コマンドを入力すると表示されます。

inspect esmtp コマンドは、SMTP バナーの文字を、「2」、「0」、「0」の文字を除いて、アスタリスクに変更します。復帰（CR）と改行（LF）は、無視されます。

SMTP 検査がイネーブルの場合、次の規則が順守されていないときは、対話型の SMTP に使用される Telnet セッションがハングする場合があります。この規則とは、SMTP コマンドは少なくとも 4 文字の長さが必要である、SMTP コマンドは改行と復帰で終了する必要がある、次の返信を発行する前に応答を待つ必要がある、というものです。

SMTP サーバは、数値の応答コードと任意の読み取り可能な文字によって、クライアントの要求に応答します。SMTP アプリケーション検査は、ユーザが使用できるコマンドや、サーバが返すメッセージを制御および削減します。SMTP 検査は、次の 3 つの主要なタスクを実行します。

- SMTP 要求を 7 つの基本的な SMTP コマンドと 8 つの拡張コマンドに制限する。
- SMTP コマンド応答シーケンスを監視する。
- 監査証跡を生成する。メール アドレスに埋め込まれていた無効な文字が置き換えられた場合、監査レコード 108002 が生成されます。詳細については、RFC 821 を参照してください。

SMTP 検査は、コマンドと応答のシーケンスを監視して、次の異常なシグニチャを検出します。

- 不完全なコマンド。
- コマンドの不正な終了（<CR><LR> で終了していない）。
- MAIL コマンドと RCPT コマンドには、メールの送信者と受信者が指定されています。不正な文字が含まれているかどうか、メール アドレスがスキャンされます。パイプライン文字 | は削除されます（スペースに変更されます）。ただし、| はメール アドレスの定義に使用されている場合にのみ許可されます（| の前に「<」があることが条件です）。
- SMTP サーバによる予期しない移行。
- 未知のコマンドがあると、セキュリティ アプライアンスはパケット内のすべての文字を X に変更します。この場合、サーバは、クライアントに対するエラー コードを生成します。パケット内が変更されるため、TCP チェックサムの再計算または調整が必要になります。
- TCP ストリームの編集。
- コマンドのパイプライン化。

例

次の例に示すように、SMTP 検査エンジンをイネーブルにします。この例では、デフォルト ポート（25）上の SMTP トラフィックに一致するクラスマップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map smtp-port
hostname(config-cmap)# match port tcp eq 25
hostname(config-cmap)# exit
hostname(config)# policy-map smtp_policy
hostname(config-pmap)# class smtp-port
hostname(config-pmap-c)# inspect esmtp
hostname(config-pmap-c)# exit
hostname(config)# service-policy smtp_policy interface outside
```

すべてのインターフェイスに対して SMTP 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

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 smtp	SMTP のデバッグ情報をイネーブルにします。
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。
service-policy	1 つまたは複数のインターフェイスにポリシーマップを適用します。
show conn	SMTP など、さまざまな接続タイプの接続状態を表示します。

inspect ftp

FTP 検査用のポートを設定する場合や、高度な検査をイネーブルにする場合は、クラス コンフィギュレーション モードで **inspect ftp** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシーマップ コンフィギュレーション モードからアクセスできます。この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。

inspect ftp [**strict** [*map_name*]]

no inspect ftp [**strict** [*map_name*]]

シンタックスの説明

map_name	FTP マップの名前。
strict	（オプション）FTP トラフィックの高度な検査をイネーブルにし、強制的に RFC 標準に準拠させます。

注意　FTP を上位のポートに移動する場合は、注意が必要です。たとえば、FTP ポートを 2021 に設定した場合、ポート 2021 に向けて開始する接続はすべて、データ ペイロードが FTP コマンドとして解釈されます。

デフォルト

セキュリティ アプライアンスは、デフォルトでは、ポート 21 で FTP があるかどうかリスンします。

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
クラス 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、**fixup** コマンドは置き換えられて廃止されました。*map_name* オプションが追加されました。

使用上のガイドライン

FTP アプリケーション検査は、FTP セッションを検査し、次の 4 つのタスクを実行します。

- ダイナミックなセカンダリ データ接続を準備する
- ***ftp*** コマンド応答シーケンスを追跡する
- 監査証跡を生成する
- 埋め込み IP アドレスの NAT を実行する

FTP アプリケーション検査は、FTP データ転送用にセカンダリ チャネルを準備します。チャネルは、ファイルのアップロード、ファイルのダウンロード、またはディレクトリ一覧イベントの応答として割り当てられます。ただし、事前にネゴシエートされている必要があります。ポートは、PORT コマンドまたは PASV コマンドによってネゴシエートされます。

（注）　**no inspect ftp** コマンドを使用して、FTP 検査エンジンをディセーブルにすると、発信ユーザはパッシブ モードだけで接続を開始でき、着信 FTP はすべてディセーブルになります。

strict オプションの使用方法

strict オプションは、Web ブラウザが FTP 要求内の埋め込みコマンドを送信しないようにします。各 ***ftp*** コマンドは、新しいコマンドが許可される前に確認される必要があります。埋め込みコマンドを送信する接続は、ドロップされます。**strict** オプションは、FTP サーバが 227 コマンドを生成することだけを許可し、FTP クライアントが PORT コマンドを生成することだけを許可します。227 コマンドと PORT コマンドはチェックして、エラー文字列内に表示されないようにします。

注意　***strict*** オプションを使用すると、RFC 標準に準拠していない FTP クライアントが遮断されることがあります。

strict オプションがイネーブルの場合、次の異常なアクティビティについて、各 ***ftp*** コマンドと応答シーケンスが追跡されます。

- 不完全なコマンド：PORT および PASV 応答コマンド内のカンマの数が 5 つかどうかが確認されます。5 つ以外の場合、PORT コマンドは不完全であると見なされ、TCP 接続は終了します。
- 不正なコマンド：RFC に規定されているように、***ftp*** コマンドが <CR><LF> 文字で終了しているかどうかが確認されます。異なっている場合、接続は終了します。
- RETR コマンドと STOR コマンドのサイズ：固定値になっているかどうかが確認されます。サイズが固定値より大きい場合、エラー メッセージがログに記録され、接続は終了します。
- コマンド スプーフィング：PORT コマンドは常にクライアントから送信される必要があります。PORT コマンドがサーバから送信されている場合、TCP 接続は拒否されます。
- 応答スプーフィング：PASV　応答コマンド（227）は常にサーバから送信される必要があります。PASV 応答コマンドがクライアントから送信されている場合、TCP 接続は拒否されます。この拒否により、ユーザが「227 xxxxx a1, a2, a3, a4, p1, p2」を実行した場合のセキュリティ ホールが防止されます。
- TCP ストリームの編集。
- 無効なポートのネゴシエーション：ネゴシエートされたダイナミック ポートの値が 1024 未満かどうかが確認されます。1 ～ 1024 の範囲のポート番号は既知の接続用に予約されているため、ネゴシエートされたポートがこの範囲内の場合は、TCP 接続は開放されます。
- コマンドのパイプライン化：PORT および PASV 応答コマンド内のポート番号の後にある文字数が定数の 8 であるかどうかが相互確認されます。9 以上の場合、TCP 接続は終了します。
- セキュリティ アプライアンスが、SYST コマンドに対する FTP サーバの応答を一連の X に置き換え、サーバのシステム タイプが FTP クライアントに知られることを防止します。このデフォルト動作を無効にするには、FTP マップ コンフィギュレーション モードで **no mask-syst-reply** コマンドを使用します。

（注）　セキュリティ アプライアンスを通過させない特定の FTP コマンドを指定するには、FTP マップを指定し、**request-command deny** コマンドを使用します。詳細については、**ftp-map** コマンドと **request-command deny** コマンドのページを参照してください。

FTP ログ メッセージ

FTP アプリケーション検査は、次のログ メッセージを生成します。

- 取得またはアップロードされた各ファイルについて、監査レコード 302002 が生成されます。
- **ftp** コマンドが RETR または STOR であるかが確認され、取得コマンドと格納コマンドがログに記録されます。
- ユーザ名は、IP アドレスを提供するテーブルを検索することで取得されます。
- ユーザ名、送信元 IP アドレス、宛先 IP アドレス、NAT アドレス、およびファイル操作がログに記録されます。
- メモリ不足によってセカンダリ ダイナミック チャネルの準備に失敗した場合、監査レコード 201005 が生成されます。

FTP アプリケーション検査は、NAT と連携して、アプリケーション ペイロード内の IP アドレスを変換します。詳細については、RFC 959 を参照してください。

例

次の例では、FTP トラフィックを識別し、FTP マップを定義し、ポリシーを定義し、厳密な FTP 検査をイネーブルにして、そのポリシーを外部インターフェイスに適用します。

```
hostname(config)# class-map ftp-port
hostname(config-cmap)# match port tcp eq 21
hostname(config-cmap)# exit
hostname(config)# ftp-map inbound_ftp
hostname(config-inbound_ftp)# request-command deny put stou appe
hostname(config-ftp-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class ftp-port
hostname(config-pmap-c)# inspect ftp strict inbound_ftp
hostname(config-pmap-c)# exit
hostname(config-pmap)# exit
hostname(config)# service-policy inbound_policy interface outside
```

すべてのインターフェイスに対して厳密な FTP アプリケーション検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

（注） FTP 制御接続用のポートだけを指定して、データ接続用は指定しません。セキュリティ アプライアンス ステートフル検査は、必要に応じて、ダイナミックにデータ接続を用意します。

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。
mask-syst-reply	FTP サーバ応答をクライアントから見えないようにします。
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。
request-command deny	禁止する FTP コマンドを指定します。
service-policy	1 つまたは複数のインターフェイスにポリシーマップを適用します。

inspect gtp

GTP 検査をイネーブルまたはディセーブルにする場合や、GTP トラフィックまたはトンネルを制御するための GTP マップを定義する場合は、クラス コンフィギュレーション モードで **inspect gtp** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシーマップ コンフィギュレーション モードからアクセスできます。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。

inspect gtp [*map_name*]

no inspect gtp [*map_name*]

（注）　GTP 検査には、特別なライセンスが必要です。セキュリティ アプライアンス上で **inspect gtp** コマンドを入力する場合、必要なライセンスを持っていないときは、セキュリティ アプライアンス上にエラー メッセージが表示されます。

シンタックスの説明

map_name	（オプション）GTP マップの名前。

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
クラス 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

GTP は、GPRS 用のトンネリング プロトコルで、ワイヤレス ネットワーク上のセキュアなアクセスを可能にします。GPRS は、既存の GSM ネットワークを統合するために設計されたデータ ネットワーク アーキテクチャです。モバイル ユーザに対して、企業ネットワークとインターネットにアクセスするためのパケット スイッチ データ サービスを中断なく提供します。GTP の概要については、『*Cisco Security Appliance Command Line Configuration Guide*』の「Applying Application Layer Protocol Inspection」の章を参照してください。

GTP のパラメータの定義に使用する特定のマップを指定するには、**gtp-map** コマンドを使用します。このコマンドを入力すると、システムがコンフィギュレーション モードに入って、個々のマップを定義するためのさまざまなコマンドを入力できるようになります。基準を満たさないメッセージに対して指定できるアクションは、**allow**、**reset**、**drop** などのさまざまなコンフィギュレーション コマンドを使用して設定します。これらのアクションに加えて、イベントをログに記録するかどうかも指定できます。

GTP マップを定義したら、**inspect gtp** コマンドを使用してマップをイネーブルにします。**class-map**、**policy-map**、および **service-policy** の各コマンドを使用して、トラフィックのクラスを定義し、**inspect** コマンドをクラスに適用し、ポリシーを 1 つまたはそれ以上のインターフェイスに適用します。

ポート値として使用される **gtp** という文字列は、ポート値 3386 に自動的に変換されます。GTP 用の既知ポートは次のとおりです。

- 3386
- 2123

次の機能は 7.0(1) ではサポートされていません。

- NAT、PAT、外部 NAT、エイリアス、およびポリシー NAT
- 3386、2123、および 2152 以外のポート
- トンネリング IP パケットとその内容の検証

シグナリング メッセージの検査

シグナリング メッセージを検査する場合、**inspect gtp** コマンドでは、多くの場合、メディア エンドポイント（たとえば、IP 電話）の場所を判別する必要があります。

この情報は、メディア トラフィックのためのアクセス制御と NAT 状態を準備して、手作業での設定なしでメディア トラフィックを透過的にファイアウォールを通過させるために使用されます。

この場所を判別する場合、**inspect gtp** コマンドは、トンネル デフォルト ゲートウェイのルートを使用し**ません**。トンネル デフォルト ゲートウェイのルートは、**route** *interface* **0 0** *metric* **tunneled** という形式のルートです。このルートは、IPSec トンネルから出力されるパケットのデフォルト ルートを上書きします。そのため、VPN トラフィックに対して **inspect gtp** コマンドが必要となる場合は、トンネル デフォルト ゲートウェイのルートを設定しないでください。代わりに、他のスタティック ルーティングまたはダイナミック ルーティングを使用します。

例

次の例は、アクセスリストを使用して GTP トラフィックを識別し、GTP マップを定義し、ポリシーを定義して、そのポリシーを外部インターフェイスに適用する方法を示しています。

```
hostname(config)# access-list gtp-acl permit udp any any eq 3386
hostname(config)# access-list gtp-acl permit udp any any eq 2123
hostname(config)# class-map gtp-traffic
hostname(config)# match access-list gtp-acl
hostname(config)# gtp-map gtp-policy
hostname(config)# policy-map inspection_policy
hostname(config-pmap)# class gtp-traffic
hostname(config-pmap-c)# inspect gtp gtp-policy
hostname(config)# service-policy inspection_policy interface outside
```

（注） 次の例では、デフォルト値を使用して GTP 検査をイネーブルにします。デフォルト値を変更するには、**gtp-map** コマンドのページと、GTP マップ コンフィギュレーション モードから入力する各コマンドのページを参照してください。

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。
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。
service-policy	1 つまたは複数のインターフェイスにポリシーマップを適用します。

inspect h323

H.323 アプリケーション検査をイネーブルにする場合や、セキュリティ アプライアンスがリスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect h323** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシーマップ コンフィギュレーション モードからアクセスできます。この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。

inspect h323 {**h225** | **ras** }

no inspect h323 {**h225** | **ras** }

シンタックスの説明

h225	H.225 シグナリング検査をイネーブルにします。
ras	RAS 検査をイネーブルにします。

デフォルト

デフォルトのポート割り当ては次のとおりです。

- h323 h225 1720
- h323 ras 1718-1719

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
クラス 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、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

inspect h323 コマンドは、Cisco CallManager および VocalTec Gatekeeper などの H.323 に準拠したアプリケーションをサポートしています。H.323 は、International Telecommunication Union（ITU; 国際電気通信連合）が定義した LAN 上のマルチメディア会議用のプロトコル スイートです。セキュリティ アプライアンスは、One Call Signaling Channel 上の Multiple Calls の H.323 v3 機能など、Version 4 までの H.323 をサポートしています。

H.323 検査がイネーブルの場合、セキュリティ アプライアンスは、H.323 Version 3 で導入された機能である、同一のコール シグナリング チャネル上の複数のコールをサポートします。この機能を使用すると、コール セットアップ時間が短縮され、セキュリティ アプライアンス上のポートの使用も削減されます。

H.323 検査には、次の 2 つの主要な機能があります。

- H.225 および H.245 メッセージ内の必要な埋め込み IPv4 アドレスの NAT を実行する。H.323 メッセージは PER 符号化フォーマットで符号化されているため、セキュリティ アプライアンスは、ASN.1 デコーダを使用して H.323 メッセージをデコードします。
- ネゴシエートされた H.245 接続および RTP/RTCP 接続をダイナミックに割り当てる。

H.323 の動作

H.323 のプロトコル コレクションでは、集合的に、2 つまでの TCP 接続と 4 ～ 6 の UDP 接続を使用できます。FastStart は TCP 接続を 1 つだけ使用し、RAS は登録、許可、およびステータス用に 1 つの UDP 接続を使用します。

H.323 クライアントでは、最初に、TCP ポート 1720 を使用して H.323 サーバへの TCP 接続を確立し、Q.931 コールのセットアップを要求できます。コール セットアップ プロセスの一部として、H.323 端末は、H.245 TCP 接続に使用するポート番号をクライアントに提供します。H.245 接続は、コール ネゴシエーションとメディア チャネルのセットアップに使用されます。H.323 ゲートキーパーを使用している環境では、最初のパケットは UDP を使用して送信されます。

H.323 検査は、Q.931 TCP 接続を監視して、H.245 ポート番号を判別します。H.323 端末が FastStart を使用していない場合、セキュリティ アプライアンスは、H.225 メッセージの検査に基づいて、H.245 接続をダイナミックに割り当てます。

（注） H.225 接続は、RAS を使用してダイナミックに割り当てることもできます。

各 H.245 メッセージ内で、H.323 エンドポイントは、以降の UDP データ ストリームに使用するポート番号を交換します。H.323 検査は、H.245 メッセージを検査してこれらのポートを識別し、メディア交換用の接続をダイナミックに作成します。Real-Time Transport Protocol（RTP）は、ネゴシエートされたポート番号を使用しますが、RTP Control Protocol（RTCP）は、次の上位ポート番号を使用します。

H.323 コントロール チャネルは、H.225、H.245、および H.323 RAS を処理します。H.323 検査は、次のポートを使用します。

- 1718：ゲートキーパー検出に使用される UDP ポート
- 1719：RAS およびゲートキーパー検出に使用される UDP ポート
- 1720：TCP 制御ポート

ゲートキーパーからの ACF メッセージがセキュリティ アプライアンスを通過する場合は、H.225 接続用のピンホールが空けられます。H.245 シグナリング ポートは、H.225 シグナリングのエンドポイント間でネゴシエートされます。H.323 ゲートキーパーが使用される場合、セキュリティ アプライアンスは、ACF メッセージの検査に基づいて、H.225 接続を開きます。セキュリティ アプライアンスに ACF メッセージが表示されない場合は、H.225 コール シグナリング用に既知の H.323 ポート 1720 のアクセスリストを開くことが必要となる場合があります。

セキュリティ アプライアンスは、H.225 メッセージを検査した後で、H.245 チャネルをダイナミックに割り当て、同様にフィックスアップする H.245 チャネルに接続します。これは、セキュリティ アプライアンスを通過した H.245 メッセージはすべて、H.245 アプリケーション検査を通過し、埋め込み IP アドレスの NAT が実行され、ネゴシエートされたメディア チャネルが開かれることを意味します。

H.323 ITU 標準では、信頼できる接続に送信する前に、メッセージ長を定義する TPKT ヘッダーを H.225 および H.245 の前に配置することが規定されています。TPKT ヘッダーは H.225/H.245 メッセージと同じ TCP パケットで送信されない場合もあるため、メッセージを正しく処理およびデコードするには、セキュリティ アプライアンスで TPKT 長を保持しておく必要があります。セキュリティ アプライアンスは、各接続のデータ構造を保持し、このデータ構造には、次に受信されるメッセージの TPKT 長が含まれます。

セキュリティ アプライアンスで任意の IP アドレスの NAT を実行する必要がある場合は、チェックサム、UUIE（user-user information element）の長さ、および TPKT（H.225 メッセージの TCP パケットに含まれている場合）を変更する必要があります。TPKT が別の TCP パケットで送信される場合、セキュリティ アプライアンスは TPKT のプロキシ ACK を実行し、H.245 メッセージに新しい長さの新しい TPKT を付加します。

（注）　セキュリティ アプライアンスによる TPKT のプロキシ ACK では、TCP オプションはサポートされません。

H.323 検査を通過するパケットを使用する各 UDP 接続は、H.323 接続としてマークされ、**timeout** コマンドを使用して設定された H.323 タイムアウトでタイムアウトします。

制限と制約事項

次に、H.323 アプリケーション検査を使用する上での既知の問題および制限の一部を示します。

- スタティック PAT は、H.323 メッセージ内のオプション フィールドに埋め込まれた IP アドレスを正しく変換しない場合があります。この種の問題が発生した場合は、H.323 に対してスタティック PAT を使用しないでください。
- NetMeeting クライアントが、H.323 ゲートキーパーに登録されている状態で、同じく H.323 ゲートキーパーに登録されている H.323 ゲートウェイにコールを発信しようとする場合、接続は確立されますが、音声が双方向で聞こえない現象が報告されています。この問題は、セキュリティ アプライアンスとは無関係です。
- ネットワーク スタティックを設定する場合、そのネットワーク スタティックがサードパーティのネットマスクおよびアドレスと同じであるときは、すべての発信 H.323 接続が失敗します。

シグナリング メッセージの検査

シグナリング メッセージを検査する場合、**inspect h323** コマンドでは、多くの場合、メディア エンドポイント（たとえば、IP 電話）の場所を判別する必要があります。

この情報は、メディア トラフィックのためのアクセス制御と NAT 状態を準備して、手作業での設定なしでメディア トラフィックを透過的にファイアウォールを通過させるために使用されます。

この場所を判別する場合、**inspect h323** コマンドは、トンネル デフォルト ゲートウェイのルートを使用し**ません**。トンネル デフォルト ゲートウェイのルートは、**route** *interface* **0 0** *metric* **tunneled** という形式のルートです。このルートは、IPSec トンネルから出力されるパケットのデフォルト ルートを上書きします。そのため、VPN トラフィックに対して **inspect h323** コマンドが必要となる場合は、トンネル デフォルト ゲートウェイのルートを設定しないでください。代わりに、他のスタティック ルーティングまたはダイナミック ルーティングを使用します。

例

次の例に示すように、H.323 検査エンジンをイネーブルにします。この例では、デフォルト ポート（1720）上の H.323 トラフィックに一致するクラスマップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map h323-port
hostname(config-cmap)# match port tcp eq 1720
hostname(config-cmap)# exit
hostname(config)# policy-map h323_policy
hostname(config-pmap)# class h323-port
hostname(config-pmap-c)# inspect h323
hostname(config-pmap-c)# exit
hostname(config)# service-policy h323_policy interface outside
```

すべてのインターフェイスに対して H.323 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
debug h323	H.323 のデバッグ情報の表示をイネーブルにします。
show h225	セキュリティ アプライアンスを越えて確立された H.225 セッションの情報を表示します。
show h245	スロースタートを使用しているエンドポイントがセキュリティ アプライアンスを越えて確立した H.245 セッションの情報を表示します。
show h323-ras	セキュリティ アプライアンスを越えて確立された H.323 RAS セッションの情報を表示します。
timeout {**h225** | **h323**}	H.225 シグナリング接続または H.323 制御接続に許容されるアイドル時間で、経過後にその接続が終了します。

inspect http

HTTP アプリケーション検査をイネーブルにする場合や、セキュリティ アプライアンスがリスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect http コマンド**を使用します。クラス コンフィギュレーション モードには、ポリシーマップ コンフィギュレーション モードからアクセスできます。この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。

inspect http [*map_name*]

no inspect http [*map_name*]

シンタックスの説明

map_name	（オプション）HTTP マップの名前。

デフォルト

HTTP のデフォルト ポートは、80 です。

高度な HTTP 検査は、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
クラス 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、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

inspect http コマンドは、HTTP トラフィックに関連する可能性のある特定の攻撃やその他の脅威から保護します。HTTP 検査は、いくつかの機能を実行します。

- 高度な HTTP 検査
- N2H2 または Websense を使用する URL のスクリーニング
- Java と ActiveX のフィルタリング

後の 2 つの機能は、**filter** コマンドと共に設定されます。

高度な HTTP 検査は、HTTP メッセージが RFC 2616 に準拠していること、RFC で定義されている方式やサポートされている拡張方式を使用していること、および他のさまざまな基準を満たしていることを確認します。多くの場合、これらの基準と、その基準が満たされないときのシステムの応答を設定できます。基準を満たさないメッセージに対して指定できるアクションは、**allow**、**reset**、**drop** などのさまざまなコンフィギュレーション コマンドを使用して設定します。これらのアクションに加えて、イベントをログに記録するかどうかも指定できます。

HTTP メッセージに適用できる基準には、次のものがあります。

- リスト（設定可能）に挙げられているメソッドを含んでいない。
- 特定の転送符号化方式またはアプリケーション タイプ。
- HTTP トランザクションが RFC 仕様に沿っている。

- メッセージ本文のサイズが、制限値（設定可能）以下である。
- 要求と応答のメッセージ ヘッダーのサイズが、制限値（設定可能）以下である。
- URI の長さが制限値（設定可能）以下である。
- メッセージ本文の content-type が、ヘッダーと一致している。
- 応答メッセージの content-type が、要求メッセージの *accept-type* フィールドと一致している。
- メッセージの content-type が、事前定義済みの内部リストに挙げられている。
- メッセージが、RFC による HTTP 形式の基準を満たしている。
- 選択したサポート可能アプリケーションが存在している（または、存在していない）。
- 選択した符号化タイプが存在している（または、存在していない）。

（注） 基準を満たさないメッセージに対して指定できるアクションは、**allow**、**reset**、**drop** などのさまざまなコンフィギュレーション コマンドを使用して設定します。これらのアクションに加えて、イベントをログに記録するかどうかも指定できます。

高度な HTTP 検査をイネーブルにするには、**inspect http** *http-map* コマンドを使用します。このコマンドが HTTP トラフィックに適用する規則は、特定の HTTP マップで定義されます。この HTTP マップを設定するには、**http-map** コマンドと HTTP マップ コンフィギュレーション モードのコマンドを入力します。

（注） HTTP マップを使用して HTTP 検査をイネーブルにすると、デフォルトでは、アクション reset および log を使用した厳密な HTTP 検査がイネーブルになります。検査に合格しない場合に実行されるアクションは変更できますが、HTTP マップがイネーブルのままである限り、厳密な検査をディセーブルにすることはできません。

例

次の例は、HTTP トラフィックを識別し、HTTP マップを定義し、ポリシーを定義して、そのポリシーを外部インターフェイスに適用する方法を示しています。

```
hostname(config)# class-map http-port
hostname(config-cmap)# match port tcp eq 80
hostname(config-cmap)# exit
hostname(config)# http-map inbound_http
hostname(config-http-map)# content-length min 100 max 2000 action reset log
hostname(config-http-map)# content-type-verification match-req-rsp reset log
hostname(config-http-map)# max-header-length request bytes 100 action log reset
hostname(config-http-map)# max-uri-length 100 action reset log
hostname(config-http-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class http-port
hostname(config-pmap-c)# inspect http inbound_http
hostname(config-pmap-c)# exit
hostname(config-pmap)# exit
hostname(config)# service-policy inbound_policy interface outside
```

この例では、次のコンテンツを含んでいるトラフィックをセキュリティ アプライアンスが検出したときに、接続をリセットして syslog エントリを作成します。

- 100 バイト未満または 2,000 バイトを超えるメッセージ
- サポートされていないコンテンツ タイプ
- 100 バイトを超える HTTP ヘッダー
- 100 バイトを超える URI

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 appfw	HTTP アプリケーション検査に関する詳細情報を表示します。
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。
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。

inspect icmp

ICMP 検査エンジンを設定するには、クラス コンフィギュレーション モードで **inspect icmp** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシーマップ コンフィギュレーション モードからアクセスできます。

inspect icmp

no inspect icmp

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
クラス 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、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

ICMP 検査エンジンを使用すると、ICMP トラフィックを TCP および UDP トラフィックと同様に検査できます。ICMP 検査エンジンを使用しない場合は、ACL により ICMP にセキュリティ アプライアンスを通過させないことをお勧めします。ステートフル検査が実行されない場合、ICMP はネットワークの攻撃に利用されることがあります。ICMP 検査エンジンは、各要求に対する応答が 1 つだけであり、シーケンス番号が正しいことを確認します。

ICMP 検査エンジンがディセーブルの場合（デフォルト設定）、低セキュリティ インターフェイスから高セキュリティ インターフェイスへの ICMP エコー応答メッセージは拒否されます。このメッセージが ICMP エコー要求への応答である場合も同様です。

例

次の例に示すように、ICMP アプリケーション検査をイネーブルにします。この例では、ICMP プロトコル ID（IPv4 は 1、IPv6 は 58）を使用して、ICMP トラフィックに一致するクラスマップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map icmp-class
hostname(config-cmap)# match default-inspection-traffic
hostname(config-cmap)# exit
hostname(config)# policy-map icmp_policy
hostname(config-pmap)# class icmp-class
hostname(config-pmap-c)# inspect icmp
hostname(config-pmap-c)# exit
hostname(config)# service-policy icmp_policy interface outside
```

すべてのインターフェイスに対して ICMP 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

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。
icmp	セキュリティ アプライアンス インターフェイスで終端する ICMP トラフィックに対して、アクセス規則を設定します。
policy-map	セキュリティ アクションを 1 つまたはそれ以上のトラフィック クラスに関連付けるためのポリシーを定義します。
service-policy	1 つまたは複数のインターフェイスにポリシーマップを適用します。

inspect icmp error

ICMP エラー メッセージに対するアプリケーション検査をイネーブルにするには、クラス コンフィギュレーション モードで **inspect icmp error** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシーマップ コンフィギュレーション モードからアクセスできます。

inspect icmp error

no inspect icmp error

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
クラス 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、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

icmp error コマンドは、スタティック /NAT のコンフィギュレーションに基づいて、ICMP エラー メッセージを送信する中間ホップの xlate を作成する場合に使用します。セキュリティ アプライアンスは、パケットを変換後の IP アドレスで上書きします。

イネーブルの場合、ICMP エラー検査エンジンは、ICMP パケットに次の変更を加えます。

- IP ヘッダーで、NAT IP が Client IP（宛先アドレス）に変更され、IP チェックサムが変更されます。
- ICMP ヘッダーで、ICMP チェックサムが ICMP パケットの変更に応じて変更されます。
- ペイロードでは、次の変更が加えられます。
  - 元のパケットの NAT IP が Client IP に変更されます。
  - 元のパケットの NAT ポートが Client Port に変更されます。
  - 元のパケットの IP チェックサムが再計算されます。

ICMP エラー メッセージが取得されると、ICMP エラー検査がイネーブルかどうかに関係なく、ICMP ペイロードがスキャンされ、元のパケットから 5 つのタプル（src ip、dest ip、src port、dest port、および ip プロトコル）が取得されます。取得された 5 つのタプルを使用して検索が実行され、クライアントの元のアドレスが判別され、特定の 5 つのタプルに関連付けられた既存のセッションが検出されます。セッションが検出されない場合、ICMP エラー メッセージはドロップされます。

例

次の例に示すように、ICMP エラー アプリケーション検査をイネーブルにします。この例では、ICMP プロトコル ID（IPv4 は 1、IPv6 は 58）を使用して、ICMP トラフィックに一致するクラスマップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map icmp-class
hostname(config-cmap)# match default-inspection-traffic
hostname(config-cmap)# exit
hostname(config)# policy-map icmp_policy
hostname(config-pmap)# class icmp-class
hostname(config-pmap-c)# inspect icmp error
hostname(config-pmap-c)# exit
hostname(config)# service-policy icmp_policy interface outside
```

すべてのインターフェイスに対して ICMP エラー検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

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。
icmp	セキュリティ アプライアンス インターフェイスで終端する ICMP トラフィックに対して、アクセス規則を設定します。
inspect icmp	ICMP 検査エンジンをイネーブルまたはディセーブルにします。
policy-map	セキュリティ アクションを 1 つまたはそれ以上のトラフィック クラスに関連付けるためのポリシーを定義します。
service-policy	1 つまたは複数のインターフェイスにポリシーマップを適用します。

inspect ils

ILS アプリケーション検査をイネーブルにする場合や、セキュリティ アプライアンスがリスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect ils コマンド**を使用します。クラス コンフィギュレーション モードには、ポリシーマップ コンフィギュレーション モードからアクセスできます。この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。

inspect ils

no inspect ils

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
クラス 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、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

inspect ils コマンドは、LDAP を使用して ILS サーバとディレクトリ情報を交換する Microsoft NetMeeting、SiteServer、および Active Directory 製品の NAT をサポートします。

port オプションを使用して、デフォルトのポート割り当てを 389 から変更します。*-port* オプションを使用して、ILS 検査を一定範囲のポート番号に適用します。

セキュリティ アプライアンスは ILS の NAT をサポートしています。ILS は、ILS または SiteServer Directory のエンドポイントの登録および検出に使用されます。LDAP データベースには IP アドレスだけが保管されるため、PAT はサポートできません。

LDAP サーバが外部にある場合、検索応答を実行するには、NAT を使用して、外部 LDAP サーバに登録されている内部ピア間のローカル通信を可能にすることを考慮する必要があります。このような検索応答では、xlate、DNAT エントリの順に検索され、正しいアドレスが取得されます。両方の検索に失敗した場合、アドレスは変更されません。NAT 0 を使用している（NAT を使用していない）サイトや、DNAT 対話を想定していないサイトについては、パフォーマンスを向上させるために、検査エンジンをオフにすることをお勧めします。

ILS サーバがセキュリティ アプライアンス境界の内側にある場合は、追加の設定が必要になることがあります。この場合は、指定ポート（通常は TCP 389）上で LDAP サーバにアクセスする外部クライアント用のホールが必要です。

ILS トラフィックはセカンダリ UDP チャネルだけで発生するため、TCP 接続は、TCP 非アクティビティ間隔が経過すると切断されます。デフォルトでは、この間隔は 60 分です。間隔を調整するには、**timeout** コマンドを使用します。

ILS/LDAP は、クライアント / サーバ モデルに基づいて、単一 TCP 接続上のセッションを処理します。これらのセッションの一部は、クライアントのアクションに応じて作成される場合があります。

接続のネゴシエーション中に、クライアントからサーバに対して BIND PDU が送信されます。サーバから BIND RESPONSE を正常に受信すると、他の操作メッセージ（ADD、DEL、SEARCH、または MODIFY など）が交換され、ILS Directory 上で処理が実行されます。ADD REQUEST および SEARCH RESPONSE PDU には、NetMeeting セッションを確立するために H.323（SETUP および CONNECT メッセージ）によって使用される NetMeeting ピアの IP アドレスが含まれる場合があります。Microsoft NetMeeting v2.X および v3.X では、ILS がサポートされています。

ILS 検査は、次の処理を実行します。

- BER デコード機能を使用して、LDAP REQUEST/RESPONSE PDU をデコードする
- LDAP パケットを解析する
- IP アドレスを抽出する
- 必要に応じて IP アドレスを変換する
- BER 符号化機能を使用して、変換後のアドレスで PDU を符号化する
- 新しく符号化した PDU を TCP パケットにコピーする
- TCP チェックサムとシーケンス番号を差分的に調整する

ILS 検査には、次の制限があります。

- 照会の要求および応答はサポートされません。
- 複数のディレクトリのユーザは統合されません。
- 複数のディレクトリに別々の ID を持つ単一ユーザは、NAT では認識できません。

（注） H225 コール シグナリング トラフィックはセカンダリ UDP チャネルだけで発生するため、TCP 接続は、TCP **timeout** コマンドで指定された間隔が経過すると切断されます。この間隔は、デフォルトでは 60 分に設定されています。

例

次の例に示すように、ILS 検査エンジンをイネーブルにします。この例では、デフォルト ポート（389）上の ILS トラフィックに一致するクラスマップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map ils-port
hostname(config-cmap)# match port tcp eq 389
hostname(config-cmap)# exit
hostname(config)# policy-map ils_policy
hostname(config-pmap)# class ils-port
hostname(config-pmap-c)# inspect ils
hostname(config-pmap-c)# exit
hostname(config)# service-policy ils_policy interface outside
```

すべてのインターフェイスに対して ILS 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

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 ils	ILS のデバッグ情報をイネーブルにします。
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。
service-policy	1 つまたは複数のインターフェイスにポリシーマップを適用します。

inspect mgcp

MGCP アプリケーション検査をイネーブルにする場合や、セキュリティ アプライアンスがリスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect mgcp** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシーマップ コンフィギュレーション モードからアクセスできます。この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。

inspect mgcp [*map_name*]

no inspect mgcp [*map_name*]

シンタックスの説明

map_name	（オプション）MGCP マップの名前。

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
クラス 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、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

MGCP を使用する場合、通常、少なくとも 2 つの **inspect** コマンドを設定する必要があります。1 つはゲートウェイがコマンドを受信するポート用で、もう 1 つは Call Agent がコマンドを受信するポート用です。通常、Call Agent は、ゲートウェイのデフォルトの MGCP ポート 2427 にコマンドを送信し、ゲートウェイは、Call Agents のデフォルトの MGCP ポート 2727 にコマンドを送信します。

MGCP は、メディア ゲートウェイ コントローラまたはコール エージェントと呼ばれる外部のコール制御要素からメディア ゲートウェイを制御するために使用されます。メディア ゲートウェイは、一般的に、電話回線上で伝送されるオーディオ信号と、インターネットまたは他のパケット ネットワーク上で伝送されるデータ パケットとの変換を行うネットワーク要素です。MGCP で NAT および PAT を使用すると、限られた数の外部（グローバル）アドレスで、内部ネットワーク上の多数のデバイスをサポートできます。

次に、メディア ゲートウェイの例を示します。

- トランキング ゲートウェイ。これは、電話網と Voice over IP ネットワーク間のインターフェイスです。このゲートウェイは、一般的に、多数のデジタル回線を管理します。
- レジデンシャル ゲートウェイ。これは、Voice over IP ネットワークに従来のアナログ（RJ11）インターフェイスを提供します。レジデンシャル ゲートウェイの例には、ケーブル モデム / ケーブル セットトップ ボックス、xDSL デバイス、ブロードバンド ワイヤレス デバイスなどがあります。

- ビジネス ゲートウェイ。これは、Voice over IP ネットワークに従来のデジタル PBX インターフェイスまたは統合 *soft PBX* インターフェイスを提供します。

MGCP メッセージは、UDP 上で転送されます。応答は、コマンドの送信元アドレス（IP アドレスおよび UDP ポート番号）に返送されますが、コマンドの宛先と同じアドレスから返送されない場合があります。この状況が発生するのは、複数のコール エージェントがフェールオーバー コンフィギュレーションで使用され、コマンドを受信したコール エージェントからバックアップ コール エージェントに制御が渡された後で、バックアップ コール エージェントが応答を返送する場合です。

（注）　MGCP コール エージェントは、AUEP メッセージを送信して、MGCP エンドポイントが存在するかどうかを判別します。この結果、セキュリティ アプライアンスからのフローが確立され、MGCP エンドポイントがコール エージェントに登録できるようになります。

1 つ以上のコール エージェントおよびゲートウェイの IP アドレスを設定するには、MGCP マップ コンフィギュレーション モードで **call-agent** コマンドと **gateway** コマンドを使用します。コマンド キューに一度に入れることができる MGCP コマンドの最大数を指定するには、MGCP マップ コンフィギュレーション モードで **command-queue** コマンドを使用します。

シグナリング メッセージの検査

シグナリング メッセージを検査する場合、**inspect mgcp** コマンドでは、多くの場合、メディア エンドポイント（たとえば、IP 電話）の場所を判別する必要があります。

この情報は、メディア トラフィックのためのアクセス制御と NAT 状態を準備して、手作業での設定なしでメディア トラフィックを透過的にファイアウォールを通過させるために使用されます。

この場所を判別する場合、**inspect mgcp** コマンドは、トンネル デフォルト ゲートウェイのルートを使用し**ません**。トンネル デフォルト ゲートウェイのルートは、**route** *interface* **0 0** *metric* **tunneled** という形式のルートです。このルートは、IPSec トンネルから出力されるパケットのデフォルト ルートを上書きします。そのため、VPN トラフィックに対して **inspect mgcp** コマンドが必要となる場合は、トンネル デフォルト ゲートウェイのルートを設定しないでください。代わりに、他のスタティック ルーティングまたはダイナミック ルーティングを使用します。

例

次の例は、MGCP トラフィックを識別し、MGCP マップを定義し、ポリシーを定義して、そのポリシーを外部インターフェイスに適用する方法を示しています。この例では、デフォルト ポート（2427 および 2727）上の MGCP トラフィックに一致するクラスマップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# access-list mgcp_acl permit tcp any any eq 2427
hostname(config)# access-list mgcp_acl permit tcp any any eq 2727
hostname(config)# class-map mgcp_port
hostname(config-cmap)# match access-list mgcp_acl
hostname(config-cmap)# exit
hostname(config)# mgcp-map inbound_mgcp
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
hostname(config-mgcp-map)# command-queue 150
hostname(config-mgcp-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class mgcp_port
hostname(config-pmap-c)# inspect mgcp mgcp-map inbound_mgcp
hostname(config-pmap-c)# exit
hostname(config)# service-policy inbound_policy interface outside
```

このコンフィギュレーションにより、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なり、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なります。キューに入れることができる MGCP コマンドの最大数は、150 です。

```
To enable MGCP inspection for all interfaces, use the global parameter in place of
interface outside.
```

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 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 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。

inspect netbios

NetBIOS アプリケーション検査をイネーブルにする場合や、セキュリティ アプライアンスがリスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect netbios コマンド**を使用します。クラス コンフィギュレーション モードには、ポリシーマップ コンフィギュレーション モードからアクセスできます。この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。

inspect netbios

no inspect netbios

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。

シンタックスの説明

port	アプリケーション検査をイネーブルにするポート。ポート番号またはサポートされているポート リテラルが使用できます。有効なポートのリテラル名の一覧については、『*Cisco Security Appliance Command Line Configuration Guide*』の付録 D「Addresses, Protocols, and Ports」を参照してください。
port-port	ポートの範囲を指定します。

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。

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
クラス 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、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

inspect netbios コマンドは、NetBIOS プロトコルの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ます。

例

次の例に示すように、NetBIOS 検査エンジンをイネーブルにします。この例では、デフォルト ポート（139）上の NetBIOS トラフィックに一致するクラスマップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map netbios-port
hostname(config-cmap)# match port tcp eq 139
hostname(config-cmap)# exit
hostname(config)# policy-map netbios_policy
hostname(config-pmap)# class netbios-port
hostname(config-pmap-c)# inspect netbios 139
hostname(config-pmap-c)# exit
hostname(config)# service-policy netbios_policy interface outside
```

すべてのインターフェイスに対して NetBIOS 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

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。
service-policy	1 つまたは複数のインターフェイスにポリシーマップを適用します。

inspect pptp

PPTP アプリケーション検査をイネーブルにする場合や、セキュリティ アプライアンスがリスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect pptp** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシーマップ コンフィギュレーション モードからアクセスできます。この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。

```
inspect pptp

no inspect pptp
```

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
クラス 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、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン　Point-to-Point Tunneling Protocol（PPTP）は、PPP トラフィックをトンネリングするためのプロトコルです。PPTP セッションを構成するのは、1 つの TCP チャネルと、通常 2 つの PPTP GRE トンネルです。TCP チャネルは、PPTP GRE トンネルをネゴシエートおよび管理するためのコントロール チャネルです。GRE トンネルは、2 つのホスト間で PPP セッションを伝送します。

イネーブルの場合、PPTP アプリケーション検査は、PPTP プロトコル パケットを検査し、PPTP トラフィックを許可するのに必要な GRE 接続と xlate をダイナミックに作成します。RFC 2637 に定義されている Version 1 だけがサポートされます。

PAT は、PPTP TCP コントロール チャネルを越えてネゴシエートされる場合、GRE **[**RFC 2637**]** の修正版に対してだけ実行されます。PAT は、修正前のバージョンの GRE **[**RFC 1701、RFC 1702**]** に対しては実行されません。

特に、セキュリティ アプライアンスは、PPTP バージョンのアナウンスメントと発信コールの要求 / 応答シーケンスを検査します。RFC 2637 に定義されている PPTP Version 1 だけが検査されます。どちらかの側でアナウンスされたバージョンが Version 1 でなければ、TCP コントロール チャネルはそれ以上検査されません。さらに、発信コール要求と応答シーケンスが追跡されます。接続と xlate は、必要に応じてダイナミックに割り当てられて、それ以後のセカンダリ GRE データ トラフィックを送ることが可能になります。

PPTP 検査エンジンは、PPTP トラフィックを PAT で変換するためにイネーブルにする必要があります。さらに、PAT は、GRE（RFC2637）の修正版に対してだけで実行されます。これは、PPTP TCP コントロール チャネルを越えてネゴシエートされる場合だけです。PAT は、修正前のバージョンの GRE（RFC 1701 と RFC 1702）に対しては実行されません。

RFC 2637 で規定されているように、PPTP プロトコルは、主に、モデム バンク PAC（PPTP Access Concentrator）から開始された PPP セッションをヘッドエンド PNS（PPTP Network Server）へトンネリングするために使用されます。この使用方法では、PAC はリモート クライアントとなり、PNS はサーバとなります。

ただし、Windows によって VPN 用に使用される場合、対話関係は逆になります。PNS は、ヘッドエンド PAC への接続を開始して中央ネットワークにアクセスするリモート シングルユーザ PC です。

例

次の例に示すように、PPTP 検査エンジンをイネーブルにします。この例では、デフォルト ポート（1723）上の PPTP トラフィックに一致するクラスマップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map pptp-port
hostname(config-cmap)# match port tcp eq 1723
hostname(config-cmap)# exit
hostname(config)# policy-map pptp_policy
hostname(config-pmap)# class pptp-port
hostname(config-pmap-c)# inspect pptp
hostname(config-pmap-c)# exit
hostname(config)# service-policy pptp_policy interface outside
```

すべてのインターフェイスに対して PPTP 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

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 pptp	PPTP のデバッグ情報をイネーブルにします。
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。
service-policy	1 つまたは複数のインターフェイスにポリシーマップを適用します。

inspect rsh

RSH アプリケーション検査をイネーブルにする場合や、セキュリティ アプライアンスがリスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect rsh** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシーマップ コンフィギュレーション モードからアクセスできます。この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。

inspect rsh

no inspect rsh

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
クラス 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、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

RSH プロトコルは、TCP ポート 514 上で、RSH クライアントから RSH サーバへの TCP 接続を使用します。クライアントとサーバは、クライアントが STDERR 出力ストリームをリスンする TCP ポート番号をネゴシエートします。RSH 検査は、必要に応じて、ネゴシエートされたポート番号の NAT をサポートします。

例

次の例に示すように、RSH 検査エンジンをイネーブルにします。この例では、デフォルト ポート（514）上の RSH トラフィックに一致するクラスマップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map rsh-port
hostname(config-cmap)# match port tcp eq 514
hostname(config-cmap)# exit
hostname(config)# policy-map rsh_policy
hostname(config-pmap)# class rsh-port
hostname(config-pmap-c)# inspect rsh
hostname(config-pmap-c)# exit
hostname(config)# service-policy rsh_policy interface outside
```

すべてのインターフェイスに対して RSH 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

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。
service-policy	1 つまたは複数のインターフェイスにポリシーマップを適用します。

inspect rtsp

RTSP アプリケーション検査をイネーブルにする場合や、セキュリティ アプライアンスがリスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect rtsp** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシーマップ コンフィギュレーション モードからアクセスできます。この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。

inspect rtsp

no inspect rtsp

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
クラス 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、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン　**inspect rtsp** コマンドを使用すると、セキュリティ アプライアンスが RTSP パケットを通過させることができます。RTSP は、RealAudio、RealNetworks、Apple QuickTime 4、RealPlayer、および Cisco IP/TV 接続が使用します。

（注）　Cisco IP/TV の場合は、RTSP TCP ポート 554 と TCP 8554 を使用します。

RTSP アプリケーションは、コントロール チャネルとして、既知ポート 554 と TCP（まれに UDP）を使用します。セキュリティ アプライアンスは、RFC 2326 に準拠して、TCP だけをサポートしています。この TCP コントロール チャネルは、クライアント上で設定された転送モードに応じて、オーディオ/ビデオ トラフィックの伝送に使用するデータ チャネルをネゴシエートするために使用されます。

サポートされる RDT 転送は、rtp/avp、rtp/avp/udp、x-real-rdt、x-real-rdt/udp、および x-pn-tng/udp です。

セキュリティ アプライアンスは、Setup 応答メッセージをステータス コード 200 によって解析します。応答メッセージが着信の場合、サーバはセキュリティ アプライアンスの外側にあるため、サーバからの着信接続用にダイナミック チャネルを開く必要があります。応答メッセージが発信の場合、セキュリティ アプライアンスでダイナミック チャネルを開く必要はありません。

RFC 2326 では、SETUP 応答メッセージにクライアントとサーバのポートを含めることを規定していないため、セキュリティ アプライアンスで状態を保持し、SETUP メッセージ内のクライアント ポートを記憶しておく必要があります。QuickTime では、SETUP メッセージにクライアント ポートが設定され、サーバはサーバ ポートでのみ応答します。

RealPlayer の使用方法

RealPlayer を使用している場合、転送モードを正しく設定することが重要です。セキュリティ アプライアンスでは、**access-list** コマンド文は、サーバからクライアントへと、またはその逆で追加されます。RealPlayer の場合、**Options** > **Preferences** > **Transport** > **RTSP Settings** をクリックすることで、転送モードを変更します。

RealPlayer 上で TCP モードを使用している場合、**Use TCP to Connect to Server** チェックボックスと **Attempt to use TCP for all content** チェックボックスをオンにします。セキュリティ アプライアンス上では、検査エンジンを設定する必要はありません。

RealPlayer 上で UDP モードを使用している場合、**Use TCP to Connect to Server** チェックボックスと **Attempt to use UDP for all content** チェックボックスをオンにします。Multicast 経由で入手できないライブ コンテンツに対しても同様です。セキュリティ アプライアンス上で、**inspect rtsp** *port* コマンド文を追加します。

制約事項と制限

inspect rtsp コマンドには、次の制約事項が適用されます。

- セキュリティ アプライアンスは、UDP を介したマルチキャスト RTSP または RTSP メッセージをサポートしていません。
- **inspect rtsp** コマンドは、PAT をサポートしていません。
- セキュリティ アプライアンスには、RTSP メッセージが HTTP メッセージ内に隠されている HTTP クローキングを認識する機能はありません。
- セキュリティ アプライアンスは、RTSP メッセージについて NAT は実行できません。その理由は、埋め込み IP アドレスが HTTP または RTSP メッセージの一部として、SDP ファイルに含まれているからです。パケットはフラグメント化される可能性があり、セキュリティ アプライアンスは、フラグメント化されたパケットについて NAT は実行できません。
- Cisco IP/TV では、メッセージの SDP 部分についてセキュリティ アプライアンスが実行する NAT の数は、Content Manager にあるプログラム リストの数に比例します（各プログラム リストには、少なくとも 6 個の埋め込み IP アドレスを含めることができます）。
- Apple QuickTime 4 または RealPlayer 用の NAT を設定できます。Viewer と Content Manager が外部ネットワークに、サーバが内部ネットワークにある場合、Cisco IP/TV は、NAT が使用できる場合に限り動作します。
- HTTP を介して配信されるメディア ストリームは、RTSP アプリケーション検査ではサポートされません。これは、RTSP 検査が HTTP クローキング（HTTP でラップされた RTSP）をサポートしていないためです。

例

次の例に示すように、RTSP 検査エンジンをイネーブルにします。この例では、デフォルト ポート（554 および 8554）上の RTSP トラフィックに一致するクラスマップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# access-list rtsp-acl permit tcp any any eq 554
hostname(config)# access-list rtsp-acl permit tcp any any eq 8554
hostname(config)# class-map rtsp-traffic
hostname(config-cmap)# match access-list rtsp-acl
hostname(config-cmap)# exit
hostname(config)# policy-map rtsp_policy
hostname(config-pmap)# class rtsp-port
hostname(config-pmap-c)# inspect rtsp
hostname(config-pmap-c)# exit
hostname(config)# service-policy rtsp_policy interface outside
```

すべてのインターフェイスに対して RTSP 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

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 rtsp	RTSP のデバッグ情報をイネーブルにします。
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。
service-policy	1 つまたは複数のインターフェイスにポリシーマップを適用します。

inspect sip

SIP アプリケーション検査をイネーブルにする場合や、セキュリティ アプライアンスがリスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect sip** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシーマップ コンフィギュレーション モードからアクセスできます。この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。

inspect sip

no inspect sip

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、デフォルトではディセーブルになっています。

SIP に対するデフォルトのポート割り当ては 5060 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
クラス 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、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

SIP は、IETF で定義されているように、VoIP コールをイネーブルにします。SIP は SDP と連携して、コール シグナリングを処理します。SDP は、メディア ストリームの詳細を指定します。SIP を使用すると、セキュリティ アプライアンスは、あらゆる SIP Voice over IP（VoIP）ゲートウェイおよび VoIP プロキシ サーバをサポートできます。SIP と SDP は、次の RFC に定義されています。

- SIP：Session Initiation Protocol、RFC 2543
- SDP：Session Description Protocol、RFC 2327

セキュリティ アプライアンス経由の SIP コールをサポートするには、メディア接続アドレスのシグナリング メッセージ、メディア ポート、およびメディアの初期接続を検査する必要があります。これは、シグナリングが既知の宛先ポート（UDP/TCP 5060）上で送信される間に、メディア ストリームがダイナミックに割り当てられるためです。また、SIP は、IP パケットのユーザデータ部分に IP アドレスを埋め込みます。SIP 検査は、これらの埋め込み IP アドレスに NAT を適用します。

（注）　リモート エンドポイントから、セキュリティ アプライアンスによって保護されたネットワーク上の SIP プロキシに登録する場合、ごく特殊な条件に合致すると登録が失敗します。この条件とは、PAT がリモート エンドポイントに対して設定されている場合、SIP レジストラ サーバが外部ネットワーク上にある場合、およびエンドポイントからプロキシ サーバに送信される REGISTER メッセージの contact フィールドにポートが指定されていない場合です。

インスタント メッセージ

インスタント メッセージとは、ほぼリアルタイムで行われるユーザ間のメッセージ転送を指します。MESSAGE/INFO 方式と 202 Accept 応答は、次の RFC で定義されている IM をサポートするために使用されます。

- Session Initiation Protocol (SIP)-Specific Event Notification、RFC 3265
- Session Initiation Protocol (SIP) Extension for Instant Messaging、RFC 3428

MESSAGE/INFO 要求は、登録 / 加入が完了するといつでも受信できます。たとえば、2 つのユーザはいつでもオンラインにできますが、何時間もチャットすることはできません。そのため、SIP 検査エンジンは、設定された SIP タイムアウト値に従ってタイムアウトするピンホールを空けます。この値には、加入期間より 5 分以上長い値を設定する必要があります。加入期間は、Contact Expires 値で定義されます。通常は、30 分にします。

MESSAGE/INFO 要求は、通常、ダイナミックに割り当てられたポート（ポート 5060 を除く）を使用して送信されるため、SIP 検査エンジンを通過する必要があります。

（注）　現在サポートされているのは、チャット機能のみです。ホワイトボード、ファイル転送、およびアプリケーション共有はサポートされていません。RTC Client 5.0 はサポートされていません。

技術的詳細

SIP 検査は、SIP のテキストベースのメッセージについて NAT を実行し、メッセージの SDP 部分に関するコンテンツの長さを再計算し、パケット長とチェックサムを再計算します。また、エンドポイントがリスンするアドレス / ポートとして SIP メッセージの SDP 部分で指定されたポートに対して、メディア接続をダイナミックに開きます。

SIP 検査には、コールや送信元 / 宛先を識別する SIP ペイロードからの CALL_ID/FROM/TO インデックスに関するデータベースがあります。このデータベースには、SDP メディア情報フィールドに含まれていたメディア アドレスとメディア ポート、およびメディア タイプが保管されます。1 つのセッションに対して複数のメディア アドレスとポートを指定できます。RTP/RTCP 接続は、これらのメディア アドレス / ポートを使用して 2 つのエンドポイント間で開かれます。

初回のコール セットアップ（INVITE）メッセージには、既知ポート 5060 を使用する必要があります。ただし、以降のメッセージには、このポート番号を使用しなくてもかまいません。SIP 検査エンジンは、シグナリング接続のピンホールを空け、これらの接続を SIP 接続としてマークします。これは、メッセージを SIP アプリケーションに到達させ、メッセージに NAT を適用するためです。

コールがセットアップされると、SIP セッションは「一時的な」状態にあると見なされます。この状態は、宛先エンドポイントがリスンしている RTP メディア アドレスおよびポートを示す Response メッセージが受信されるまで維持されます。1 分以内に応答メッセージが受信されなかった場合、シグナリング接続は切断されます。

最後のハンドシェイクが完了すると、コールの状態がアクティブに移行し、BYE メッセージを受信するまでシグナリング接続が維持されます。

内部エンドポイントから外部エンドポイントにコールを開始する場合は、内部エンドポイントからの INVITE メッセージに指定される内部エンドポイントのメディア アドレスおよびメディア ポートに RTP/RTCP UDP パケットが転送されるように、外部インターフェイスに対してメディア ホールが空けられます。内部インターフェイスへの非送信請求 RTP/RTCP UDP パケットは、セキュリティ アプライアンス コンフィギュレーションで特別に許可されている場合を除き、セキュリティ アプライアンスを通過しません。

メディア接続は、接続がアイドル状態になってから 2 分以内に切断されます。ただし、このタイムアウトは設定変更できるため、期間を増減して設定できます。

シグナリング メッセージの検査

シグナリング メッセージを検査する場合、**inspect sip** コマンドでは、多くの場合、メディア エンドポイント（たとえば、IP 電話）の場所を判別する必要があります。

この情報は、メディア トラフィックのためのアクセス制御と NAT 状態を準備して、手作業での設定なしでメディア トラフィックを透過的にファイアウォールを通過させるために使用されます。

この場所を判別する場合、**inspect sip** コマンドは、トンネル デフォルト ゲートウェイのルートを使用し**ません**。トンネル デフォルト ゲートウェイのルートは、**route** *interface* **0 0** *metric* **tunneled** という形式のルートです。このルートは、IPSec トンネルから出力されるパケットのデフォルト ルートを上書きします。そのため、VPN トラフィックに対して **inspect sip** コマンドが必要となる場合は、トンネル デフォルト ゲートウェイのルートを設定しないでください。代わりに、他のスタティック ルーティングまたはダイナミック ルーティングを使用します。

例

次の例に示すように、SIP 検査エンジンをイネーブルにします。この例では、デフォルト ポート（5060）上の SIP トラフィックに一致するクラスマップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map sip-port
hostname(config-cmap)# match port tcp eq 5060
hostname(config-cmap)# exit
hostname(config)# policy-map sip_policy
hostname(config-pmap)# class sip-port
hostname(config-pmap-c)# inspect sip
hostname(config-pmap-c)# exit
hostname(config)# service-policy sip_policy interface outside
```

すべてのインターフェイスに対して SIP 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

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。
show sip	セキュリティ アプライアンスを介して確立された SIP セッションに関する情報を表示します。
debug sip	SIP のデバッグ情報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。
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。

inspect skinny

SCCP（Skinny）アプリケーション検査をイネーブルにする場合や、セキュリティ アプライアンスがリスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect skinny** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシーマップ コンフィギュレーション モードからアクセスできます。この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。

inspect skinny

no inspect skinny

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
クラス 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、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

Skinny（または Simple）Client Control Protocol（SCCP）は、VoIP ネットワークで使用される簡易プロトコルです。SCCP を使用する Cisco IP Phone は、H.323 環境で共存できます。Cisco CallManager を併用することで、SCCP クライアントは、H.323 準拠端末と相互運用できます。セキュリティ アプライアンスのアプリケーション レイヤ機能は、SCCP Version 3.3 を認識します。アプリケーション レイヤ ソフトウェアの機能により、SCCP シグナリング パケットの NAT を実行して、すべての SCCP シグナリングおよびメディア パケットがセキュリティ アプライアンスを通過できることが保証されます。

SCCP プロトコルのバージョンには、2.4、3.0.4、3.1.1、3.2、および 3.3.2 の 5 つがあります。セキュリティ アプライアンスは、Version 3.3.2 までのバージョンをすべてサポートします。また、SCCP の PAT および NAT を両方サポートします。IP Phone で使用するグローバル IP アドレスの数を制限している場合は、PAT が必要です。

Cisco CallManager と Cisco IP Phone 間の通常のトラフィックは、SCCP を使用します。また、特に設定しない限り、SCCP 検査によって処理されます。セキュリティ アプライアンスは、また、DHCP オプション 150 および 66 をサポートしているため、TFTP サーバの場所を Cisco IP Phone や他の DHCP クライアントに送信できます。詳細については、**dhcp-server** コマンドを参照してください。

Cisco IP Phone のサポート

Cisco CallManager が Cisco IP Phone よりもセキュリティの高いインターフェイス上にあるトポロジにおいて、Cisco CallManager IP アドレスの NAT が必要になる場合、Cisco IP Phone では Cisco CallManager IP アドレスをそのコンフィギュレーションで明示的に指定する必要があるため、マッピングは**スタティック**にする必要があります。ID スタティック エントリを使用した場合、高セキュリティ インターフェイス上の Cisco CallManager は Cisco IP Phone からの登録を受け入れることができます。

Cisco IP Phone は、TFTP サーバにアクセスして、Cisco CallManager サーバへの接続時に必要となるコンフィギュレーション情報ダウンロードする必要があります。

Cisco IP Phone が TFTP サーバよりもセキュリティの低いインターフェイス上にある場合は、アクセスリストを使用して、UDP ポート 69 上で保護された TFTP サーバに接続する必要があります。TFTP サーバにはスタティック エントリが必要ですが、「ID」スタティック エントリにする必要はありません。NAT を使用する場合、ID スタティック エントリは同じ IP アドレスにマッピングされます。PAT を使用する場合は、同じ IP アドレスおよびポートにマッピングされます。

Cisco IP Phone が TFTP サーバおよび Cisco CallManager よりもセキュリティの高いインターフェイス上にある場合、Cisco IP Phone で接続を開始できるようにするためのアクセスリストまたはスタティック エントリは必要ありません。

制約事項と制限

次に、SCCP に対する現行バージョンの PAT および NAT サポートに適用される制限を示します。

- PAT は、**alias** コマンドを使用すると、コンフィギュレーションとは連携動作しません。
- 外部 NAT または PAT はサポートされ**ません**。

（注） 現在、SCCP コールのステートフル フェールオーバーは、コール セットアップ中のコールを除いて、サポートされています。

内部の Cisco CallManager のアドレスが NAT または PAT 用に別の IP アドレスかポートを設定している場合、セキュリティ アプライアンスは、現在のところ TFTP を経由して転送するファイルの内容に対して NAT または PAT をサポートしていないため、外部の Cisco IP Phone 用の登録は失敗します。セキュリティ アプライアンスは、TFTP メッセージの NAT をサポートしており、TFTP ファイル用のピンホールを空けて、セキュリティ アプライアンスを通過させますが、電話機の登録中に TFTP を使用して転送される Cisco IP Phone のコンフィギュレーション ファイルに埋め込まれている Cisco CallManager IP アドレスとポートは変換できません。

シグナリング メッセージの検査

シグナリング メッセージを検査する場合、**inspect skinny** コマンドでは、多くの場合、メディア エンドポイント（たとえば、IP 電話）の場所を判別する必要があります。

この情報は、メディア トラフィックのためのアクセス制御と NAT 状態を準備して、手作業での設定なしでメディア トラフィックを透過的にファイアウォールを通過させるために使用されます。

この場所を判別する場合、**inspect skinny** コマンドは、トンネル デフォルト ゲートウェイのルートを使用し**ません**。トンネル デフォルト ゲートウェイのルートは、**route** *interface* **0 0** *metric* **tunneled** という形式のルートです。このルートは、IPSec トンネルから出力されるパケットのデフォルト ルートを上書きします。そのため、VPN トラフィックに対して **inspect skinny** コマンドが必要となる場合は、トンネル デフォルト ゲートウェイのルートを設定しないでください。代わりに、他のスタティック ルーティングまたはダイナミック ルーティングを使用します。

例

次の例に示すように、SCCP 検査エンジンをイネーブルにします。この例では、デフォルト ポート（2000）上の SCCP トラフィックに一致するクラスマップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map skinny-port
hostname(config-cmap)# match port tcp eq 2000
hostname(config-cmap)# exit
hostname(config)# policy-map skinny_policy
hostname(config-pmap)# class skinny-port
hostname(config-pmap-c)# inspect skinny
hostname(config-pmap-c)# exit
hostname(config)# service-policy skinny_policy interface outside
```

すべてのインターフェイスに対して SCCP 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

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 skinny	SCCP のデバッグ情報をイネーブルにします。
show skinny	セキュリティ アプライアンスを介して確立された SCCP セッションに関する情報を表示します。
show conn	さまざまな接続タイプの接続状態を表示します。
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。

inspect snmp

SNMP アプリケーション検査をイネーブルにする場合や、セキュリティ アプライアンスがリスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect snmp** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシーマップ コンフィギュレーション モードからアクセスできます。この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。

inspect snmp *map_name*

no inspect snmp *map_name*

シンタックスの説明

map_name	SNMP マップの名前。

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
クラス 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

inspect snmp コマンドは、SNMP マップに関する設定値を使用して SNMP 検査をイネーブルにするために使用します。SNMP マップを作成するには、**snmp-map** コマンドを使用します。SNMP トラフィックを特定のバージョンの SNMP に制限するには、SNMP マップ コンフィギュレーション モードで **deny version** コマンドを使用します。

以前のバージョンの SNMP はセキュリティ レベルが低いため、セキュリティ ポリシーで SNMP トラフィックを Version 2 に制限することが必要となる場合があります。特定のバージョンの SNMP を拒否するには、SNMP マップ内で **deny version** コマンドを使用します。SNMP マップを作成するには、**snmp-map** コマンドを使用します。SNMP マップを設定したら、**inspect snmp** コマンドを使用してマップをイネーブルにします。次に、**service-policy** コマンドを使用して、1 つまたは複数のインターフェイスにマップを適用します。

例

次の例では、SNMP トラフィックを識別し、SNMP マップを定義し、ポリシーを定義し、SNMP 検査をイネーブルにして、そのポリシーを外部インターフェイスに適用します。

```
hostname(config)# access-list snmp-acl permit tcp any any eq 161
hostname(config)# access-list snmp-acl permit tcp any any eq 162
hostname(config)# class-map snmp-port
hostname(config-cmap)# match access-list snmp-acl
hostname(config-cmap)# exit
hostname(config)# snmp-map inbound_snmp
hostname(config-snmp-map)# deny version 1
hostname(config-snmp-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class snmp-port
hostname(config-pmap-c)# inspect snmp inbound_snmp
hostname(config-pmap-c)# exit
```

すべてのインターフェイスに対して厳密な SNMP アプリケーション検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

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。
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。
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。
service-policy	1 つまたは複数のインターフェイスにポリシーマップを適用します。

inspect sqlnet

Oracle SQL*Net アプリケーション検査をイネーブルにするには、クラス コンフィギュレーション モードで **inspect sqlnet** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシーマップ コンフィギュレーション モードからアクセスできます。この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。

inspect sqlnet

no inspect sqlnet

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。

デフォルトのポート割り当ては 1521 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
クラス 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、既存の **fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

SQL*Net プロトコルは種々のパケット タイプで構成されています。セキュリティ アプライアンスは、セキュリティ アプライアンスの両側でデータ ストリームが Oracle アプリケーションと一致して見えるように、これらのパケット タイプを処理します。

SQL*Net のデフォルトのポート割り当ては 1521 です。この値は、Oracle for SQL*Net で使用されるものですが、Structured Query Language（SQL; 構造化照会言語）の IANA ポート割り当てとは一致しません。**class-map** コマンドを使用して、ポート番号の範囲に SQL*Net 検査を適用します。

セキュリティ アプライアンスは、すべてのアドレスの NAT を実行し、パケット内の埋め込みポートをすべて検索して、SQL*Net Version 1 用に開きます。

SQL*Net Version 2 では、データ長が 0 の REDIRECT パケットの直後に続くすべての DATA または REDIRECT パケットがフィックスアップされます。

フィックスアップを必要とするパケットには、埋め込みホスト / ポート アドレスが次の形式で含まれています。

```
(ADDRESS=(PROTOCOL=tcp)(DEV=6)(HOST=a.b.c.d)(PORT=a))
```

SQL*Net Version 2 TNSFrame タイプ（Connect、Accept、Refuse、Resend、および Marker）では、NAT 対象のアドレスを検出するためのスキャンは実行されません。また、検査によってパケット内の埋め込みポートに対してダイナミック接続が開かれることもありません。

SQL*Net Version 2 TNSFrames、Redirect、および Data パケットの直前に、ペイロードのデータ長が 0 である REDIRECT TNSFrame タイプがある場合は、開くポートおよび NAT 対象のアドレスを検出するためにスキャンが実行されます。データ長が 0 の Redirect メッセージがセキュリティ アプライアンスを通過すると、次に到着する Data または Redirect メッセージが NAT 対象で、ポートがダイナミックに開かれることを示すために、接続データ構造にフラグが設定されます。前述の TNS フレームのいずれかが Redirect メッセージの後に到着した場合、フラグはリセットされます。

SQL*Net 検査エンジンは、新しいメッセージと古いメッセージの長さのデータを使用して、チェックサムを再計算し、IP/TCP の長さを変更し、シーケンス番号と確認応答番号を再調整します。

その他すべてのケースでは、SQL*Net Version 1 の使用が前提となっています。TNSFrame タイプ（Connect、Accept、Refuse、Resend、Marker、Redirect、および Data）とすべてのパケットがスキャンされ、ポートとアドレスが検出されます。アドレスに NAT が適用され、ポート接続が開かれます。

例

次の例に示すように、SQL*Net 検査エンジンをイネーブルにします。この例では、デフォルト ポート（1521）上の SQL*Net トラフィックに一致するクラスマップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map sqlnet-port
hostname(config-cmap)# match port tcp eq 1521
hostname(config-cmap)# exit
hostname(config)# policy-map sqlnet_policy
hostname(config-pmap)# class sqlnet-port
hostname(config-pmap-c)# inspect sqlnet
hostname(config-pmap-c)# exit
hostname(config)# service-policy sqlnet_policy interface outside
```

すべてのインターフェイスに対して SQL*Net 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

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 sqlnet	SQL*Net のデバッグ情報をイネーブルにします。
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。
service-policy	1 つまたは複数のインターフェイスにポリシーマップを適用します。
show conn	SQL*Net など、さまざまな接続タイプの接続状態を表示します。

inspect sunrpc

Sun RPC アプリケーション検査をイネーブルにする場合や、セキュリティ アプライアンスがリスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect sunrpc** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシーマップ コンフィギュレーション モードからアクセスできます。この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。

inspect sunrpc

no inspect sunrpc

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
クラス 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、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

Sun RPC アプリケーション検査をイネーブルにする場合や、セキュリティ アプライアンスがリスンするポートを変更する場合は、ポリシーマップ クラス コンフィギュレーション モードで **inspect sunrpc** コマンドを使用します。ポリシーマップ クラス コンフィギュレーション モードには、ポリシーマップ コンフィギュレーション モードで **class** コマンドを使用することでアクセスできます。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。

inspect sunrpc コマンドは、Sun RPC プロトコルの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ます。Sun RPC は、NFS および NIS で使用されます。Sun RPC サービスは、システム上のどのポートでも動作可能です。クライアントからサーバ上の Sun RPC サービスにアクセスする場合は、サービスが動作しているポートを検出する必要があります。検出するには、既知ポート 111 上のポートマッパー プロセスにクエリーします。

クライアントは、サービスの Sun RPC プログラム番号を送信して、ポート番号を取得します。この時点で、クライアント プログラムはその新しいポートに Sun RPC クエリーを送信します。サーバから応答が送信されると、セキュリティ アプライアンスはこのパケットを代行受信し、そのポート上で TCP および UDP の両方の初期接続を開きます。

（注） Sun RPC ペイロード情報の NAT または PAT はサポートされません。

例

次の例に示すように、RPC 検査エンジンをイネーブルにします。この例では、デフォルト ポート（111）上の RPC トラフィックに一致するクラスマップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map sunrpc-port
hostname(config-cmap)# match port tcp eq 111
hostname(config-cmap)# exit
hostname(config)# policy-map sample_policy
hostname(config-pmap)# class sunrpc-port
hostname(config-pmap-c)# inspect sunrpc
hostname(config-pmap-c)# exit
hostname(config)# service-policy sample_policy interface outside
```

すべてのインターフェイスに対して RPC 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
clear configure sunrpc_server	**sunrpc-server** コマンドを使用して実行されたコンフィギュレーションを削除します。
clear sunrpc-server active	NFS や NIS など、特定のサービスの Sun RPC アプリケーション検査で空けられたピンホールをクリアします。
show running-config sunrpc-server	Sun RPC サービス テーブル コンフィギュレーションに関する情報を表示します。
sunrpc-server	NFS や NIS などの Sun RPC サービスに対して、タイムアウトを指定してピンホールを作成できるようにします。
show sunrpc-server active	Sun RPC サービスに対して空けられたピンホールを表示します。

inspect tftp

TFTP アプリケーション検査をディセーブルにする場合や、ディセーブルの状態からイネーブルにする場合は、クラス コンフィギュレーション モードで **inspect tftp** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシーマップ コンフィギュレーション モードからアクセスできます。この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。

inspect tftp

no inspect tftp

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。

デフォルトのポート割り当ては 69 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
クラス 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、既存の **fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

RFC 1350 で規定されている Trivial File Transfer Protocol（TFTP）は、TFTP サーバとクライアント間でファイルの読み書きを行うための簡易プロトコルです。

セキュリティ アプライアンスは、TFTP トラフィックを検査し、必要に応じて接続と変換をダイナミックに作成して、TFTP クライアントとサーバ間のファイル転送を許可します。特に、検査エンジンは、TFTP 読み取り要求（RRQ）、書き込み要求（WRQ）およびエラー通知（ERROR）を検査します。

有効な読み取り（RRQ）要求または書き込み（WRQ）要求が受信されると、必要に応じて、ダイナミック セカンダリ チャネルと PAT 変換が割り当てられます。このセカンダリ チャネルは、後で TFTP によってファイル転送またはエラー通知に使用されます。

セカンダリ チャネル上でトラフィックを開始できるのは、TFTP サーバのみです。また、TFTP クライアントとサーバ間に存在できる不完全なセカンダリ チャネルは最大で 1 つです。サーバからエラー通知が送信されると、セカンダリ チャネルは閉じられます。

TFTP トラフィックのリダイレクトにスタティック PAT が使用される場合は、TFTP 検査をイネーブルにする必要があります。

例

次の例に示すように、TFTP 検査エンジンをイネーブルにします。この例では、デフォルト ポート（69）上の TFTP トラフィックに一致するクラスマップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map tftp-port
hostname(config-cmap)# match port udp eq 69
hostname(config-cmap)# exit
hostname(config)# policy-map tftp_policy
hostname(config-pmap)# class tftp-port
hostname(config-pmap-c)# inspect tftp
hostname(config-pmap-c)# exit
hostname(config)# service-policy tftp_policy interface outside
```

すべてのインターフェイスに対して TFTP 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

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。
service-policy	1 つまたは複数のインターフェイスにポリシーマップを適用します。

inspect xdmcp

XDMCP アプリケーション検査をイネーブルにする場合や、セキュリティ アプライアンスがリスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect xdmcp コマンド**を使用します。クラス コンフィギュレーション モードには、ポリシーマップ コンフィギュレーション モードからアクセスできます。この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。

inspect xdmcp

no inspect xdmcp

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
クラス 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、既存の **fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

inspect xdmcp コマンドは、XDMCP プロトコルの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ます。

XDMCP は、UDP ポート 177 を使用して X セッションをネゴシエートするプロトコルです。X セッションは、確立後は TCP を使用します。

ネゴシエーションを成功させ、XWindows セッションを正常に起動するには、セキュリティ アプライアンスは、Xhosted コンピュータからの TCP バック接続を許可する必要があります。バック接続を許可するには、セキュリティ アプライアンス上で **established** コマンドを使用します。XDMCP がディスプレイ送信用ポートをネゴシエートすると、**established** コマンドが参照され、このバック接続を許可する必要があるかどうかが確認されます。

XWindows セッション中は、管理者は既知ポート 6000 | n 上で Xserver ディスプレイと通信します。次の端末設定を行うと、各ディスプレイが Xserver に個別に接続されます。

```
setenv DISPLAY Xserver:n
```

n は、ディスプレイの番号です。

XDMCP を使用すると、ディスプレイが IP アドレスを使用してネゴシエートされます。この IP アドレスは、セキュリティ アプライアンスが必要に応じて NAT を実行できるものです。XDCMP 検査は、PAT をサポートしていません。

例

次の例に示すように、XDMCP 検査エンジンをイネーブルにします。この例では、デフォルト ポート（177）上の XDMCP トラフィックに一致するクラスマップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map xdmcp-port
hostname(config-cmap)# match port tcp eq 177
hostname(config-cmap)# exit
hostname(config)# policy-map xdmcp_policy
hostname(config-pmap)# class xdmcp-port
hostname(config-pmap-c)# inspect xdmcp
hostname(config-pmap-c)# exit
hostname(config)# service-policy xdmcp_policy interface outside
```

すべてのインターフェイスに対して XDMCP 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

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 xdmcp	XDMCP のデバッグ情報をイネーブルにします。
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。
service-policy	1 つまたは複数のインターフェイスにポリシーマップを適用します。

intercept-dhcp

DHCP 代行受信をイネーブルにするには、グループポリシー コンフィギュレーション モードで **intercept-dhcp enable** コマンドを使用します。DHCP 代行受信をディセーブルにするには、**intercept-dhcp disable** コマンドを使用します。

intercept-dhcp アトリビュートを実行コンフィギュレーションから削除するには、**no intercept-dhcp** コマンドを使用します。このコマンドを使用すると、ユーザは、デフォルト グループポリシーまたは他のグループポリシーから DHCP 代行受信コンフィギュレーションを継承できます。

DHCP 代行受信を使用すると、Microsoft XP クライアントは、セキュリティ アプライアンスに対してスプリット トンネリングを使用できます。セキュリティ アプライアンスは、Microsoft Windows XP クライアントの DHCP Inform メッセージに直接応答し、そのクライアントにトンネル IP アドレスのサブネット マスク、ドメイン名、およびクラスレス スタティック ルートを提供します。XP 以前の Windows クライアントに対しては、DHCP 代行受信は、ドメイン名とサブネット マスクを提供します。この機能は、DHCP サーバを使用することに利点がない環境に有用です。

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

no intercept-dhcp

シンタックスの説明

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

デフォルト

DHCP 代行受信はディセーブルになっています。

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
グループポリシー 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

スプリット トンネル オプションが 225 バイトを超えていると、Microsoft XP に異常が発生し、ドメイン名が破損します。この問題を回避するには、セキュリティ アプライアンスで送信ルートの数を 27 ～ 40 ルートに制限します。ルートの数は、ルートのクラスによって異なります。

例

次の例は、FirstGroup というグループポリシーに DHCP 代行受信を設定する方法を示しています。

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

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 モードに入るには、グローバル コンフィギュレーション モードで **interface** コマンドを使用します。論理サブインターフェイスを作成するには、*subinterface* 引数を使用します。サブインターフェイスを削除するには、このコマンドの **no** 形式を使用します。物理インターフェイスは削除できません。インターフェイス コンフィギュレーション モードでは、ハードウェア設定値を設定し、名前、VLAN、および IP アドレスを割り当て、それ以外の多数の設定値を設定することができます。

interface {*physical_interface*[**.***subinterface*] | *mapped_name*}

no interface *physical_interface***.***subinterface*

シンタックスの説明

mapped_name	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、その名前を入力します。
physical_interface	物理インターフェイスのタイプ、スロット、およびポート番号で、*type*[*slot*/]*port* として指定します。タイプとスロット / ポートの間にスペースを入れるかどうかは任意です。 物理インターフェイスのタイプには、次のものがあります。 • **ethernet** • **gigabitethernet** PIX 500 シリーズ セキュリティ アプライアンスの場合は、タイプに続けてポート番号を入力します（たとえば、**ethernet0**）。 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は、タイプに続けてスロット / ポートを入力します（たとえば、**gigabitethernet0/1**）。シャーシに組み込まれたインターフェイスはスロット 0 に割り当てられ、4GE SSM 上のインターフェイスはスロット 1 に割り当てられます。 ASA 5500 シリーズ適応型セキュリティ アプライアンスには、次のタイプもあります。 • **management** 管理インターフェイスは、管理トラフィック専用に設計されたファースト イーサネット インターフェイスで、**management0/0** として指定されます。ただし、必要に応じて、通過トラフィックに使用することもできます（**management-only** コマンドを参照）。透過ファイアウォール モードでは、通過トラフィック用の 2 つのインターフェイスのほかに、管理インターフェイスを使用できます。また、管理インターフェイスにサブインターフェイスを追加して、マルチ コンテキスト モードのセキュリティ コンテキストごとに管理することができます。 インターフェイス タイプ、スロット、およびポート番号を特定するには、使用中のモデルに付属しているハードウェア ドキュメント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。サブインターフェイスの最大数は、セキュリティ アプライアンスのモデルによって異なります。プラットフォームごとのサブインターフェイスの最大数については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

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、すべての物理インターフェイスに対して **interface** コマンドを自動的に生成します。

マルチ コンテキスト モードでは、セキュリティ アプライアンスは、**allocate-interface** コマンドを使用してコンテキストに割り当てられたインターフェイスすべてに対して、**interface** コマンドを自動的に生成します。

物理インターフェイスは、デフォルトではすべてシャットダウンされます。コンフィギュレーションでは、コンテキスト内の割り当て済みインターフェイスはシャットダウンされません。

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(1)	このコマンドは、新しいサブインターフェイスの命名規則が適用できるように、また、インターフェイス コンフィギュレーション モードで引数が独立したコマンドとなるように変更されました。

使用上のガイドライン

デフォルトでは、物理インターフェイスはすべてシャットダウンされます。イネーブルになっているサブインターフェイスをトラフィックが通過できるようにするには、物理インターフェイスを事前にイネーブルにしておく必要があります。マルチ コンテキスト モードの場合、物理インターフェイスまたはサブインターフェイスをコンテキストに割り当てると、インターフェイスはデフォルトではそのコンテキスト内でイネーブルになります。ただし、トラフィックがコンテキスト インターフェイスを通過するためには、そのインターフェイスをシステム コンフィギュレーションでもイネーブルにする必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、そのインターフェイスを共有しているすべてのコンテキストでダウンします。

イネーブルになっているインターフェイスをトラフィックが通過できるようにするには、インターフェイス コンフィギュレーション モードのコマンドである **nameif** および（ルーテッド モード用の）**ip address** を設定します。サブインターフェイスの場合は、**vlan** コマンドを設定します。セキュリティ レベルは、デフォルトでは 0（最低レベル）になっています。インターフェイスのデフォルト レベルについて調べる場合や、インターフェイスの相互通信を可能にするためにデフォルトの 0 から変更する場合は、**security-level** コマンドを参照してください。

ASA 適応型セキュリティ アプライアンスには、Management 0/0 と呼ばれる専用の管理インターフェイスが含まれており、このインターフェイスによってセキュリティ アプライアンスへのトラフィックをサポートします。ただし、**management-only** コマンドを使用することで、任意のインターフェイスを管理専用インターフェイスとして設定できます。また、Management 0/0 の管理専用モードをディセーブルにして、他のインターフェイスと同様にトラフィックを通過させることもできます。

（注）　透過ファイアウォール モードでは、2 つのインターフェイスのみがトラフィックを通過させることができます。ただし、ASA 適応型セキュリティ アプライアンスでは、専用の管理インターフェイス（物理インターフェイスまたはサブインターフェイス）を管理トラフィック用の第 3 のインターフェイスとして使用できます。モードはこの場合設定不能であり、常に管理専用にする必要があります。

インターフェイス設定を変更する場合、既存の接続がタイムアウトするのを待たずに新しいセキュリティ情報を使用するときは、**clear local-host** コマンドを使用して接続を消去してもかまいません。

interface コマンドの **no** 形式を使用して物理インターフェイスを削除することも、コンテキスト内の割り当て済みインターフェイスを削除することもできません。

マルチ コンテキスト モードでは、物理パラメータ、サブインターフェイス、および VLAN 割り当ては、システム コンフィギュレーションのみに設定します。それ以外のパラメータは、コンテキスト コンフィギュレーションのみに設定します。

例

次の例では、シングルモードで、物理インターフェイスのパラメータを設定します。

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

次の例では、シングルモードで、サブインターフェイスのパラメータを設定します。

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

次の例では、マルチ コンテキスト モードで、システム コンフィギュレーションのインターフェイス パラメータを設定し、gigabitethernet 0/1.1 サブインターフェイスを contextA に割り当てます。

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

次の例では、マルチ コンテキスト モードで、コンテキスト コンフィギュレーションのパラメータを設定します。

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

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。
clear interface	**show interface** コマンドのカウンタを消去します。
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。

interface (vpn load-balancing)

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

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

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

シンタックスの説明

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

デフォルト

interface コマンドを省略した場合、デフォルトでは、***lbprivate*** インターフェイスは***内部***に、***lbpublic*** インターフェイスは***外部***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
vpn load-balancing	•	—	•	—	—

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。

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

このコマンドの no 形式を使用すると、インターフェイスがデフォルトに戻ります。

例

次に、**vpn load-balancing** コマンド シーケンスの例を示します。このコマンド シーケンスには、クラスタのパブリック インターフェイスを「test」として指定する **interface** コマンドと、クラスタのプライベート インターフェイスをデフォルト（内部）に戻す interface コマンドが含まれています。

```
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)# no interface lbprivate
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
vpn load-balancing	VPN ロードバランシング モードに入ります。

interface-policy

監視中にインターフェイスの障害が検出された場合のフェールオーバーのポリシーを指定するには、フェールオーバー グループ コンフィギュレーション モードで **interface-policy** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

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

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

シンタックスの説明

num	1 ～ 100 の数を指定するか（パーセンテージとして使用する場合）、または 1 からインターフェイスの最大数までの数を指定します。
%	（オプション）*num* の数が監視対象インターフェイスのパーセンテージであることを指定します。

デフォルト

装置に対して **failover interface-policy** コマンドが設定されている場合は、その値が **interface-policy** フェールオーバー グループ コマンドのデフォルトと見なされます。設定されていなければ、*num* は 1 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
フェールオーバー グループ 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

num 引数とオプションの **%** キーワードの間にスペースを含めないでください。

障害が発生したインターフェイスの数が設定済みポリシーの基準を満たした場合、他のセキュリティ アプライアンスが正常に機能しているときは、セキュリティ アプライアンスは自身を障害としてマークし、場合によってはフェールオーバーが発生します（アクティブなセキュリティ アプライアンスに障害が発生した場合）。ポリシーでカウントされるのは、**monitor-interface** コマンドで監視対象として指定したインターフェイスのみです。

例

次の例（抜粋）は、フェールオーバー グループに対して適用可能なコンフィギュレーションを示しています。

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

関連コマンド

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

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には、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 **ip-address** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip-address *ip-address*

no ip-address

シンタックスの説明

ip-address	セキュリティ アプライアンスの IP アドレスを指定します。

デフォルト

デフォルト設定では、IP アドレスは含まれません。

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
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、central トラストポイントの暗号 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、central トラストポイントの登録要求にセキュリティ アプライアンスの IP アドレスを含めます。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# ip-address 209.165.200.225
```

関連コマンド

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

ip address

インターフェイスの IP アドレス（ルーテッド モード）または管理アドレスの IP アドレス（透過モード）を設定するには、**ip address** コマンドを使用します。ルーテッド モードの場合は、インターフェイス コンフィギュレーション モードでこのコマンドを入力します。透過モードの場合は、グローバル コンフィギュレーション モードでこのコマンドを入力します。IP アドレスを削除するには、このコマンドの **no** 形式を使用します。このコマンドは、また、フェールオーバー用のスタンバイ アドレスを設定します。

ip address *ip_address* [*mask*] [***standby*** *ip_address*]

no ip address [*ip_address*]

シンタックスの説明

ip_address	インターフェイスの IP アドレス（ルーテッド モード）、または管理 IP アドレス（透過モード）。
mask	（オプション）IP アドレスのサブネット マスク。マスクを設定しない場合、セキュリティ アプライアンスは IP アドレス クラスのデフォルト マスクを使用します。
standby *ip_address*	（オプション）フェールオーバー用のスタンバイ装置の 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
インターフェイス コンフィギュレーション	•	—	•	•	—
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)	ルーテッド モードに関して、このコマンドが、グローバル コンフィギュレーション コマンドからインターフェイス コンフィギュレーション モードのコマンドに変更されました。

使用上のガイドライン

シングル コンテキスト ルーテッド ファイアウォール モードでは、各インターフェイス アドレスは一意のサブネット上にある必要があります。マルチ コンテキスト モードでは、このインターフェイスが共有インターフェイス上にある場合、各 IP アドレスは一意で、同じサブネット上にある必要があります。インターフェイスが一意の場合、この IP アドレスは、必要に応じて他のコンテキストで使用することができます。

透過ファイアウォールは、IP ルーティングには参加しません。セキュリティ アプライアンスに必要な唯一の IP コンフィギュレーションは、管理 IP アドレスを設定することです。このアドレスが必要な理由は、セキュリティ アプライアンスが セキュリティ アプライアンス上で発信するトラフィック（システム メッセージや AAA サーバとの通信など）の送信元アドレスとして、このアドレスを使用するためです。また、このアドレスは、リモート管理アクセスに使用することもできます。このアドレスは、アップストリーム ルータおよびダウンストリーム ルータと同じサブネット上にある必要があります。マルチ コンテキスト モードの場合は、各コンテキスト内で管理 IP アドレスを設定します。

スタンバイ IP アドレスは、メイン IP アドレスと同じサブネット上にある必要があります。

例

次の例では、2 つのインターフェイスの IP アドレスとスタンバイ アドレスを設定します。

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

次の例では、透過ファイアウォールの管理アドレスとスタンバイ アドレスを設定します。

```
hostname(config)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
ip address dhcp	DHCP サーバから IP アドレスを取得するようにインターフェイスを設定します。
show ip address	インターフェイスに割り当てられた IP アドレスを表示します。

ip address dhcp

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

ip address dhcp [*setroute*]

no ip address dhcp

シンタックスの説明

setroute	（オプション）DHCP サーバから提供されるデフォルト ルートをセキュリティ アプライアンスが使用できるようにします。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
インターフェイス 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、グローバル コンフィギュレーション コマンドからインターフェイス コンフィギュレーション モードのコマンドに変更されました。また、このコマンドが、外部インターフェイスだけでなく、すべてのインターフェイス上でイネーブルにできるようになりました。

使用上のガイドライン

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

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

setroute オプションをイネーブルにする場合は、**route** コマンドを使用してデフォルト ルートを設定しないでください。

no shutdown コマンドを使用してインターフェイスをイネーブルにしないで **ip address dhcp** コマンドを入力すると、一部の DHCP 要求が送信されない場合があります。

例

次の例では、gigabitethernet0/1 インターフェイス上で DHCP をイネーブルにします。

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

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
ip address	インターフェイスの IP アドレスを設定します。または、透過ファイアウォールの管理 IP アドレスを設定します。
show ip address dhcp	DHCP サーバから取得した IP アドレスを表示します。

ip audit attack

攻撃シグニチャに一致するパケットに対するデフォルト アクションを設定するには、グローバル コンフィギュレーション モードで **ip audit attack** コマンドを使用します。デフォルト アクションに戻す（接続をリセットする）には、このコマンドの **no** 形式を使用します。アクションは複数指定することも、一切指定しないこともできます。

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

no ip audit attack

シンタックスの説明

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

デフォルト

デフォルト アクションは、アラームの送信です。

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

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

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

例

次の例では、攻撃シグニチャに一致するパケットに対するデフォルト アクションを、alarm および reset に設定します。内部インターフェイスの監査ポリシーは、このデフォルトを無効にして alarm のみに設定します。一方、外部インターフェイスのポリシーは、**ip audit attack** コマンドで設定されたデフォルト設定を使用します。

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

関連コマンド

コマンド	説明
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 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 signature	シグニチャをディセーブルにします。
show running-config ip audit attack	**ip audit attack** コマンドのコンフィギュレーションを表示します。

ip audit info

情報シグニチャに一致するパケットに対するデフォルト アクションを設定するには、グローバル コンフィギュレーション モードで **ip audit info** コマンドを使用します。デフォルト アクションに戻す（アラームを生成する）には、このコマンドの **no** 形式を使用します。アクションは複数指定することも、一切指定しないこともできます。

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

no ip audit info

シンタックスの説明

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

デフォルト

デフォルト アクションは、アラームの生成です。

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

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

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

例

次の例では、情報シグニチャに一致するパケットに対するデフォルト アクションを、alarm および reset に設定します。内部インターフェイスの監査ポリシーは、このデフォルトを無効にして alarm および drop に設定します。一方、外部インターフェイスのポリシーは、**ip audit info** コマンドで設定されたデフォルト設定を使用します。

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

関連コマンド

コマンド	説明
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 attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit interface	インターフェイスに監査ポリシーを割り当てます。
ip audit signature	シグニチャをディセーブルにします。
show running-config ip audit info	**ip audit info** コマンドのコンフィギュレーションを表示します。

ip audit interface

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

ip audit interface *interface_name policy_name*

no ip audit interface *interface_name policy_name*

シンタックスの説明

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

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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、監査ポリシーを内部インターフェイスと外部インターフェイスに適用します。

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

関連コマンド

コマンド	説明
ip audit attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit info	情報シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
ip audit signature	シグニチャをディセーブルにします。
show running-config ip audit interface	**ip audit interface** コマンドのコンフィギュレーションを表示します。

ip audit name

パケットが定義済みの攻撃シグニチャまたは情報シグニチャに一致する場合に実行するアクションを識別する、名前付き監査ポリシーを作成するには、グローバル コンフィギュレーション モードで **ip audit name** コマンドを使用します。シグニチャは、既知の攻撃パターンに一致するアクティビティです。たとえば、DoS 攻撃に一致するシグニチャがあります。ポリシーを削除するには、このコマンドの **no** 形式を使用します。

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

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

シンタックスの説明

action	（オプション）一連のアクションを定義することを指定します。このキーワードの後に何もアクションを指定しない場合、セキュリティ アプライアンスはアクションを実行しません。***action*** キーワードを入力しない場合、セキュリティ アプライアンスは、**ip audit attack** コマンドと **ip audit info** コマンドで設定されたデフォルト アクションを使用します。
alarm	（オプション）パケットがシグニチャに一致したことを示すシステム メッセージを生成します。
attack	攻撃シグニチャの監査ポリシーを作成します。パケットは、DoS 攻撃や不正な FTP コマンドなど、ネットワークに対する攻撃の一部である可能性があります。
drop	（オプション）パケットをドロップします。
info	情報シグニチャの監査ポリシーを作成します。パケットは、現在のところ、ネットワークを攻撃することはありませんが、ポート スィープなど、情報収集アクティビティの一部である可能性があります。
name	ポリシーの名前を設定します。
reset	（オプション）パケットをドロップし、接続を閉じます。

デフォルト

ip audit attack コマンドと **ip audit info** コマンドを使用してデフォルト アクションを変更していなければ、攻撃シグニチャと情報シグニチャに対するデフォルト アクションは、アラームの生成になっています。

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
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

ポリシーを適用するには、**ip audit interface** コマンドを使用してインターフェイスにポリシーを割り当てます。各インターフェイスに ***info*** ポリシーと ***attack*** ポリシーを割り当てることができます。

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

トラフィックがシグニチャに一致する場合、そのトラフィックに対してアクションを実行するときは、**shun** コマンドを使用して、攻撃ホストからの新しい接続を防止し、既存の接続からのパケットを拒否します。

例

次の例では、攻撃シグニチャと情報シグニチャに対してアラームを生成するように、内部インターフェイスの監査ポリシーを設定します。一方、外部インターフェイスのポリシーでは、攻撃の接続をリセットします。

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

関連コマンド

コマンド	説明
ip audit attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit info	情報シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit interface	インターフェイスに監査ポリシーを割り当てます。
ip audit signature	シグニチャをディセーブルにします。
shun	特定の送信元アドレスと宛先アドレスが指定されたパケットをブロックします。

ip audit signature

監査ポリシーのシグニチャをディセーブルにするには、グローバル コンフィギュレーション モードで **ip audit signature** コマンドを使用します。シグニチャを再度イネーブルにするには、このコマンドの **no** 形式を使用します。正当なトラフィックがシグニチャに継続的に一致する場合、シグニチャをディセーブルにするリスクがあっても多数のアラームを回避することを考えているときは、ディセーブルにしてもかまいません。

ip audit signature *signature_number* ***disable***

no ip audit signature *signature_number*

シンタックスの説明

signature_number	ディセーブルにするシグニチャの番号を指定します。サポートされているシグニチャのリストについては、表 5-4 を参照してください。
disable	シグニチャをディセーブルにします。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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

表 5-4 に、サポートされているシグニチャとシステム メッセージ番号を示します。

表 5-4　シグニチャ ID とシステム メッセージ番号

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
1000	400000	IP オプション：不良オプション リスト	情報	受信した IP データグラムの IP データグラム ヘッダーにある IP オプションのリストが不完全な場合や変造されている場合にトリガーされます。IP オプションのリストには、種々のネットワーク管理タスクやデバッグ タスクを実行するオプションが 1 つ以上含まれています。
1001	400001	IP オプション：記録パケット ルート	情報	受信した IP データグラムの IP オプション リストにオプション 7（記録パケット ルート）が含まれている場合にトリガーされます。
1002	400002	IP オプション:タイムスタンプ	情報	受信した IP データグラムの IP オプション リストにオプション 4（タイムスタンプ）が含まれている場合にトリガーされます。

表 5-4　シグニチャ ID とシステム メッセージ番号（続き）

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
1003	400003	IP オプション：セキュリティ	情報	受信した IP データグラムの IP オプション リストにオプション 2（セキュリティ オプション）が含まれている場合にトリガーされます。
1004	400004	IP オプション：発信元ルートの損失	情報	受信した IP データグラムの IP オプション リストにオプション 3（発信元ルートの損失）が含まれている場合にトリガーされます。
1005	400005	IP オプション：SATNET ID	情報	受信した IP データグラムの IP オプション リストにオプション 8（SATNET ストリーム ID）が含まれている場合にトリガーされます。
1006	400006	IP オプション:完全発信元ルート	情報	受信した IP データグラムの IP オプション リストにオプション 2（完全発信ルーティング）が含まれている場合にトリガーされます。
1100	400007	IP フラグメント攻撃	攻撃	受信した IP データグラムのオフセット フィールドに含まれているオフセット値が 0 より大きく 5 より小さい場合にトリガーされます。
1102	400008	IP 不可能パケット	攻撃	到着した IP パケットの送信元アドレスと宛先アドレスが一致している場合にトリガーされます。このシグニチャは、いわゆる Land 攻撃を捕捉します。
1103	400009	IP フラグメント重複（Teardrop）	攻撃	同じ IP データグラムに含まれている 2 つのフラグメントが、データグラム内で両フラグメントが位置決めを共有していることを示すオフセットを持っている場合にトリガーされます。これは、フラグメント A がフラグメント B によって完全に上書きされること、またはフラグメント A がフラグメント B によって部分的に上書きされることを意味する場合があります。一部のオペレーティング システムは、このように重複するフラグメントを正しく処理しないため、重複フラグメントを受信したときに、例外を投げたり、不適切に動作したりする場合があります。このようにして、Teardrop 攻撃から DoS が引き起こされます。
2000	400010	ICMP エコー応答	情報	受信した IP データグラムの IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 0（エコー応答）に設定されている場合にトリガーされます。
2001	400011	ICMP ホスト到達不能	情報	受信した IP データグラムの IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 3（ホスト到達不能）に設定されている場合にトリガーされます。
2002	400012	ICMP Source Quench	情報	受信した IP データグラムの IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 4（Source Quench）に設定されている場合にトリガーされます。

表 5-4　シグニチャ ID とシステム メッセージ番号（続き）

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
2003	400013	ICMP リダイレクト	情報	受信した IP データグラムの IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 5（リダイレクト）に設定されている場合にトリガーされます。
2004	400014	ICMP エコー要求	情報	受信した IP データグラムの IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 8（エコー要求）に設定されている場合にトリガーされます。
2005	400015	データグラムの ICMP タイム超過	情報	受信した IP データグラムの IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 11（データグラムのタイム超過）に設定されている場合にトリガーされます。
2006	400016	データグラム上の ICMP パラメータ問題	情報	受信した IP データグラムの IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 12（データグラム上のパラメータ問題）に設定されている場合にトリガーされます。
2007	400017	ICMP タイムスタンプ要求	情報	受信した IP データグラムの IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 13（タイムスタンプ要求）に設定されている場合にトリガーされます。
2008	400018	ICMP タイムスタンプ応答	情報	受信した IP データグラムの IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 14（タイムスタンプ応答）に設定されている場合にトリガーされます。
2009	400019	ICMP 情報要求	情報	受信した IP データグラムの IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 15（情報要求）に設定されている場合にトリガーされます。
2010	400020	ICMP 情報応答	情報	受信した IP データグラムの IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 16（ICMP 情報応答）に設定されている場合にトリガーされます。
2011	400021	ICMP アドレス マスク要求	情報	受信した IP データグラムの IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 17（アドレス マスク要求）に設定されている場合にトリガーされます。
2012	400022	ICMP アドレス マスク応答	情報	受信した IP データグラムの IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 18（アドレス マスク応答）に設定されている場合にトリガーされます。

表 5-4　シグニチャ ID とシステム メッセージ番号（続き）

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
2150	400023	フラグメント化された ICMP トラフィック	攻撃	受信した IP データグラムの IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定されているほか、それ以外にも 1（ICMP）に設定されたフラグメント フラグがあるか、またはオフセット フィールドにオフセットが含まれている場合にトリガーされます。
2151	400024	大きい ICMP トラフィック	攻撃	受信した IP データグラムの IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、IP の長さが 1024 より大きい場合にトリガーされます。
2154	400025	Ping of Death 攻撃	攻撃	受信した IP データグラムの IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、Last Fragment ビットが設定され、（IP オフセット * 8）+（IP データ長）> 65,535 の式が成り立つ場合にトリガーされます。この式は、IP オフセット（元のパケットにおけるこのフラグメントの開始位置で、8 バイト単位）と残りのパケットの合計が IP パケットの最大サイズを超えていることを意味します。
3040	400026	TCP NULL フラグ	攻撃	SYN、FIN、ACK、または RST フラグがいずれも設定されていない単一の TCP パケットが、特定のホストに送信された場合にトリガーされます。
3041	400027	TCP SYN+FIN フラグ	攻撃	SYN および FIN フラグが設定されている単一の TCP パケットが、特定のホストに送信された場合にトリガーされます。
3042	400028	TCP FIN のみのフラグ	攻撃	単一の身元不明 TCP FIN パケットが、特定のホスト上の特権ポート（ポート番号は 1024 より小さい）に送信された場合にトリガーされます。
3153	400029	FTP に誤ったアドレスを指定	情報	ポート コマンドが、要求元ホストとは異なるアドレスを使用して発行された場合にトリガーされます。
3154	400030	FTP に誤ったポートを指定	情報	ポート コマンドが、1024 未満または 65535 を超えるデータ ポートを指定して発行された場合にトリガーされます。
4050	400031	UDP Bomb 攻撃	攻撃	指定された UDP の長さが、指定された IP の長さより小さい場合にトリガーされます。この変造パケット タイプは、DoS 攻撃に関連付けられています。
4051	400032	UDP Snork 攻撃	攻撃	検出された UDP パケットの送信元ポートが 135、7、または 19 のいずれかで、宛先ポートが 135 の場合にトリガーされます。
4052	400033	UDP Chargen DoS 攻撃	攻撃	このシグニチャがトリガーされるのは、検出された UDP パケットの送信元ポートが 7 で、宛先ポートが 19 の場合です。
6050	400034	DNS HINFO 要求	情報	DNS サーバの HINFO レコードにアクセスする攻撃が発生した場合にトリガーされます。
6051	400035	DNS ゾーン転送	情報	通常の DNS ゾーン転送（送信元ポートは 53）が発生した場合にトリガーされます。

表 5-4　シグニチャ ID とシステム メッセージ番号（続き）

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
6052	400036	ハイポートからの DNS ゾーン転送	情報	不正な DNS ゾーン転送（送信元ポートは 53 以外）が発生した場合にトリガーされます。
6053	400037	すべての記録の DNS 要求	攻撃	すべての記録の DNS 要求を受信した場合にトリガーされます。
6100	400038	RPC ポート登録	情報	ターゲット ホストに対して新しい RPC サービスを登録する攻撃が発生した場合にトリガーされます。
6101	400039	RPC ポート非登録	情報	ターゲット ホストに対して既存の RPC サービスを登録解除する攻撃が発生した場合にトリガーされます。
6102	400040	RPC Dump	情報	ターゲット ホストに RPC ダンプ要求が発行された場合にトリガーされます。
6103	400041	プロキシの RPC 要求	攻撃	ターゲット ホストのポートマッパーにプロキシの RPC 要求が送信された場合にトリガーされます。
6150	400042	ypserv（YP サーバ デーモン）Portmap 要求	情報	YP サーバ デーモン（ypserv）ポートのポートマッパーに要求が送信された場合にトリガーされます。
6151	400043	ypbind（YP バインド デーモン）Portmap 要求	情報	YP バインド デーモン（ypbind）ポートのポートマッパーに要求が送信された場合にトリガーされます。
6152	400044	yppasswdd（YP パスワード デーモン）Portmap 要求	情報	YP パスワード デーモン（yppasswdd）ポートのポートマッパーに要求が送信された場合にトリガーされます。
6153	400045	ypupdated（YP アップデート デーモン）Portmap 要求	攻撃	YP アップデート デーモン（ypupdated）ポートのポートマッパーに要求が送信された場合にトリガーされます。
6154	400046	ypxfrd（YP 転送デーモン）Portmap 要求	攻撃	YP 転送デーモン（ypxfrd）ポートのポートマッパーに要求が送信された場合にトリガーされます。
6155	400047	mountd（マウント デーモン）Portmap 要求	情報	マウント デーモン（mountd）ポートのポートマッパーに要求が送信された場合にトリガーされます。
6175	400048	rexd（リモート実行デーモン）Portmap 要求	情報	リモート実行デーモン（rexd）ポートのポートマッパーに要求が送信された場合にトリガーされます。
6180	400049	rexd（リモート実行デーモン）攻撃	情報	rexd プログラムが呼び出された場合にトリガーされます。リモート実行デーモンは、リモート プログラムの実行を担当するサーバです。これは、システム リソースに不正アクセスする攻撃の兆候である可能性があります。
6190	400050	statd バッファ オーバーフロー	攻撃	大規模な statd 要求が送信された場合にトリガーされます。これは、バッファをオーバーフローさせ、システム リソースにアクセスする攻撃である可能性があります。

例　次の例では、シグニチャ 6100 をディセーブルにします。

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

関連コマンド

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

ip local pool

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

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

no ip local pool *poolname*

シンタックスの説明

first-address	IP アドレスの範囲の開始アドレスを指定します。
last-address	IP アドレスの範囲の最終アドレスを指定します。
mask *mask*	（オプション）アドレス プールのサブネット マスクを指定します。
poolname	IP アドレス プールの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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

VPN クライアントに割り当てられた IP アドレスが非標準のネットワークに属する場合は、マスク値を指定する必要があります。デフォルト マスクを使用すると、データが誤ってルーティングされる可能性があります。一般的な例として、デフォルトでクラス A ネットワークになっている IP ローカル プールに 10.10.10.0/255.255.255.0 のアドレスが含まれている場合を考えます。この場合、VPN クライアントが複数のインターフェイス上で 10 ネットワーク内の複数のサブネットにアクセスしようとすると、ルーティングの問題が発生する可能性があります。たとえば、アドレス 10.10.100.1/255.255.255.0 のプリンタがインターフェイス 2 経由で使用可能で、10.10.10.0 ネットワークが VPN トンネル上およびインターフェイス 1 経由で使用可能な場合、VPN クライアントでは、プリンタ宛のデータのルーティング先について混乱が生じます。10.10.10.0 と 10.10.100.0 のサブネットは両方とも 10.0.0.0 クラス A ネットワークに該当するため、プリンタのデータは VPN トンネル上で送信される場合があります。

例

次の例では、firstpool という IP アドレス プールを設定します。開始アドレスは 10.20.30.40 で、終了アドレスは 10.20.30.50 です。ネットワーク マスクは 255.255.255.0 です。

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

関連コマンド

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

ip-comp

LZS IP 圧縮をイネーブルにするには、グループポリシー コンフィギュレーション モードで **ip-comp enable** コマンドを使用します。IP 圧縮をディセーブルにするには、**ip-comp disable** コマンドを使用します。

ip-comp アトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、値を別のグループポリシーから継承できます。

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

no ip-comp

シンタックスの説明

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

デフォルト

IP 圧縮はディセーブルになっています。

コマンドのモード

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

データ圧縮をイネーブルにすると、モデムで接続しているリモート ダイヤルイン ユーザのデータ伝送速度が向上する場合があります。

注意　データ圧縮を行うと、各ユーザ セッションのメモリ要件と CPU 使用率が増加するため、セキュリティ アプライアンスのスループット全体が低下します。このため、データ圧縮は、モデムで接続しているリモート ユーザに対してのみイネーブルにすることをお勧めします。モデム ユーザに固有のグループポリシーを設計し、このユーザに対してのみ圧縮をイネーブルにします。

例

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

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

ip-phone-bypass

IP Phone Bypass をイネーブルにするには、グループポリシー コンフィギュレーション モードで **ip-phone-bypass enable** コマンドを使用します。IP Phone Bypass をディセーブルにするには、**ip-phone-bypass disable** コマンドを使用します。IP phone Bypass アトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、IP Phone Bypass の値を別のグループポリシーから継承できます。

IP Phone Bypass を使用すると、ハードウェア クライアントの背後にある IP 電話を接続するときに、ユーザ認証プロセスが不要になります。イネーブルの場合、Secure Unit Authentication は有効なままになります。

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

no ip-phone-bypass

シンタックスの説明

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

デフォルト

IP Phone Bypass はディセーブルになっています。

コマンドのモード

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

IP Phone Bypass を設定する必要があるのは、ユーザ認証をイネーブルにした場合のみです。

例

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

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

関連コマンド

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

ips

ASA 5500 シリーズ適応型セキュリティ アプライアンスは、AIP SSM をサポートしています。AIP SSM は拡張 IPS ソフトウェアを実行して、インライン モードまたはプロミスキャス モードで詳細なセキュリティ検査を実行します。セキュリティ アプライアンスが AIP SSM にパケットを転送するのは、パケットが出力インターフェイスを通過する直前（または VPN 暗号化が設定されている場合は暗号化が行われる前）と、他のファイアウォール ポリシーが適用された後です。たとえば、アクセスリストによってブロックされたパケットは、AIP SSM に転送されません。

セキュリティ アプライアンスからのトラフィックを AIP SSM に割り当てるには、クラス コンフィギュレーション モードで **ips** コマンドを使用します。このコマンドを削除するには、このコマンドの **no** 形式を使用します。

ips {***inline*** | ***promiscuous***} {***fail-close*** | ***fail-open***}

no ips {***inline*** | ***promiscuous***} {***fail-close*** | ***fail-open***}

シンタックスの説明

fail-close	AIP SSM に障害が発生した場合にトラフィックをブロックします。
fail-open	AIP SSM に障害が発生した場合にトラフィックを許可します。
inline	AIP SSM にパケットを転送します。パケットは、IPS 動作の結果としてドロップされる場合があります。
promiscuous	AIP SSM に対するパケットを複製します。元のパケットを AIP SSM でドロップすることはできません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
クラス 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

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

AIP SSM にトラフィックを転送するようにセキュリティ アプライアンスを設定したら、AIP SSM の検査と保護ポリシーを設定します。このポリシーは、トラフィックの検査方法と、進入が検知されたときの処理を判別します。セキュリティ アプライアンスから AIP SSM へのセッションを確立するか（**session** コマンド）、または管理インターフェイス上で SSH や Telnet を使用して AIP SSM に直接接続することができます。別の方法として、ASDM を使用することもできます。AIP SSM の設定の詳細については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface*』を参照してください。

例

次の例では、プロミスキャス モードですべての IP トラフィックを AIP SSM に転送し、何らかの理由で AIP SSM カードに障害が発生した場合には、すべての IP トラフィックをブロックします。

```
hostname(config)# access-list IPS permit ip any any
hostname(config)# class-map my-ips-class
hostname(config-cmap)# match access-list IPS
hostname(config-cmap)# policy-map my-ids-policy
hostname(config-pmap)# class my-ips-class
hostname(config-pmap-c)# ips promiscuous fail-close
hostname(config-pmap-c)# service-policy my-ips-policy 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。
class-map	ポリシーマップで使用するトラフィックを指定します。
clear configure policy-map	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。ただし、ポリシーマップが **service-policy** コマンド内で使用されている場合、そのポリシーマップは削除されません。
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	現在のすべての**ポリシーマップ** コンフィギュレーションを表示します。

ipsec-udp

IPSec over UDP をイネーブルにするには、グループポリシー コンフィギュレーション モードで **ipsec-udp enable** コマンドを使用します。IPSec over UDP をディセーブルにするには、**ipsec-udp disable** コマンドを使用します。IPSec over UDP アトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、IPSec over UDP の値を別のグループポリシーから継承できます。

IPSec over UDP（IPSec through NAT と呼ばれる場合もある）を使用すると、Cisco VPN Client またはハードウェア クライアントから、NAT を実行しているセキュリティ アプライアンスに UDP を介して接続できます。

ipsec-udp {enable | disable}

no ipsec-udp

シンタックスの説明

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

デフォルト

IPSec over UDP はディセーブルになっています。

コマンドのモード

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 over UDP を使用するには、**ipsec-udp-port** コマンドを設定する必要もあります。

また、Cisco VPN Client でも、IPSec over UDP を使用するように設定する必要があります（デフォルトでは、使用するように設定されています）。VPN 3002 では、IPSec over UDP を使用するように設定する必要はありません。

IPSec over UDP は独自の方式で、リモートアクセス接続のみに適用され、モード コンフィギュレーションを必要とします。これは、SA のネゴシエート中にセキュリティ アプライアンスがクライアントとコンフィギュレーション パラメータを交換することを意味します。

IPSec over UDP を使用すると、システム パフォーマンスがわずかに低下する場合があります。

例

次の例は、FirstGroup というグループポリシーに IPSec over UDP を設定する方法を示しています。

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

関連コマンド

コマンド	説明
ipsec-udp-port	セキュリティ アプライアンスが UDP トラフィックをリスンするポートを指定します。

ipsec-udp-port

IPSec over UDP の UDP ポート番号を設定するには、グループポリシー コンフィギュレーション モードで **ipsec-udp-port** コマンドを使用します。UDP ポートをディセーブルにするには、このコマンドの **no** 形式を使用します。このオプションを使用すると、IPSec over UDP ポートの値を別のグループポリシーから継承できます。

IPSec ネゴシエーションでは、セキュリティ アプライアンスは、設定済みのポート上でリスンし、そのポートに対する UDP トラフィックを転送します。これは、他のフィルタ規則によって UDP トラフィックがドロップされる場合でも同様です。

ipsec-udp-port *port*

no ipsec-udp-port

シンタックスの説明

port	4001 ～ 49151 の整数を使用して、UDP ポート番号を指定します。

デフォルト

デフォルト ポートは、10000 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
グループポリシー 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

この機能をイネーブルにした複数のグループポリシーを設定できます。グループポリシーごとに、別々のポート番号を使用できます。

例

次の例は、FirstGroup というグループポリシーの IPSec over UDP ポートをポート 4025 に設定する方法を示しています。

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

関連コマンド

コマンド	説明
ipsec-udp	Cisco VPN Client またはハードウェア クライアントから、NAT を実行しているセキュリティ アプライアンスに UDP を介して接続できるようにします。

ip verify reverse-path

Unicast RPF をイネーブルにするには、グローバル コンフィギュレーション モードで **ip verify reverse-path** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。Unicast RPF は、IP スプーフィング（パケットが不正な送信元 IP アドレスを使用して実際の送信元を隠す）から保護します。この機能により、すべてのパケットの送信元 IP アドレスが、ルーティング テーブルに従って、正しい送信元インターフェイスに一致することが保証されます。

ip verify reverse-path interface *interface_name*

no ip verify reverse-path interface *interface_name*

シンタックスの説明

interface_name	Unicast RPF をイネーブルにするインターフェイス。

デフォルト

この機能は、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
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

通常、セキュリティ アプライアンスは、パケットの転送先を判別するときは宛先アドレスだけを参照します。Unicast RPF は、送信元アドレスも参照するようにセキュリティ アプライアンスに指示します。この機能が Reverse Path Forwarding（RPF）と呼ばれるのはこのためです。セキュリティ アプライアンスを通過できるようにするすべてのトラフィックについて、送信元アドレスに戻るルートをセキュリティ アプライアンス ルーティング テーブルに含める必要があります。詳細については、RFC 2267 を参照してください。

たとえば、外部トラフィックについては、セキュリティ アプライアンスはデフォルト ルートを使用して Unicast RPF 保護を機能させることができます。外部インターフェイスからトラフィックが着信した場合、送信元アドレスがルーティング テーブルにおいて未知のときは、セキュリティ アプライアンスはデフォルト ルートを使用して、外部インターフェイスを送信元インターフェイスとして正しく識別します。

ルーティング テーブルにおいて既知のアドレスから外部インターフェイスにトラフィックが着信した場合、そのアドレスが内部インターフェイスに関連付けられているときは、セキュリティ アプライアンスはパケットをドロップします。同様に、未知の送信元アドレスから内部インターフェイスにトラフィックが着信した場合、一致したルート（デフォルト ルート）は外部インターフェイスを示すため、セキュリティ アプライアンスはパケットをドロップします。

Unicast RPF は、次のように実装されます。

- ICMP パケットにはセッションがないため、個々のパケットはチェックされません。
- UDP と TCP にはセッションがあるため、最初のパケットは逆ルート ルックアップが必要です。セッション中に到着する後続のパケットは、セッションの一部として保持されている既存の状態を使用してチェックされます。最初のパケット以外のパケットは、最初のパケットと同じインターフェイスに到着したことを保証するためにチェックされます。

例

次の例では、外部インターフェイス上で Unicast RPF をイネーブルにします。

```
hostname(config)# ip verify reverse-path interface outside
```

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。
clear ip verify statistics	Unicast RPF の統計情報を消去します。
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。

ipv6 access-list

IPv6 アクセスリストを設定するには、グローバル コンフィギュレーション モードで **ipv6 access-list** コマンドを使用します。ACE を削除するには、このコマンドの **no** 形式を使用します。アクセスリストは、セキュリティ アプライアンスが通過させる、またはブロックするトラフィックを定義します。

ipv6 access-list *id* [***line*** *line-num*] {***deny*** | ***permit***} {*protocol* | ***object-group*** *protocol_obj_grp_id*} {*source-ipv6-prefix*/*prefix-length* | ***any*** | ***host*** *source-ipv6-address* | ***object-group*** *network_obj_grp_id*} [*operator* {*port* [*port*] | ***object-group*** *service_obj_grp_id*}] {*destination-ipv6-prefix*/*prefix-length* | ***any*** | ***host*** *destination-ipv6-address* | ***object-group*** *network_obj_grp_id*} [{*operator port* [*port*] | ***object-group*** *service_obj_grp_id*}] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]]

no ipv6 access-list *id* [***line*** *line-num*] {***deny*** | ***permit***} {*protocol* | ***object-group*** *protocol_obj_grp_id*} {*source-ipv6-prefix*/*prefix-length* | ***any*** | ***host*** *source-ipv6-address* | ***object-group*** *network_obj_grp_id*} [*operator* {*port* [*port*] | ***object-group*** *service_obj_grp_id*}] {*destination-ipv6-prefix*/*prefix-length* | ***any*** | ***host*** *destination-ipv6-address* | ***object-group*** *network_obj_grp_id*} [{*operator port* [*port*] | ***object-group*** *service_obj_grp_id*}] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]]

ipv6 access-list *id* [***line*** *line-num*] {***deny*** | ***permit***} ***icmp6*** {*source-ipv6-prefix*/*prefix-length* | ***any*** | ***host*** *source-ipv6-address* | ***object-group*** *network_obj_grp_id*} {*destination-ipv6-prefix*/*prefix-length* | ***any*** | ***host*** *destination-ipv6-address* | ***object-group*** *network_obj_grp_id*} [*icmp_type* | ***object-group*** *icmp_type_obj_grp_id*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]]

no ipv6 access-list *id* [***line*** *line-num*] {***deny*** | ***permit***} ***icmp6*** {*source-ipv6-prefix*/*prefix-length* | ***any*** | ***host*** *source-ipv6-address* | ***object-group*** *network_obj_grp_id*} {*destination-ipv6-prefix*/*prefix-length* | ***any*** | ***host*** *destination-ipv6-address* | ***object-group*** *network_obj_grp_id*} [*icmp_type* | ***object-group*** *icmp_type_obj_grp_id*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]]

シンタックスの説明

any	IPv6 プレフィックス ::/0 の短縮形で、任意の IPv6 アドレスを示します。
default	（オプション）ACE 用に syslog メッセージ 106100 が生成されるように指定します。
deny	条件に合致している場合、アクセスを拒否します。
destination-ipv6-address	トラフィックを受信するホストの IPv6 アドレス。
destination-ipv6-prefix	トラフィックの宛先となる IPv6 ネットワーク アドレス。
disable	（オプション）syslog メッセージングをディセーブルにします。
host	アドレスが特定のホストを指していることを指定します。
icmp6	セキュリティ アプライアンスを通過する ICMPv6 トラフィックにアクセス規則が適用されるように指定します。

icmp_type	アクセス規則によってフィルタリングされる ICMP メッセージ タイプを指定します。値は、有効な ICMP タイプ番号（0 ～ 255）または次の ICMP タイプ リテラルのいずれかにできます。 • destination-unreachable • packet-too-big • time-exceeded • parameter-problem • echo-request • echo-reply • membership-query • membership-report • membership-reduction • router-renumbering • router-solicitation • router-advertisement • neighbor-solicitation • neighbor-advertisement • neighbor-redirect *icmp_type* 引数を省略すると、すべての ICMP タイプを示します。
icmp_type_obj_grp_id	（オプション）オブジェクト グループの ICMP タイプ ID を指定します。
id	アクセスリストの名前または番号。
interval *secs*	（オプション）syslog メッセージ 106100 を生成する時間間隔を指定します。有効値の範囲は 1 ～ 600 秒です。デフォルトの間隔は 300 秒です。この値は、非アクティブのフローを削除するためのタイムアウト値としても使用されます。
level	（オプション）メッセージ 106100 の syslog レベルを指定します。有効値の範囲は 0 ～ 7 です。デフォルト レベルは 6（情報）です。
line *line-num*	（オプション）アクセス規則を挿入するリスト内の行番号。行番号を指定しない場合、ACE はアクセスリストの末尾に追加されます。
log	（オプション）ACE のロギング アクションを指定します。**log** キーワードを指定しない場合や、**log default** キーワードを指定した場合、ACE によってパケットが拒否されると、メッセージ 106023 が生成されます。log キーワードを単独で指定した場合や、レベルまたは間隔と一緒に指定した場合、ACE によってパケットが拒否されると、メッセージ 106100 が生成されます。アクセスリストの末尾にある暗黙的な拒否によって拒否されるパケットについては、ログに記録されません。ロギングをイネーブルにするには、ACE でパケットを明示的に拒否する必要があります。
network_obj_grp_id	既存のネットワーク オブジェクト グループの ID。
object-group	（オプション）オブジェクト グループを指定します。
operator	（オプション）送信元 IP アドレスを宛先 IP アドレスと比較するための演算子を指定します。*operator* は、送信元 IP アドレスまたは宛先 IP アドレスのポートを比較します。使用できる演算子は、**lt**（小なり）、**gt**（大なり）**eq**（同値）、**neq**（非同値）、および **range**（範囲）です。すべてのポートを含めるには（デフォルト）、演算子およびポートを使用せずに **ipv6 access-list** コマンドを使用します。

permit	条件に合致している場合、アクセスを許可します。
port	（オプション）アクセスを許可または拒否するポートを指定します。*port* 引数を入力する場合は、0 ～ 65535 の数を使用するか、*protocol* が ***tcp*** または ***udp*** であればリテラル名を使用して、ポートを指定します。 使用可能な TCP リテラル名は、**aol**、**bgp**、**chargen**、**cifc**、**citrix-ica**、**cmd**、**ctiqbe**、**daytime**、**discard**、**domain**、**echo**、**exec**、**finger**、**ftp**、**ftp-data**、**gopher**、**h323**、**hostname**、**http**、**https**、**ident**、**irc**、**kerberos**、**klogin**、**kshell**、**ldap**、**ldaps**、**login**、**lotusnotes**、**lpd**、**netbios-ssn**、**nntp**、**pop2**、**pop3**、**pptp**、**rsh**、**rtsp**、**smtp**、**sqlnet**、**ssh**、**sunrpc**、**tacacs**、**talk**、**telnet**、**uucp**、**whois**、および **www** です。 使用可能な UDP リテラル名は、**biff**、**bootpc**、**bootps**、**cifs**、**discard**、**dnsix**、**domain**、**echo**、**http**、**isakmp**、**kerberos**、**mobile-ip**、**nameserver**、**netbios-dgm**、**netbios-ns**、**ntp**、**pcanywhere-status**、**pim-auto-rp**、**radius**、**radius-acct**、**rip**、**secureid-udp**、**snmp**、**snmptrap**、**sunrpc**、**syslog**、**tacacs**、**talk**、**tftp**、**time**、**who**、**www**、および **xdmcp** です。
prefix-length	アドレスの高次の連続ビットのうち、何個が IPv6 プレフィックス（IPv6 アドレスのネットワーク部分）を構成しているかを指定します。
protocol	IP プロトコルの名前または番号。有効値は、**icmp**、**ip**、**tcp**、**udp** のいずれか、または IP プロトコル番号を表す 1 ～ 254 までの整数です。
protocol_obj_grp_id	既存のプロトコル オブジェクト グループの ID。
service_obj_grp_id	（オプション）オブジェクト グループを指定します。
source-ipv6-address	トラフィックを送信するホストの IPv6 アドレス。
source-ipv6-prefix	ネットワーク トラフィックの発信元の IPv6 ネットワーク アドレス。

デフォルト

log キーワードを指定したときの syslog メッセージ 106100 のデフォルト レベルは、6（情報）です。

デフォルトのロギング間隔は 300 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。

使用上のガイドライン

ipv6 access-list コマンドを使用すると、IPv6 アドレスがポートまたはプロトコルにアクセスすることを許可または拒否するかどうかを指定できます。各コマンドは、ACE と呼ばれます。同じアクセスリスト名を持つ 1 つまたは複数の ACE は、アクセスリストと呼ばれます。アクセスリストをインターフェイスに適用するには、**access-group** コマンドを使用します。

アクセスリストを使用してアクセスを特別に許可しない限り、セキュリティ アプライアンスは、外部インターフェイスから内部インターフェイスへのパケットをすべて拒否します。内部インターフェイスから外部インターフェイスへのすべてのパケットは、特にアクセスを拒否しない限り、デフォルトで許可されます。

ipv6 access-list コマンドは、IPv6 専用であるという点を除き、**access-list** コマンドと類似しています。アクセスリストの詳細については、**access-list extended** コマンドを参照してください。

ipv6 access-list icmp コマンドは、セキュリティ アプライアンスを通過する ICMPv6 メッセージをフィルタリングするために使用されます。特定のインターフェイスでの発信および終端を許可する ICMPv6 トラフィックを設定するには、**ipv6 icmp** コマンドを使用します。

オブジェクト グループの設定方法については、**object-group** コマンドの項を参照してください。

例

次の例では、TCP を使用するすべてのホストが 3001:1::203:A0FF:FED6:162D のサーバにアクセスできるようにします。

```
hostname(config)# ipv6 access-list acl_grp permit tcp any host
3001:1::203:A0FF:FED6:162D
```

次の例では、**eq** とポートを使用して、FTP へのアクセスのみを拒否します。

```
hostname(config)# ipv6 access-list acl_out deny tcp any host
3001:1::203:A0FF:FED6:162D eq ftp
hostname(config)# access-group acl_out in interface inside
```

次の例では、**lt** を使用して、ポート 2025 より小さいすべてのポートへのアクセスを許可します。その結果、既知ポート（1 ～ 1024）へのアクセスが許可されます。

```
hostname(config)# ipv6 access-list acl_dmz1 permit tcp any host
3001:1::203:A0FF:FED6:162D lt 1025
hostname(config)# access-group acl_dmz1 in interface dmz1
```

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割り当てます。
ipv6 icmp	セキュリティ アプライアンスのインターフェイスで終端する ICMP メッセージに対して、アクセス規則を設定します。
object-group	オブジェクト グループ（アドレス、ICMP タイプ、およびサービス）を作成します。

ipv6 address

IPv6 をイネーブルにし、インターフェイス上で IPv6 アドレスを設定するには、インターフェイス コンフィギュレーション モードで **ipv6 address** コマンドを使用します。IPv6 アドレスを削除するには、このコマンドの **no** 形式を使用します。

ipv6 address {***autoconfig*** | *ipv6-prefix*/*prefix-length* [***eui-64***] | *ipv6-address* ***link-local***}

no ipv6 address {***autoconfig*** | *ipv6-prefix*/*prefix-length* [***eui-64***] | *ipv6-address* ***link-local***}

シンタックスの説明

autoconfig	インターフェイス上でステートレス自動設定を使用して、IPv6 アドレスの自動設定をイネーブルにします。
eui-64	（オプション）IPv6 アドレスの下位 64 ビットにインターフェイス ID を指定します。
ipv6-address	インターフェイスに割り当てられた IPv6 リンク ローカル アドレス。
ipv6-prefix	インターフェイスに割り当てられた IPv6 ネットワーク アドレス。
link-local	アドレスがリンク ローカル アドレスであることを指定します。
prefix-length	アドレスの高次の連続ビットのうち、何個が IPv6 プレフィックス（IPv6 アドレスのネットワーク部分）を構成しているかを指定します。

デフォルト

IPv6 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
インターフェイス 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

インターフェイス上で IPv6 アドレスを設定すると、IPv6 がそのインターフェイス上でイネーブルになります。IPv6 アドレスの指定後に **ipv6 enable** コマンドを使用する必要はありません。

ipv6 address ***autoconfig*** コマンドは、ステートレス自動設定を使用して、インターフェイス上で IPv6 アドレスの自動設定をイネーブルにするために使用されます。アドレスは、ルータ アドバタイズメント メッセージで受信されたプレフィックスに基づいて設定されます。リンク ローカル アドレスが設定されていなければ、このインターフェイス用に自動的に生成されます。そのリンク ローカル アドレスを別のホストが使用している場合は、エラー メッセージが表示されます。

ipv6 address eui-64 コマンドは、インターフェイスの IPv6 アドレスを設定するために使用されます。オプションの **eui-64** が指定されている場合は、アドレスの下位 64 ビットに EUI-64 インターフェイス ID が使用されます。*prefix-length* 引数に指定した値が 64 ビットより大きい場合は、プレフィックス ビットがインターフェイス ID に優先します。指定されたアドレスを別のホストが使用している場合は、エラー メッセージが表示されます。

Modified EUI-64 形式のインターフェイス ID は、リンク レイヤ アドレスの上位 3 バイト（OUI フィールド）と下位 3 バイト（シリアル番号）の間に 16 進数の FFFE を挿入することで、48 ビット リンク レイヤ（MAC）アドレスから生成されます。選択されたアドレスが一意のイーサネット MAC アドレスから生成されることを保証するため、上位バイトの下位から 2 番目のビット（ユニバーサル / ローカル ビット）が反転され、48 ビット アドレスの一意性が示されます。たとえば、MAC アドレス 00E0.B601.3B7A のインターフェイスには、02E0:B6FF:FE01:3B7A の 64 ビット インターフェイス ID が指定されます。

ipv6 address *link-local* コマンドは、インターフェイスの IPv6 リンク ローカル アドレスを設定するために使用されます。このコマンドで指定する *ipv6-address* は、インターフェイス用に自動的に生成されるリンク ローカル アドレスを上書きします。リンク ローカル アドレスは、リンク ローカル プレフィックス FE80::/64 と、Modified EUI-64 形式のインターフェイス ID で構成されます。MAC アドレス 00E0.B601.3B7A のインターフェイスには、リンク ローカル アドレス FE80::2E0:B6FF:FE01:3B7A が指定されます。指定されたアドレスを別のホストが使用している場合は、エラー メッセージが表示されます。

例

次の例では、選択したインターフェイスのグローバル アドレスとして 3FFE:C00:0:1::576/64 を割り当てます。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 address 3ffe:c00:0:1::576/64
```

次の例では、選択したインターフェイスに IPv6 アドレスを自動的に割り当てます。

```
hostname(config)# interface gigabitethernet 0/1
hostname(config-if)# ipv6 address autoconfig
```

次の例では、選択したインターフェイスに IPv6 アドレス 3FFE:C00:0:1::/64 を割り当て、アドバイザーの下位 64 ビットに EUI-64 インターフェイス ID を指定します。

```
hostname(config)# interface gigabitethernet 0/2
hostname(onfig-if)# ipv6 address 3FFE:C00:0:1::/64 eui-64
```

次の例では、選択したインターフェイスのリンク レベル アドレスとして FE80::260:3EFF:FE11:6670 を割り当てます。

```
hostname(config)# interface gigabitethernet 0/3
hostname(config-if)# ipv6 address FE80::260:3EFF:FE11:6670 link-local
```

関連コマンド

コマンド	説明
debug ipv6 interface	IPv6 インターフェイスに関するデバッグ情報を表示します。
show ipv6 interface	IPv6 用に設定したインターフェイスのステータスを表示します。

ipv6 enable

明示的な IPv6 アドレスが設定されていないインターフェイス上で IPv6 処理をイネーブルにするには、インターフェイス コンフィギュレーション モードで **ipv6 enable** コマンドを使用します。明示的な IPv6 アドレスが設定されていないインターフェイス上で IPv6 処理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。

ipv6 enable

no ipv6 enable

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

IPv6 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
インターフェイス 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

ipv6 enable コマンドは、インターフェイス上で IPv6 リンク ローカル ユニキャスト アドレスを自動的に設定し、インターフェイスの IPv6 処理をイネーブルにします。

no ipv6 enable コマンドは、明示的な IPv6 アドレスが指定されているインターフェイス上では IPv6 処理をディセーブルにしません。

例

次の例では、選択したインターフェイス上で IPv6 処理をイネーブルにします。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 enable
```

関連コマンド

コマンド	説明
ipv6 address	インターフェイスの IPv6 アドレスを設定し、インターフェイス上で IPv6 処理をイネーブルにします。
show ipv6 interface	IPv6 用に設定したインターフェイスのユーザビリティ ステータスを表示します。

ipv6 icmp

インターフェイスの ICMP アクセス規則を設定するには、グローバル コンフィギュレーション モードで **ipv6 icmp** コマンドを使用します。ICMP アクセス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。

ipv6 icmp {***permit*** | ***deny***} {*ipv6-prefix*/*prefix-length* | ***any*** | ***host*** *ipv6-address*} [*icmp-type*] *if-name*

no ipv6 icmp {***permit*** | ***deny***} {*ipv6-prefix*/*prefix-length* | ***any*** | ***host*** *ipv6-address*} [*icmp-type*] *if-name*

シンタックスの説明

any	任意の IPv6 アドレスを指定するキーワード。IPv6 プレフィックス ::/0 の短縮形。
deny	選択したインターフェイス上で、指定した ICMP トラフィックを拒否します。
host	アドレスが特定のホストを指していることを指定します。
icmp-type	アクセス規則によってフィルタリングされる ICMP メッセージ タイプを指定します。値は、有効な ICMP タイプ番号（0 ～ 255）または次の ICMP タイプ リテラルのいずれかにできます。 • destination-unreachable • packet-too-big • time-exceeded • parameter-problem • echo-request • echo-reply • membership-query • membership-report • membership-reduction • router-renumbering • router-solicitation • router-advertisement • neighbor-solicitation • neighbor-advertisement • neighbor-redirect
if-name	アクセス規則の適用先となるインターフェイスの名前（**nameif** コマンドで指定したもの）。
ipv6-address	ICMPv6 メッセージをインターフェイスに送信するホストの IPv6 アドレス。
ipv6-prefix	ICMPv6 メッセージをインターフェイスに送信する IPv6 ネットワーク。
permit	選択したインターフェイス上で、指定した ICMP トラフィックを許可します。
prefix-length	IPv6 プレフィックスの長さ。この値は、アドレスの高次の連続ビットのうち、何個がプレフィックス（ネットワーク部分）を構成しているかを指定します。プレフィックスの長さ値の前に、スラッシュ（/）を入力する必要があります。

デフォルト

ICMP アクセス規則が定義されていない場合、ICMP トラフィックはすべて許可されます。

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。

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
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

IPv6 機能の ICMP は、IPv4 の ICMP と同じです。ICMPv6 は、ICMP エコー要求メッセージおよび応答メッセージに類似した ICMP 宛先到達不能メッセージおよび情報メッセージなどのエラーメッセージを生成します。また、IPv6 の ICMP パケットは、IPv6 近隣探索プロセスとパス MTU 探索で使用されます。

インターフェイスに ICMP 規則が定義されていない場合、IPv6 ICMP トラフィックはすべて許可されます。

インターフェイスに ICMP 規則が定義されている場合は、最初に一致した規則が処理され、それ以降の規則はすべて暗黙的に拒否されます。たとえば、最初に一致した規則が許可規則の場合、その ICMP パケットは処理されます。最初に一致した規則が拒否規則の場合や、ICMP パケットがそのインターフェイス上のどの規則にも一致しなかった場合、セキュリティ アプライアンスはその ICMP パケットを廃棄し、syslog メッセージを生成します。

このため、ICMP 規則に入力する順序が重要になります。特定のネットワークからの ICMP トラフィックをすべて拒否する規則を入力してから、そのネットワーク上にある特定のホストからの ICMP トラフィックを許可する規則を入力した場合、そのホスト規則が処理されることはありません。ICMP トラフィックは、ネットワーク規則によってブロックされます。ただし、ホスト規則を入力してから、ネットワーク規則を入力した場合、ホストの ICMP トラフィックは許可されますが、それ以外の当該ネットワークからの ICMP トラフィックはすべてブロックされます。

ipv6 icmp コマンドは、セキュリティ アプライアンス インターフェイスで終端する ICMP トラフィックのアクセス規則を設定します。パススルー ICMP トラフィックのアクセス規則を設定するには、**ipv6 access-list** コマンドを参照してください。

例

次の例では、外部インターフェイスで、すべての ping 要求を拒否し、すべての Packet Too Big メッセージを許可します（パス MTU 探索をサポートするため）。

```
hostname(config)# ipv6 icmp deny any echo-reply outside
hostname(config)# ipv6 icmp permit any packet-too-big outside
```

次の例では、ホスト 2000:0:0:4::2 またはプレフィックス 2001::/64 上のホストに、外部インターフェイスへの ping を許可します。

```
hostname(config)# ipv6 icmp permit host 2000:0:0:4::2 echo-reply outside
hostname(config)# ipv6 icmp permit 2001::/64 echo-reply outside
hostname(config)# ipv6 icmp permit any packet-too-big outside
```

関連コマンド

コマンド	説明
ipv6 access-list	アクセスリストを設定します。

ipv6 nd dad attempts

重複アドレスの検出中にインターフェイス上で送信される連続的なネイバー送信要求メッセージの数を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd dad attempts** コマンドを使用します。送信される重複アドレス検出メッセージの数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。

ipv6 nd dad attempts *value*

no ipv6 nd dad [**attempts** *value*]

シンタックスの説明

value	0 ～ 600 の数。0 を入力すると、指定されたインターフェイス上で重複アドレス検出がディセーブルになります。1 を入力すると、1 回だけ送信するように設定されます。デフォルト値は 1 つのメッセージです。

デフォルト

デフォルトの試行回数は 1 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
インターフェイス 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

アドレスがインターフェイスに割り当てられる前に、重複アドレス検出によって、新しいユニキャスト IPv6 アドレスの一意性が確認されます（重複アドレス検出の実行中、新しいアドレスは一時的な状態になります）。重複アドレス検出では、ネイバー送信要求メッセージを使用して、ユニキャスト IPv6 アドレスの一意性を確認します。ネイバー送信要求メッセージの送信頻度を設定するには、**ipv6 nd ns-interval** コマンドを使用します。

管理上のダウン状態にあるインターフェイスでは、重複アドレス検出は一時停止されます。インターフェイスが管理上のダウン状態にある場合、そのインターフェイスに割り当てられたユニキャスト IPv6 アドレスは保留状態に設定されます。

インターフェイスが管理上のアップ状態に戻ると、インターフェイス上で重複アドレス検出が自動的に再開されます。管理上のアップ状態に戻っているインターフェイスでは、インターフェイス上のすべてのユニキャスト IPv6 アドレスに対して重複アドレス検出が再開されます。

（注） インターフェイスのリンク ローカル アドレスに対して重複アドレス検出が実行されている間、他の IPv6 アドレスは引き続き一時的な状態に設定されます。リンク ローカル アドレスに対する重複アドレス検出が完了すると、残りの IPv6 アドレスに対して重複アドレス検出が実行されます。

重複アドレス検出によって重複アドレスが特定された場合、そのアドレスの状態は DUPLICATE に設定され、アドレスは使用されなくなります。重複アドレスがインターフェイスのリンク ローカル アドレスの場合は、そのインターフェイス上で IPv6 パケットの処理がディセーブルになり、次のようなエラー メッセージが発行されます。

```
%PIX-4-DUPLICATE: Duplicate address FE80::1 on outside
```

重複アドレスがインターフェイスのグローバル アドレスの場合、そのアドレスは使用されなくなり、次のようなエラー メッセージが発行されます。

```
%PIX-4-DUPLICATE: Duplicate address 3000::4 on outside
```

重複アドレスに関連付けられているコンフィギュレーション コマンドはすべて設定済みのままになりますが、アドレスの状態は DUPLICATE に設定されます。

インターフェイスのリンク ローカル アドレスが変更された場合は、新しいリンク ローカル アドレスに対して重複アドレス検出が実行され、そのインターフェイスに関連付けられている他の IPv6 アドレスがすべて再生成されます（重複アドレス検出は新しいリンク ローカル アドレスに対してのみ実行されます）。

例

次の例では、インターフェイスの一時的なユニキャスト IPv6 アドレスに対して重複アドレス検出が実行されている間に 5 つの連続したネイバー送信要求メッセージが送信されるように設定します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd dad attempts 5
```

次の例では、選択したインターフェイス上で重複アドレス検出をディセーブルにします。

```
hostname(config)# interface gigabitethernet 0/1
hostname(config-if)# ipv6 nd dad attempts 0
```

関連コマンド

コマンド	説明
ipv6 nd ns-interval	インターフェイス上でネイバー送信要求メッセージの送信間隔を設定します。
show ipv6 interface	IPv6 用に設定したインターフェイスのユーザビリティ ステータスを表示します。

ipv6 nd ns-interval

インターフェイス上で IPv6 ネイバー送信要求メッセージの再送信間隔を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd ns-interval** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd ns-interval *value*

no ipv6 nd ns-interval [*value*]

シンタックスの説明

value	IPv6 ネイバー送信要求メッセージの送信間隔（ミリ秒単位）。有効となる値の範囲は 1,000 ～ 3,600,000 ミリ秒です。デフォルト値は 1,000 ミリ秒です。

デフォルト

ネイバー送信要求メッセージの送信間隔は 1,000 ミリ秒になっています。

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
インターフェイス 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

この値は、このインターフェイスから送信されるすべての IPv6 ルータ アドバタイズメントに含まれます。

例

次の例では、Gigabitethernet 0/0 に対して IPv6 ネイバー送信要求メッセージの送信間隔を 9,000 ミリ秒に設定します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd ns-interval 9000
```

関連コマンド

コマンド	説明
show ipv6 interface	IPv6 用に設定したインターフェイスのユーザビリティ ステータスを表示します。

ipv6 nd prefix

IPv6 ルータ アドバタイズメントに含める IPv6 プレフィックスを設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd prefix** コマンドを使用します。プレフィックスを削除するには、このコマンドの **no** 形式を使用します。

ipv6 nd prefix *ipv6-prefix/prefix-length* | ***default*** [[*valid-lifetime preferred-lifetime*] | [***at*** *valid-date preferred-date*] | ***infinite*** | ***no-advertise*** | ***off-link*** | ***no-autoconfig***]

no ipv6 nd prefix *ipv6-prefix/prefix-length* | ***default*** [[*valid-lifetime preferred-lifetime*] | [***at*** *valid-date preferred-date*] | ***infinite*** | ***no-advertise*** | ***off-link*** | ***no-autoconfig***]

シンタックスの説明

at *valid-date preferred-date*	ライフタイムと優先順位が期限切れになる日付と時刻。プレフィックスは、この指定された日付と時刻に到達するまで有効になります。有効期限の形式は、*date-valid-expire month-valid-expire hh:mm-valid-expire date-prefer-expire month-prefer-expire hh:mm-prefer-expire* です。
default	デフォルト値が使用されます。
infinite	（オプション）この有効ライフタイムは期限切れになりません。
ipv6-prefix	ルータ アドバタイズメントに含める IPv6 ネットワーク番号。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
no-advertise	（オプション）ローカル リンク上のホストに対して、指定されたプレフィックスが IPv6 自動設定に使用されないことを示します。
no-autoconfig	（オプション）ローカル リンク上のホストに対して、指定されたプレフィックスが IPv6 自動設定に使用不能であることを示します。
off-link	（オプション）指定されたプレフィックスがオンリンクの判別に使用されないことを示します。
preferred-lifetime	指定された IPv6 プレフィックスが優先されたものとしてアドバタイズされる期間（秒単位）。有効となる値の範囲は、0 ～ 4,294,967,295 秒です。最大値は、無限を意味します。infinite で指定することもできます。デフォルトは 604,800（7 日）です。
prefix-length	IPv6 プレフィックスの長さ。この値は、アドレスの高次の連続ビットのうち、何個がプレフィックス（ネットワーク部分）を構成しているかを指定します。プレフィックスの長さ値の前に、スラッシュ（/）を入力する必要があります。
valid-lifetime	指定された IPv6 プレフィックスが有効なものとしてアドバタイズされる期間。有効となる値の範囲は、0 ～ 4,294,967,295 秒です。最大値は、無限を意味します。**infinite** として指定することもできます。デフォルトは 2,592,000（30 日）です。

デフォルト

IPv6 ルータ アドバタイズメントを発信するインターフェイス上で設定されたすべてのプレフィックスがアドバタイズされる場合、有効ライフタイム 2,592,000 秒（30 日）と優先ライフタイム 604,800 秒（7 日）が使用され、「onlink」フラグと「autoconfig」フラグの両方が設定されます。

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。

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
インターフェイス 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、プレフィックスをアドバタイズするかどうかなど、個別のパラメータをプレフィックスごとに制御できます。

デフォルトでは、**ipv6 address** コマンドを使用してインターフェイス上のアドレスとして設定されたプレフィックスは、ルータ アドバタイズメントでアドバタイズされます。**ipv6 nd prefix** コマンドを使用してアドバタイズメントのプレフィックスを設定すると、そのプレフィックスだけがアドバタイズされます。

default キーワードを使用すると、すべてのプレフィックスのデフォルト パラメータを設定できます。

日付を設定してプレフィックスの有効期限を指定することができます。有効ライフタイムと優先ライフタイムは、リアルタイムでカウントダウンされます。有効期限に到達すると、プレフィックスはアドバタイズされなくなります。

onlink が「オン」（デフォルト）の場合、指定されたプレフィックスはリンクに割り当てられます。指定されたプレフィックスを含むアドレスにトラフィックを送信するノードでは、宛先をリンク上でローカルに到達可能なものと見なします。

autoconfig が「オン」（デフォルト）の場合、ローカル リンク上のホストには、指定されたプレフィックスが IPv6 自動設定に使用可能であることが示されます。

例

次の例では、指定されたインターフェイスから送信されるルータ アドバタイズメントに、IPv6 プレフィックス 2001:200::/35、有効ライフタイム 1,000 秒、および優先ライフタイム 900 秒を含めます。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd prefix 2001:200::/35 1000 900
```

関連コマンド

コマンド	説明
ipv6 address	IPv6 アドレスを設定し、インターフェイス上で IPv6 処理をイネーブルにします。
show ipv6 interface	IPv6 用に設定したインターフェイスのユーザビリティ ステータスを表示します。

ipv6 nd ra-interval

インターフェイス上で IPv6 ルータ アドバタイズメントの送信間隔を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd ra-interval** コマンドを使用します。デフォルトの間隔に戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd ra-interval [***msec***] *value*

no ipv6 nd ra-interval [[***msec***] *value*]

シンタックスの説明

msec	（オプション）指定された値がミリ秒単位であることを示します。このキーワードがない場合、指定された値は秒単位となります。
value	IPv6 ルータ アドバタイズメントの送信間隔。有効値の範囲は 3 ～ 1,800 秒ですが、***msec*** キーワードが指定されている場合は 500 ～ 1,800,000 ミリ秒となります。デフォルトは、200 秒です。

デフォルト

200 秒

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
インターフェイス 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

ipv6 nd ra-lifetime コマンドを使用して セキュリティ アプライアンスをデフォルト ルータとして設定した場合、送信間隔は IPv6 ルータ アドバタイズメントのライフタイム以下にする必要があります。他の IPv6 ノードと同期させないようにするには、使用する実際の値を、指定された値の 20% 以内でランダムに調整します。

例

次の例では、選択したインターフェイスに対して IPv6 ルータ アドバタイズメントの送信間隔を 201 秒に設定します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd ra-interval 201
```

関連コマンド

コマンド	説明
ipv6 nd ra-lifetime	IPv6 ルータ アドバタイズメントのライフタイムを設定します。
show ipv6 interface	IPv6 用に設定したインターフェイスのユーザビリティ ステータスを表示します。

ipv6 nd ra-lifetime

インターフェイス上で IPv6 ルータ アドバタイズメントの「ルータ ライフタイム」を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd ra-lifetime** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd ra-lifetime *seconds*

no ipv6 nd ra-lifetime [*seconds*]

シンタックスの説明

seconds	このインターフェイスにおけるデフォルト ルータとしてのセキュリティ アプライアンスの有効期間。有効となる値の範囲は、0 ～ 9000 秒です。デフォルトは、1,800 秒です。0 は、セキュリティ アプライアンスを、選択したインターフェイス上のデフォルト ルータと見なさない必要があることを示します。

デフォルト

1,800 秒

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
インターフェイス 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

「ルータ ライフタイム」値は、インターフェイスから送信されるすべての IPv6 ルータ アドバタイズメントに含まれます。この値は、このインターフェイスにおけるデフォルト ルータとしてのセキュリティ アプライアンスの有効期間を示します。

値を 0 以外の値に設定することは、セキュリティ アプライアンスをこのインターフェイス上のデフォルト ルータと見なす必要があることを示します。「ルータ ライフタイム」値を 0 以外の値に設定する場合は、ルータ アドバタイズメントの送信間隔より小さくしないでください。

値を 0 に設定することは、セキュリティ アプライアンスをこのインターフェイス上のデフォルト ルータと見なさない必要があることを示します。

例

次の例では、選択したインターフェイスに対して IPv6 ルータ アドバタイズメントのライフタイムを 1,801 秒に設定します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd ra-lifetime 1801
```

関連コマンド

コマンド	説明
ipv6 nd ra-interval	インターフェイス上で IPv6 ルータ アドバタイズメントの送信間隔を設定します。
show ipv6 interface	IPv6 用に設定したインターフェイスのユーザビリティ ステータスを表示します。

ipv6 nd reachable-time

到達可能性の確認イベントが発生した後でリモート IPv6 ノードを到達可能と見なす期間を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd reachable-time** コマンドを使用します。デフォルト期間に戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd reachable-time *value*

no ipv6 nd reachable-time [*value*]

シンタックスの説明

value	リモート IPv6 ノードを到達可能と見なす期間（ミリ秒単位）。有効となる値の範囲は 0 ～ 3,600,000 ミリ秒です。デフォルトは 0 です。

デフォルト

0 ミリ秒。

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
インターフェイス 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

期間を設定すると、使用不可能なネイバーを検出できます。設定期間を短くすると、使用不可能なネイバーをより迅速に検出できます。ただし、期間を短くするほど、IPv6 ネットワークの帯域幅の消費量と、IPv6 ネットワーク デバイスすべての処理リソースの消費量が増加します。通常の IPv6 動作において、設定期間を大幅に短くすることはお勧めできません。

例

次の例では、選択したインターフェイスに対して IPv6 到達可能期間を 1,700,000 ミリ秒に設定します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd reachable-time 1700000
```

関連コマンド

コマンド	説明
show ipv6 interface	IPv6 用に設定したインターフェイスのユーザビリティ ステータスを表示します。

ipv6 nd suppress-ra

LAN インターフェイス上で IPv6 ルータ アドバタイズメントを送信しないようにするには、インターフェイス コンフィギュレーション モードで **ipv6 nd suppress-ra** コマンドを使用します。LAN インターフェイス上で IPv6 ルータ アドバタイズメントの送信を再度イネーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 nd suppress-ra

no ipv6 nd suppress-ra

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

IPv6 ユニキャスト ルーティングがイネーブルの場合は、LAN インターフェイス上でルータ アドバタイズメントが自動的に送信されます。

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
インターフェイス 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

LAN 以外のタイプのインターフェイス（たとえば、シリアル インターフェイスやトンネル インターフェイス）上で IPv6 ルータ アドバタイズメントの送信をイネーブルにするには、**no ipv6 nd suppress-ra** コマンドを使用します。

例

次の例では、選択したインターフェイス上で IPv6 ルータ アドバタイズメントを送信しないようにします。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd suppress-ra
```

関連コマンド

コマンド	説明
show ipv6 interface	IPv6 用に設定したインターフェイスのユーザビリティ ステータスを表示します。

ipv6 neighbor

IPv6 近隣探索キャッシュにスタティック エントリを設定するには、グローバル コンフィギュレーション モードで **ipv6 neighbor** コマンドを使用します。近隣探索キャッシュからスタティック エントリを削除するには、このコマンドの **no** 形式を使用します。

ipv6 neighbor *ipv6_address if_name mac_address*

no ipv6 neighbor *ipv6_address if_name* [*mac_address*]

シンタックスの説明

if_name	**nameif** コマンドによって指定される内部インターフェイス名または外部インターフェイス名。
ipv6_address	ローカルのデータリンク アドレスに対応する IPv6 アドレス。
mac_address	ローカルのデータライン（ハードウェア MAC）アドレス。

デフォルト

IPv6 近隣探索キャッシュにスタティック エントリは設定されていません。

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

ipv6 neighbor コマンドは、**arp** コマンドと類似しています。指定された IPv6 アドレスのエントリが近隣探索キャッシュにすでに存在する（IPv6 近隣探索プロセスからラーニングされた）場合、そのエントリはスタティック エントリに自動的に変換されます。**copy** コマンドを使用してコンフィギュレーションを格納すると、このエントリがコンフィギュレーションに格納されます。

IPv6 近隣探索キャッシュのスタティック エントリを表示するには、**show ipv6 neighbor** コマンドを使用します。

clear ipv6 neighbors コマンドは、IPv6 近隣探索キャッシュのすべてのエントリを、スタティック エントリを除いて削除します。**no ipv6 neighbor** コマンドは、指定したスタティック エントリを近隣探索キャッシュから削除します。このコマンドによってダイナミック エントリ（IPv6 近隣探索プロセスからラーニングされたエントリ）がキャッシュから削除されることはありません。**no ipv6 enable** コマンドを使用してインターフェイス上で IPv6 をディセーブルにすると、そのインターフェイスに設定された IPv6 近隣探索キャッシュのすべてのエントリが、スタティック エントリを除いて削除されます（エントリの状態は INCMP [Incomplete] に変更されます）。

近隣探索プロセスによって IPv6 近隣探索キャッシュのスタティック エントリが変更されることはありません。

例

次の例では、IPv6 アドレス 3001:1::45A および MAC アドレス 0002.7D1A.9472 の内部ホストのスタティック エントリを近隣探索キャッシュに追加します。

```
hostname(config)# ipv6 neighbor 3001:1::45A inside 0002.7D1A.9472
```

関連コマンド

コマンド	説明
clear ipv6 neighbors	IPv6 近隣探索キャッシュのすべてのエントリを、スタティック エントリを除いて削除します。
show ipv6 neighbor	IPv6 近隣 キャッシュ情報を表示します。

ipv6 route

IPv6 ルーティング テーブルに IPv6 ルートを追加するには、グローバル コンフィギュレーション モードで **ipv6 route** コマンドを使用します。IPv6 デフォルト ルートを削除するには、このコマンドの **no** 形式を使用します。

ipv6 route *if_name ipv6-prefix*/*prefix-length ipv6-address* [*administrative-distance*]

no ipv6 route *if_name ipv6-prefix*/*prefix-length ipv6-address* [*administrative-distance*]

シンタックスの説明

administrative-distance	（オプション）ルートの管理ディスタンス。デフォルト値は 1 です。この場合、スタティック ルートは、接続済みルートを除く他のあらゆるタイプのルートに優先します。
if_name	ルートの設定対象となるインターフェイスの名前。
ipv6-address	特定のネットワークに到達するために使用できるネクストホップの IPv6 アドレス。
ipv6-prefix	スタティック ルートの宛先となる IPv6 ネットワーク。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
prefix-length	IPv6 プレフィックスの長さ。この値は、アドレスの高次の連続ビットのうち、何個がプレフィックス（ネットワーク部分）を構成しているかを指定します。プレフィックスの長さ値の前に、スラッシュ（/）を入力する必要があります。

デフォルト

デフォルトでは、*administrative-distance* は 1 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

IPv6 ルーティング テーブルの内容を表示するには、**show ipv6 route** コマンドを使用します。

例

次の例では、ネットワーク 7fff::0/32 に対するパケットを、管理ディスタンス 110 で、3FFE:1100:0:CC00::1 にある内部インターフェイス上のネットワーキング デバイスにルーティングします。

```
hostname(config)# ipv6 route inside 7fff::0/32 3FFE:1100:0:CC00::1 110
```

関連コマンド

コマンド	説明
debug ipv6 route	IPv6 のルーティング テーブル アップデートおよびルート キャッシュ アップデートに関するデバッグ情報を表示します。
show ipv6 route	IPv6 ルーティング テーブルの現在の内容を表示します。

isakmp am-disable

アグレッシブ モードの着信接続をディセーブルにするには、グローバル コンフィギュレーション モードで **isakmp am-disable** コマンドを使用します。アグレッシブ モードの着信接続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。

isakmp am-disable

no isakmp am-disable

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

デフォルト値はイネーブルです。

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。

例

次の例では、グローバル コンフィギュレーション モードで、アグレッシブ モードの着信接続をディセーブルにします。

```
hostname(config)# isakmp am-disable
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
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。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
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。

isakmp disconnect-notify

ピアに対する切断通知をイネーブルにするには、グローバル コンフィギュレーション モードで **isakmp disconnect-notify** コマンドを使用します。切断通知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。

isakmp disconnect-notify

no isakmp disconnect-notify

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

デフォルト値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
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、グローバル コンフィギュレーション モードで、ピアに対する切断通知をイネーブルにします。

```
hostname(config)# isakmp disconnect-notify
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
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。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
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。

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で ISAKMP ネゴシエーションをイネーブルにするには、グローバル コンフィギュレーション モードで **isakmp enable** コマンドを使用します。インターフェイス上で ISAKMP 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。

isakmp enable *interface-name*

no isakmp enable *interface-name*

シンタックスの説明

interface-name	ISAKMP ネゴシエーションをイネーブルまたはディセーブルにするインターフェイス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。

例

次の例は、グローバル コンフィギュレーション モードで、内部インターフェイス上で ISAKMP をディセーブルにする方法を示しています。

```
hostname(config)# no isakmp enable inside
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
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。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
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。

isakmp identity

フェーズ 2 ID をピアに送信するように設定するには、グローバル コンフィギュレーション モードで **isakmp identity** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

isakmp identity {address | hostname | key-id *key-id-string* | **auto}**

no isakmp identity {address | hostname | key-id *key-id-string* | **auto}**

シンタックスの説明

address	ISAKMP の識別情報を交換するホストの IP アドレスを使用します。
auto	ISKMP ネゴシエーションを、接続タイプよって判別します（事前共有キーの IP アドレス、または証明書認証用の証明書 DN）。
hostname	ISAKMP の識別情報を交換するホストの完全修飾ドメイン名を使用します（デフォルト）。この名前は、ホスト名とドメイン名で構成されます。
key-id *key_id_string*	リモート ピアが事前共有キーを検索するために使用する文字列を指定します。

デフォルト

デフォルトの ISAKMP ID は、**isakmp identity hostname** 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

次の例では、グローバル コンフィギュレーション モードで、IPSec ピアと通信するためのインターフェイス上で ISAKMP ネゴシエーションを、接続タイプに応じてイネーブルにします。

```
hostname(config)# isakmp identity auto
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
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。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
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。

isakmp ipsec-over-tcp

IPSec over TCP をイネーブルにするには、グローバル コンフィギュレーション モードで **isakmp ipsec-over-tcp** コマンドを使用します。IPSec over TCP 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。

isakmp ipsec-over-tcp [**port** *port1...port10*]

no isakmp ipsec-over-tcp [**port** *port1...port10*]

シンタックスの説明

port *port1...port10*	（オプション）デバイスが IPSec over TCP 接続を受け入れるポートを指定します。最大 10 のポートを指定できます。ポート番号の範囲は 1 ～ 65535 です。デフォルトのポート番号は 10000 です。

デフォルト

デフォルト値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
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、グローバル コンフィギュレーション モードで、ポート 45 上で IPSec over TCP をイネーブルにします。

```
hostname(config)# isakmp ipsec-over-tcp port 45
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
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。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
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。

isakmp keepalive

IKE DPD を設定するには、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 **isakmp keepalive** コマンドを使用します。デフォルトでは、すべてのトンネルグループで IKE キープアライブが、デフォルトのしきい値およびリトライ値を使用してイネーブルになっています。キープアライブ パラメータを、デフォルトのしきい値およびリトライ値を使用してイネーブルにした状態に戻すには、このコマンドの ***no*** 形式を使用します。

isakmp keepalive [***threshold*** *seconds*] [***retry*** *seconds*] [**disable**]

no isakmp keepalive disable

シンタックスの説明

disable	IKE キープアライブ処理をディセーブルにします。デフォルトではイネーブルになっています。
retry *seconds*	キープアライブ応答が受信されなくなった後のリトライ間の間隔を秒単位で指定します。範囲は 2 ～ 10 秒です。デフォルトは、2 秒です。
threshold *seconds*	キープアライブのモニタリングを開始するまでピアがアイドル状態を維持できる秒数を指定します。範囲は 10 ～ 3,600 秒です。LAN-to-LAN グループのデフォルトは 10 秒で、リモートアクセス グループのデフォルトは 300 秒です。

デフォルト

リモートアクセス グループのデフォルトは、しきい値が 300 秒で、リトライが 2 秒です。

LAN-to-LAN グループのデフォルトは、しきい値が 10 秒で、リトライが 2 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
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 リモートアクセスおよび IPSec LAN-to-LAN トンネルグループ タイプだけに適用できます。

例

次の例では、config-ipsec コンフィギュレーション モードで、209.165.200.225 という IPSec LAN-to-LAN トンネルグループに対して、IKE DPD を設定し、しきい値を 15 に設定し、リトライ間隔を 10 に指定します。

```
hostname(config)# tunnel-group 209.165.200.225 type IPSec_L2L
hostname(config)# tunnel-group 209.165.200.225 ipsec-attributes
hostname(config-ipsec)# isakmp keepalive threshold 15 retry 10
```

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	すべてのトンネルグループまたは特定のトンネルグループのトンネルグループ コンフィギュレーションを表示します。
tunnel-group-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。

isakmp nat-traversal

NAT Traversal をグローバルにイネーブルにするには、グローバル コンフィギュレーション モードで ISAKMP をイネーブルにしたことを確認し（イネーブルにするには **isakmp enable** コマンドを使用します）、次に **isakmp nat-traversal** コマンドを使用します。NAT Traversal がイネーブルのときに、これ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。

isakmp nat-traversal *natkeepalive*

no isakmp nat-traversal *natkeepalive*

シンタックスの説明

natkeepalive	NAT キープアライブ間隔を 10 ～ 3,600 秒の範囲で設定します。デフォルトは、20 秒です。

デフォルト

デフォルトで、NAT Traversal（**isakmp nat-traversal**）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
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

NAT は、PAT も含め、IPSec も使用している多くのネットワークで使用されていますが、IPSec パケットが NAT デバイスを問題なく通過することを妨げる非互換性が数多くあります。
NAT Traversal を使用すると、ESP パケットが 1 つまたは複数の NAT デバイスを通過できるようになります。

セキュリティ アプライアンスは、IETF の「UDP Encapsulation of IPsec Packets」ドラフトのバージョン 2 とバージョン 3（http://www.ietf.org/html.charters/ipsec-charter.html から入手可能）に記述されているとおり NAT Traversal をサポートしています。NAT Traversal は、ダイナミックとスタティックの両方の暗号マップについてサポートされています。

このコマンドは、セキュリティ アプライアンス上で NAT-T をグローバルにイネーブルにします。暗号マップ エントリでディセーブルにするには、**crypto map set nat-t-disable** コマンドを使用します。

例

次の例では、グローバル コンフィギュレーション モードで、ISAKMP をイネーブルにし、30 秒間隔で NAT Traversal をイネーブルにします。

```
hostname(config)# isakmp enable
hostname(config)# isakmp nat-traversal 30
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
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。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
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。

isakmp policy authentication

IKE ポリシー内の認証方式を指定するには、グローバル コンフィギュレーション モードで **isakmp policy authentication** コマンドを使用します。IKE ポリシーは、IKE ネゴシエーション用のパラメータのセットを定義したものです。認証方式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。

isakmp policy *priority* **authentication** {**pre-share | dsa-sig | rsa-sig**}

no isakmp policy *priority* **authentication**

シンタックスの説明

dsa-sig	認証方式として、DSA シグニチャを指定します。
pre-share	認証方式として、事前共有キーを指定します。
priority	IKE ポリシーを一意に識別し、そのポリシーに優先順位を割り当てます。1 ～ 65534 の整数を使用します。1 は優先順位が最も高く、65534 が最も低くなります。
rsa-sig	認証方式として、RSA シグニチャを指定します。 RSA シグニチャは、IKE ネゴシエーションに対する否認防止ができます。これは、基本的にユーザがピアとの IKE ネゴシエーションを行ったかどうかを、第三者に証明できることを意味します。

デフォルト

デフォルトの ISAKMP ポリシー認証は、**pre-share** 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。DSA-Sig が 7.0 で追加されました。

使用上のガイドライン

RSA シグニチャを指定する場合は、認証局（CA）から証明書を取得するようにセキュリティ アプライアンスとそのピアを設定する必要があります。事前共有キーを指定する場合は、セキュリティ アプライアンスとそのピアに、事前共有キーを別々に設定する必要があります。

例

次の例は、グローバル コンフィギュレーション モードで、**isakmp policy authentication** コマンドを使用する方法を示しています。この例では、優先順位番号 40 の IKE ポリシーに RSA シグニチャの認証方式を使用するように設定します。

```
hostname(config)# isakmp policy 40 authentication rsa-sig
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
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。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
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。

isakmp policy encryption

IKE ポリシー内の暗号化アルゴリズムを指定するには、グローバル コンフィギュレーション モードで **isakmp policy encryption** コマンドを使用します。暗号化アルゴリズムをデフォルト値の **des** 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。

isakmp policy *priority* **encryption** {**aes | aes-192| aes-256 | des | 3des**}

no isakmp policy *priority* **encryption** {**aes | aes-192| aes-256 | des | 3des**}

シンタックスの説明

3des	IKE ポリシーで、Triple DES 暗号化アルゴリズムを使用することを指定します。
aes	IKE ポリシーで使用する暗号化アルゴリズムが、128 ビット キーを使用する AES であることを指定します。
aes-192	IKE ポリシーで使用する暗号化アルゴリズムが、192 ビット キーを使用する AES であることを指定します。
aes-256	IKE ポリシーで使用する暗号化アルゴリズムが、256 ビット キーを使用する AES であることを指定します。
des	IKE ポリシーで使用する暗号化アルゴリズムが、56 ビット DES-CBC であることを指定します。
priority	Internet Key Exchange（IKE）ポリシーを一意に識別し、そのポリシーに優先順位を割り当てます。1 ～ 65534 の整数を使用します。1 は優先順位が最も高く、65534 が最も低くなります。

デフォルト

デフォルトの ISAKMP ポリシー暗号化は **3des** 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

次の例は、グローバル コンフィギュレーション モードで、**isakmp policy encryption** コマンドを使用する方法を示しています。この例では、優先順位番号 25 の IKE ポリシーに 128 ビット キーの AES 暗号化アルゴリズムを使用するように設定します。

```
hostname(config)# isakmp policy 25 encryption aes
```

次の例では、グローバル コンフィギュレーション モードで、優先順位番号 40 の IKE ポリシーに 3DES アルゴリズムを使用するように設定します。

```
hostname(config)# isakmp policy 40 encryption 3des
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
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。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
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。

isakmp policy group

IKE ポリシーの Diffie-Hellman グループを指定するには、グローバル コンフィギュレーション モードで **isakmp policy group** コマンドを使用します。IKE ポリシーは、IKE ネゴシエーション時に使用するパラメータのセットを定義したものです。Diffie-Hellman グループ識別子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。

isakmp policy *priority* **group** {**1 | 2 | 5 | 7**}

no isakmp policy *priority* **group**

シンタックスの説明

group 1	IKE ポリシーで、768 ビットの Diffie-Hellman グループ 1 を使用することを指定します。768 ビットは、デフォルト値です。
group 2	IKE ポリシーで、1,024 ビットの Diffie-Hellman グループ 2 を使用することを指定します。
group 5	IKE ポリシーで、1,536 ビットの Diffie-Hellman グループ 5 を使用することを指定します。
group 7	IKE ポリシーで、Diffie-Hellman Group 7 を使用することを指定します。Group 7 は IPSec SA キーを生成します。楕円曲線フィールドのサイズは 163 ビットです。
priority	Internet Key Exchange（IKE）ポリシーを一意に識別し、そのポリシーに優先順位を割り当てます。1 ～ 65534 の整数を使用します。1 は優先順位が最も高く、65534 が最も低くなります。

デフォルト

デフォルトのグループポリシーは、group 2 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。Group 7 が追加されました。

使用上のガイドライン

グループ オプションには、768 ビット（DH Group 1）、1,024 ビット（DH Group 2）、1,536 ビット（DH Group 5）、および DH Group 7 の 4 つがあります。1,024 ビットと 1,536 ビットの Diffie-Hellman グループは、セキュリティが高くなりますが、CPU の処理時間は長くなります。

（注）　Cisco VPN Client Version 3.x 以降では、**isakmp policy** で DH **group 2** を設定する必要があります（DH **group 1** を設定した場合、Cisco VPN Client は接続できません）。

AES は、VPN-3DES のライセンスがあるセキュリティ アプライアンスに限りサポートされます。AES が提供するキーはサイズが大きいため、ISAKMP ネゴシエーションには、**group 1** や **group 2** ではなく、Diffie-Hellman（DH）**group 5** を使用する必要があります。この設定には、**isakmp policy priority group 5** コマンドを使用します。

例

次の例は、グローバル コンフィギュレーション モードで、**isakmp policy group** コマンドを使用する方法を示しています。この例では、優先順位番号 40 の IKE ポリシーに、グループ 2、1024 ビット Diffie Hellman を使用するように設定します。

```
hostname(config)# isakmp policy 40 group 2
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
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。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
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。

isakmp policy hash

IKE ポリシーのハッシュ アルゴリズムを指定するには、グローバル コンフィギュレーション モードで **isakmp policy hash** コマンドを使用します。IKE ポリシーは、IKE ネゴシエーション時に使用するパラメータのセットを定義したものです。

ハッシュ アルゴリズムをデフォルト値の SHA-1 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。

isakmp policy *priority* **hash** {**md5 | sha**}

no isakmp policy *priority* **hash**

シンタックスの説明

md5	IKE ポリシーで使用するハッシュ アルゴリズムとして、MD5（HMAC バリアント）を指定します。
priority	Internet Key Exchange（IKE）ポリシーを一意に識別し、そのポリシーに優先順位を割り当てます。1 ～ 65534 の整数を使用します。1 は優先順位が最も高く、65534 が最も低くなります。
sha	IKE ポリシーで使用するハッシュ アルゴリズムとして、SHA-1（HMAC バリアント）を指定します。

デフォルト

デフォルトのハッシュ アルゴリズムは SHA-1（HMAC バリアント）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
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

ハッシュ アルゴリズムのオプションには、SHA-1 と MD5 の 2 つがあります。MD5 は、SHA-1 よりもダイジェストが小さく、わずかに速いとされています。

例

次の例は、グローバル コンフィギュレーション モードで、**isakmp policy hash** コマンドを使用する方法を示しています。この例では、優先順位番号 40 の IKE ポリシーに MD5 ハッシュ アルゴリズムを使用することを指定します。

```
hostname(config)# isakmp policy 40 hash md5
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
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。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
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。

isakmp policy lifetime

IKE セキュリティ アソシエーションの期限が満了するまでのライフタイムを指定するには、グローバル コンフィギュレーション モードで **isakmp policy lifetime** コマンドを使用します。ピアがライフタイムを提示していなければ、無限のライフタイムを指定できます。セキュリティ アソシエーションのライフタイムをデフォルト値の 86,400 秒（1 日）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。

isakmp policy *priority* **lifetime** *seconds*

no isakmp policy *priority* **lifetime**

シンタックスの説明

priority	Internet Key Exchange（IKE）ポリシーを一意に識別し、そのポリシーに優先順位を割り当てます。1 ～ 65534 の整数を使用します。1 は優先順位が最も高く、65534 が最も低くなります。
seconds	各セキュリティ アソシエーションが期限満了するまでの秒数を指定します。有限のライフタイムを提示するには、120 ～ 2,147,483,647 秒の整数を使用します。無限のライフタイムを提示するには、0 秒を使用します。

デフォルト

デフォルト値は 86,400 秒（1 日）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

IKE は、ネゴシエーションを開始するとき、自身のセッション用のセキュリティ パラメータを合意しようとします。次に、各ピアのセキュリティ アソシエーションが、合意されたパラメータを参照します。ピアは、ライフタイムが期限満了するまで、セキュリティ アソシエーションを保持します。セキュリティ アソシエーションは、期限満了するまでその後の IKE ネゴシエーションで利用できるため、新しい IPSec セキュリティ アソシエーションを設定するときに時間を節約できます。ピアは、現在のセキュリティ アソシエーションが期限満了する前に、新しいセキュリティ アソシエーションをネゴシエートします。

ライフタイムを長くするほど、セキュリティ アプライアンスで以降の IPSec セキュリティ アソシエーションを設定する時間が節約されます。暗号化強度は十分なレベルにあるため、キーの再生成間隔を極端に短く（約 2 ～ 3 分ごとに）しなくてもセキュリティは保証されます。デフォルトをそのまま使用することをお勧めします。

（注） IKE セキュリティ アソシエーションが無限のライフタイムに設定されている場合、ピアが有限のライフタイムを提示したときは、ピアからのネゴシエートされた有限のライフタイムが使用されます。
次の例は、グローバル コンフィギュレーション モードで、**isakmp policy lifetime** コマンドを使用する方法を示しています。この例では、優先順位番号 40 の IKE ポリシー内に IKE セキュリティ アソシエーションのライフタイムを 50,400 秒（14 時間）に設定します。

例

この例では、グローバル コンフィギュレーション モードで、優先順位番号 40 の IKE ポリシー内に IKE セキュリティ アソシエーションのライフタイムを 50,400 秒（14 時間）に設定します。

```
hostname(config)# isakmp policy 40 lifetime 50400
```

次の例では、グローバル コンフィギュレーション モードで、IKE セキュリティ アソシエーションを無限のライフタイムに設定します。

```
hostname(config)# isakmp policy 40 lifetime 0
```

関連コマンド

clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
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。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
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。

isakmp reload-wait

すべてのアクティブなセッションが自主的に終了するまで待機してからセキュリティ アプライアンスをリブートできるようにするには、グローバル コンフィギュレーション モードで **isakmp reload-wait** コマンドを使用します。アクティブなセッションが終了するまで待機しないでセキュリティ アプライアンスのリブートを続行するには、このコマンドの **no** 形式を使用します。

isakmp reload-wait

no isakmp reload-wait

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、グローバル コンフィギュレーション モードで、すべてのアクティブなセッションが終了するまで待機してからリブートするように、セキュリティ アプライアンスに通知します。

```
hostname(config)# isakmp reload-wait
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
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。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
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。

issuer-name

規則エントリ文字列との比較対象となる CA 証明書の DN を指定するには、CA 証明書マップ コンフィギュレーション モードで **issuer-name** コマンドを使用します。発行者名を削除するには、コマンドの **no** 形式を使用します。

issuer-name [**attr** *tag*] {**eq** | **ne** | **co** | **nc**} *string*

no issuer-name [**attr** *tag*] {**eq** | **ne** | **co** | **nc**} *string*

シンタックスの説明

attr tag	証明書の DN 文字列で、指定されているアトリビュート値だけが規則エントリ文字列と比較されることを示します。タグの値を次に示します。 DNQ = DN 修飾子 GENQ = 世代修飾子 I = イニシャル GN = 名 N = 名前 SN = 姓 IP = IP アドレス SER = シリアル番号 UNAME = 非構造化名 EA = 電子メール アドレス T = 役職 O = 組織名 L = 地名 SP = 州または都道府県 C = 国または地域 OU = 組織ユニット CN = 通常名
co	DN 文字列または指定されているアトリビュートが、規則エントリ文字列の部分文字列と一致する必要があることを指定します。
eq	DN 文字列または指定されているアトリビュートが、規則の文字列全体と一致する必要があることを指定します。
nc	DN 文字列または指定されているアトリビュートが、規則エントリ文字列の部分文字列と一致しない必要があることを指定します。
ne	DN 文字列または指定されているアトリビュートが、規則の文字列全体と一致しない必要があることを指定します。
string	規則エントリ情報を指定します。

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
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、証明書マップ 4 の CA 証明書マップ モードに入り、発行者名を O = central として設定します。

```
hostname(config)# crypto ca certificate map 4
hostname(ca-certificate-map)# issuer-name attr o eq central
hostname(ca-certificate-map)# exit
```

関連コマンド

コマンド	説明
crypto ca certificate map	CA 証明書マップ モードに入ります。
subject-name（crypto ca certificate map）	規則エントリ文字列との比較対象となる、CA 証明書に含まれている DN を指定します。

join-failover-group

コンテキストをフェールオーバー グループに割り当てるには、コンテキスト コンフィギュレーション モードで **join-failover-group** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

join-failover-group *group_num*

no join-failover-group *group_num*

シンタックスの説明

group_num	フェールオーバー グループの番号を指定します。

デフォルト

フェールオーバー グループ 1。

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

管理コンテキストは、常にフェールオーバー グループ 1 に割り当てられます。フェールオーバー グループとコンテキストの関連付けを表示するには、**show context detail** コマンドを使用します。

コンテキストをフェールオーバー グループに割り当てる前に、**failover group** コマンドを使用して、フェールオーバー グループをシステム コンテキスト内に作成する必要があります。このコマンドは、コンテキストがアクティブな状態になっている装置上で入力します。デフォルトでは、未割り当てのコンテキストは、フェールオーバー グループ 1 のメンバーになっています。そのため、コンテキストがまだフェールオーバー グループに割り当てられていない場合は、フェールオーバー グループ 1 がアクティブ状態になっている装置上で、このコマンドを入力する必要があります。

システムからフェールオーバー グループを削除するには、事前に **no join-failover-group** コマンドを使用して、フェールオーバー グループからコンテキストをすべて削除しておく必要があります。

例

次の例では、ctx1 というコンテキストをフェールオーバー グループ 2 に割り当てます。

```
hostname(config)# context ctx1
hostname(config-context)# join-failover-group 2
hostname(config-context)# exit
```

関連コマンド

コマンド	説明
context	指定したコンテキストのコンテキスト コンフィギュレーション モードに入ります。
failover group	Active/Active フェールオーバーのためのフェールオーバー グループを定義します。
show context detail	コンテキストの詳細情報（名前、クラス、インターフェイス、フェールオーバー グループの関連付け、およびコンフィギュレーション ファイルの URL など）を表示します。

kerberos-realm

この Kerberos サーバのレルム名を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **kerberos-realm** コマンドを使用します。レルム名を削除するには、このコマンドの **no** 形式を使用します。

kerberos-realm *string*

no kerberos-realm

シンタックスの説明

string	大文字と小文字が区別される最大 64 文字の英数字の文字列。文字列にスペースは使用できません。

（注） Kerberos レルム名に使用できるのは、数字と大文字のアルファベットのみです。セキュリティ アプライアンスでは、*string* 引数に小文字のアルファベットを使用できますが、小文字は大文字に変換されません。必ず大文字のアルファベットだけを使用してください。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
AAA サーバ ホスト 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)	このリリースで導入されました。

使用上のガイドライン

このコマンドは、Kerberos サーバに対してのみ有効です。

Microsoft Windows の **set USERDNSDOMAIN** コマンドを Kerberos レルムの Windows 2000 Active Directory サーバ上で実行する場合は、*string* 引数の値をこのコマンドの出力と一致させる必要があります。次の例では、EXAMPLE.COM が Kerberos レルム名です。

```
C:\>set USERDNSDOMAIN
USERDNSDOMAIN=EXAMPLE.COM
```

string 引数には、数字と大文字のアルファベットのみを使用する必要があります。**kerberos-realm** コマンドでは、大文字と小文字が区別されます。また、セキュリティ アプライアンスでは、小文字は大文字に変換されません。

例

次のシーケンスは、AAA サーバ ホストの設定に関するコンテキストで Kerberos レルムを「EXAMPLE.COM」に設定するための **kerberos-realm** コマンドを示しています。

```
hostname(config)# aaa-server svrgrp1 protocol kerberos
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# kerberos-realm EXAMPLE.COM
hostname(config-aaa-server-host)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション サブモードに入って、ホスト固有の AAA サーバ パラメータを設定できるようにします。
clear configure aaa-server	すべての AAA コマンド文をコンフィギュレーションから削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

key

AAA サーバに対して NAS を認証するために使用されるサーバ シークレットの値を指定するには、AAA サーバ ホスト モードで **key** コマンドを使用します。AAA サーバ ホスト コンフィギュレーション モードには、AAA サーバ プロトコル コンフィギュレーション モードからアクセスできます。キーを削除するには、このコマンドの **no** 形式を使用します。キー（サーバ シークレット）の値によって、セキュリティ アプライアンスが AAA サーバに対して認証されます。

key *key*

no key

シンタックスの説明

key	最大 127 文字の英数字キーワード。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
AAA サーバ ホスト	•	•	•	•	—

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

key の値は、127 文字までの英数字で構成されているキーワードで、TACACS+ サーバ上のキーと同じ値にします。アルファベットの大文字と小文字は区別されます。128 文字以降に入力された文字は、すべて無視されます。このキーは、クライアントとサーバの間でやり取りするデータを暗号化するために使用されます。キーは、クライアント システムとサーバ システムの両方で同一である必要があります。キーにスペースは使用できませんが、その他の特殊文字は使用できます。

このコマンドは、RADIUS サーバと TACACS+ サーバに対してのみ有効です。

以前の PIX Firewall のバージョンで使用されていた **aaa-server** コマンドの **key** パラメータは、対応する **key** コマンドに自動的に変換されます。

例

次の例では、ホスト「1.2.3.4」上で「srvgrp1」という TACACS+ AAA サーバを設定し、タイムアウトを 9 秒に設定し、リトライ間隔を 7 秒に設定し、キーを「myexclusivemumblekey」として設定します。

```
hostname(config)# aaa-server svrgrp1 protocol tacacs+
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# key myexclusivemumblekey
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードに入って、ホスト固有の AAA サーバ パラメータを設定できるようにします。
clear configure aaa-server	すべての AAA コマンド文をコンフィギュレーションから削除します。
show running-config aaa-server	AAA サーバのコンフィギュレーションを表示します。

keypair

証明する公開キーのキー ペアを指定するには、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 **keypair** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

keypair *name*

no keypair

シンタックスの説明

name	キー ペアの名前を指定します。

デフォルト

デフォルト設定では、キー ペアは含まれません。

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
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、central トラストポイントの暗号 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、central トラストポイント用に証明するキー ペアを指定します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# keypair exchange
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。
crypto key generate dsa	DSA キーを生成します。
crypto key generate rsa	RSA キーを生成します。
default enrollment	登録パラメータをデフォルトに戻します。

kill

Telnet セッションを終了するには、特権 EXEC モードで **kill** コマンドを使用します。

kill *telnet_id*

シンタックスの説明

telnet_id	Telnet セッションの ID を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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

kill コマンドを使用すると、Telnet セッションを終了できます。Telnet セッションの ID を表示するには、**who** コマンドを使用します。Telnet セッションを終了すると、セキュリティ アプライアンスは、警告することなく、すべてのアクティブなコマンドを終了して接続をドロップします。

例

次の例は、ID「2」の Telnet セッションを終了する方法を示しています。最初に、アクティブな Telnet セッションのリストを表示するため、**who** コマンドを入力します。次に、ID「2」の Telnet セッションを終了するため、**kill 2** コマンドを入力します。

```
hostname# who
2: From 10.10.54.0

hostname# kill 2
```

関連コマンド

コマンド	説明
telnet	セキュリティ アプライアンスへの Telnet アクセスを設定します。
who	アクティブな Telnet セッションのリストを表示します。

ldap-base-dn

認可要求を受信したときに、サーバが検索を開始する LDAP 階層内の位置を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **ldap-base-dn** コマンドを使用します。AAA サーバ ホスト コンフィギュレーション モードには、AAA サーバ プロトコル コンフィギュレーション モードからアクセスできます。この指定を削除して、検索の開始位置をリストの先頭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。

ldap-base-dn *string*

no ldap-base-dn

シンタックスの説明

string	認可要求を受信したときに、サーバが検索を開始する LDAP 階層内の位置を指定する最大 128 文字の文字列で、大文字と小文字が区別されます（たとえば、OU=Cisco）。文字列にスペースは使用できませんが、その他の特殊文字は使用できます。

デフォルト

検索はリストの先頭から開始されます。

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
AAA サーバ ホスト	•	•	•	•	—

コマンド履歴

リリース	変更
7.0(1)	既存のコマンドです。このリリースで修正されました。

使用上のガイドライン

このコマンドは、LDAP サーバに対してのみ有効です。

例

次の例では、ホスト「1.2.3.4」上で「srvgrp1」という LDAP AAA サーバを設定し、タイムアウトを 9 秒に設定し、リトライ間隔を 7 秒に設定し、LDAP ベース DN を「starthere」として設定します。

```
hostname(config)# aaa-server svrgrp1 protocol ldap
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# ldap-base-dn starthere
hostname(config-aaa-server-host)# exit
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードに入って、ホスト固有の AAA サーバ パラメータを設定できるようにします。
ldap-scope	認可要求を受信したときに、サーバが実行する LDAP 階層内検索の範囲を指定します。
ldap-naming-attribute	LDAP サーバ上のエントリを一意に識別するための、相対認定者名アトリビュート（複数可）を指定します。
ldap-login-dn	ディレクトリ オブジェクトの名前を指定します。システムは、オブジェクトをこの名前でバインドします。
ldap-login-password	ログイン DN のパスワードを指定します。

ldap-defaults

LDAP のデフォルト値を定義するには、crl 設定コンフィギュレーション モードで **ldap-defaults** コマンドを使用します。crl 設定コンフィギュレーション モードには、暗号 CA トラストポイント コンフィギュレーション モードからアクセスできます。これらのデフォルト値は、LDAP サーバが必要とする場合にだけ使用されます。LDAP デフォルトを指定しない場合は、このコマンドの **no** 形式を使用します。

ldap-defaults *server* [*port*]

no ldap-defaults

シンタックスの説明

port	（オプション）LDAP サーバ ポートを指定します。このパラメータが指定されていない場合、セキュリティ アプライアンスは標準の LDAP ポート（389）を使用します。
server	LDAP サーバの IP アドレスまたはドメイン名を指定します。CRL 配布ポイント内にサーバが存在する場合、この値はそのサーバによって上書きされます。

デフォルト

デフォルト値は設定されていません。

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
crl 設定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、デフォルト ポート（389）上で LDAP デフォルト値を定義します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# ldap-defaults ldapdomain4 8389
```

関連コマンド

コマンド	説明
crl configure	ca-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。
protocol ldap	LDAP を CRL 取得方法として指定します。

ldap-dn

CRL の取得時に認証を要求する LDAP サーバに X.500 認定者名とパスワードを渡すには、crl 設定コンフィギュレーション モードで **ldap-dn** コマンドを使用します。crl 設定コンフィギュレーション モードには、暗号 CA トラストポイント コンフィギュレーション モードからアクセスできます。これらのパラメータは、LDAP サーバが必要とする場合にだけ使用されます。

LDAP DN を指定しない場合は、このコマンドの **no** 形式を使用します。

ldap-dn *x.500-name password*

no ldap-dn

シンタックスの説明

password	この認定者名のパスワードを定義します。フィールドの最大長は 128 文字です。
x.500-name	この CRL データベースにアクセスするためのディレクトリ パスを定義します（たとえば、cn=crl,ou=certs,o=CAName,c=US）。フィールドの最大長は 128 文字です。

デフォルト

デフォルト値は設定されていません。

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
crl 設定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、X.500 の名前に CN=admin,OU=devtest,O=engineering を指定し、central トラストポイントのパスワードに xxzzyy を指定します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# ldap-dn cn=admin,ou=devtest,o=engineering xxzzyy
```

関連コマンド

コマンド	説明
crl configure	crl 設定コンフィギュレーション モードに入ります。
crypto ca trustpoint	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。
protocol ldap	CRL の取得方法として LDAP を指定します。

ldap-login-dn

システムがバインドするディレクトリ オブジェクトの名前を指定するには、AAA サーバ ホスト モードで **ldap-login-dn** コマンドを使用します。AAA サーバ ホスト コンフィギュレーション モードには、AAA サーバ プロトコル コンフィギュレーション モードからアクセスできます。この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。

ldap-login-dn *string*

no ldap-login-dn

シンタックスの説明

string	LDAP 階層内のディレクトリ オブジェクトの名前を指定する最大 128 文字の文字列で、大文字と小文字が区別されます。文字列にスペースは使用できませんが、その他の特殊文字は使用できます。

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
AAA サーバ ホスト	•	•	•	•	—

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、LDAP サーバに対してのみ有効です。サポートされる文字列の最大長は 128 文字です。

Microsoft Active Directory サーバなどの LDAP サーバでは、他のすべての LDAP 動作に関する要求を受け入れる前に、セキュリティ アプライアンスが認証済みバインディングを介してハンドシェイクを確立することを要求します。セキュリティ アプライアンスは、認証済みバインディングに対して識別情報を示すときに、ユーザ認証要求に Login DN フィールドを付加します。Login DN フィールドは、セキュリティ アプライアンスの認証特性を説明します。この特性は、管理者特権を持つユーザの特性に対応している必要があります。

string 変数には、VPN コンセントレータの認証済みバインディングに関するディレクトリ オブジェクトの名前を入力します（たとえば、cn=Administrator、cn=users、ou=people、dc=XYZ Corporation、dc=com）。匿名アクセスの場合、このフィールドはブランクのままにします。

例

次の例では、ホスト「1.2.3.4」上で「srvgrp1」という LDAP AAA サーバを設定し、タイムアウトを 9 秒に設定し、リトライ間隔を 7 秒に設定し、LDAP ログイン DN を「myobjectname」として設定します。

```
hostname(config)# aaa-server svrgrp1 protocol ldap
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host))# retry 7
hostname(config-aaa-server-host))# ldap-login-dn myobjectname
hostname(config-aaa-server-host))# exit
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードに入って、ホスト固有の AAA サーバ パラメータを設定できるようにします。
ldap-base-dn	認可要求を受信したときに、サーバが検索を開始する LDAP 階層内の位置を指定します。
ldap-login-password	ログイン DN のパスワードを指定します。このコマンドは、LDAP サーバに対してのみ有効です。
ldap-naming-attribute	LDAP サーバ上のエントリを一意に識別するための、相対認定者名アトリビュート（複数可）を指定します。
ldap-scope	認可要求を受信したときに、サーバが実行する LDAP 階層内検索の範囲を指定します。

ldap-login-password

LDAP サーバのログイン パスワードを指定するには、AAA サーバ ホスト モードで **ldap-login-password** コマンドを使用します。AAA サーバ ホスト コンフィギュレーション モードには、AAA サーバ プロトコル コンフィギュレーション モードからアクセスできます。このパスワード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。

ldap-login-password *string*

no ldap-login-password

シンタックスの説明

string	大文字と小文字が区別される最大 64 文字の英数字のパスワード。パスワードにスペースは使用できません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
AAA サーバ ホスト	•	•	•	•	—

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、LDAP サーバに対してのみ有効です。パスワード文字列の最大長は 64 文字です。

例

次の例では、ホスト「1.2.3.4」上で「srvgrp1」という LDAP AAA サーバを設定し、タイムアウトを 9 秒に設定し、リトライ間隔を 7 秒に設定し、LDAP ログイン パスワードを「obscurepassword」として設定します。

```
hostname(config)# aaa-server svrgrp1 protocol ldap
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)# ldap-login-password obscurepassword
hostname(config-aaa-server)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードに入って、ホスト固有の AAA サーバ パラメータを設定できるようにします。
ldap-base-dn	認可要求を受信したときに、サーバが検索を開始する LDAP 階層内の位置を指定します。
ldap-login-dn	ディレクトリ オブジェクトの名前を指定します。システムは、オブジェクトをこの名前でバインドします。
ldap-naming-attribute	LDAP サーバ上のエントリを一意に識別するための、相対認定者名アトリビュート（複数可）を指定します。
ldap-scope	認可要求を受信したときに、サーバが実行する LDAP 階層内検索の範囲を指定します。

ldap-naming-attribute

相対認定者名アトリビュート（複数可）を指定するには、AAA サーバ ホスト モードで **ldap-naming-attribute** コマンドを使用します。AAA サーバ ホスト コンフィギュレーション モードには、AAA サーバ プロトコル コンフィギュレーション モードからアクセスできます。この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。

ldap-naming-attribute *string*

no ldap-naming-attribute

シンタックスの説明

string	LDAP サーバ上のエントリを一意に識別するための相対認定者名アトリビュート（複数可）で、大文字と小文字が区別される最大 128 文字の英数字です。文字列にスペースは使用できませんが、その他の特殊文字は使用できます。

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
aaa-server host	•	•	•	•	—

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

LDAP サーバ上のエントリを一意に識別するための、相対認定者名アトリビュート（複数可）を入力します。共通の命名アトリビュートは、通常名（cn）とユーザ ID（uid）です。

このコマンドは、LDAP サーバに対してのみ有効です。サポートされる文字列の最大長は 128 文字です。

例

次の例では、ホスト「1.2.3.4」上で「srvgrp1」という LDAP AAA サーバを設定し、タイムアウトを 9 秒に設定し、リトライ間隔を 7 秒に設定し、LDAP 命名アトリビュートを「cn」として設定します。

```
hostname(config)# aaa-server svrgrp1 protocol ldap
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# ldap-naming-attribute cn
hostname(config-aaa-server-host)# exit
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードに入って、ホスト固有の AAA サーバ パラメータを設定できるようにします。
ldap-base-dn	認可要求を受信したときに、サーバが検索を開始する LDAP 階層内の位置を指定します。
ldap-login-dn	ディレクトリ オブジェクトの名前を指定します。システムは、オブジェクトをこの名前でバインドします。
ldap-login-password	ログイン DN のパスワードを指定します。このコマンドは、LDAP サーバに対してのみ有効です。
ldap-scope	認可要求を受信したときに、サーバが実行する LDAP 階層内検索の範囲を指定します。

ldap-scope

認可要求を受信したときに、サーバが検索する LDAP 階層内の範囲を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **ldap-scope** コマンドを使用します。AAA サーバ ホスト コンフィギュレーション モードには、AAA サーバ プロトコル コンフィギュレーション モードからアクセスできます。この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。

ldap-scope *scope*

no ldap-scope

シンタックスの説明

scope	認可要求を受信したときに、サーバが検索する LDAP 階層のレベル番号を指定します。有効値は、次のとおりです。 • ***onelevel*** ：ベース DN の 1 つ下のレベルのみを検索します。 • ***subtree*** ：ベース DN の下にあるすべてのレベルを検索します。

デフォルト

デフォルト値は、***onelevel*** 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
AAA サーバ ホスト	•	•	•	•	—

コマンド履歴

リリース	変更
7.0(1)	既存のコマンドです。このリリースで修正されました。

使用上のガイドライン

スコープを ***onelevel*** として指定すると、検索速度が向上します。これは、ベース DN の 1 つ下のレベルだけが検索されるためです。***subtree*** を指定すると速度が低下します。これは、ベース DN の下にあるすべてのレベルが検索されるためです。

このコマンドは、LDAP サーバに対してのみ有効です。

例

次の例では、ホスト「1.2.3.4」上で「srvgrp1」という LDAP AAA サーバを設定し、タイムアウトを 9 秒に設定し、リトライ間隔を 7 秒に設定し、LDAP スコープがサブツリー レベルを含むように設定します。

```
hostname(config)# aaa-server svrgrp1 protocol ldap
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-serve-host)# ldap-scope subtree
hostname(config-aaa-server-host)# exit
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードに入って、ホスト固有の AAA サーバ パラメータを設定できるようにします。
ldap-base-dn	認可要求を受信したときに、サーバが検索を開始する LDAP 階層内の位置を指定します。
ldap-login-dn	ディレクトリ オブジェクトの名前を指定します。システムは、オブジェクトをこの名前でバインドします。
ldap-login-password	ログイン DN のパスワードを指定します。このコマンドは、LDAP サーバに対してのみ有効です。
ldap-naming-attribute	LDAP サーバ上のエントリを一意に識別するための、相対認定者名アトリビュート（複数可）を指定します。

leap-bypass

LEAP Bypass をイネーブルにするには、グループポリシー コンフィギュレーション モードで **leap-bypass enable** コマンドを使用します。LEAP Bypass をディセーブルにするには、**leap-bypass disable** コマンドを使用します。LEAP Bypass アトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、LEAP Bypass の値を別のグループポリシーから継承できます。

LEAP Bypass をイネーブルにすると、VPN ハードウェア クライアントの背後にあるワイヤレス デバイスからの LEAP パケットが、ユーザ認証の前に VPN トンネルを通過できるようになります。これにより、シスコの無線アクセス ポイント デバイスを使用するワークステーションで LEAP 認証を確立できます。確立後、ワークステーションはユーザごとの認証をもう一度実行します。

leap-bypass {**enable** | **disable**}

no leap-bypass

シンタックスの説明

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

デフォルト

LEAP Bypass 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
グループポリシー 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　対話型のハードウェア クライアント認証がイネーブルになっていると、この機能は正常に動作しません。

詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

（注）　認証されていないトラフィックがトンネルを通過できるようにすると、セキュリティ　リスクが生じる場合があります。

例　次の例は、「FirstGroup」というグループポリシーに LEAP Bypass を設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# leap-bypass enable
```

関連コマンド

コマンド	説明
secure-unit-authentication	VPN ハードウェア クライアントがトンネルを開始するたびに、クライアントにユーザ名とパスワードによる認証を要求します。
user-authentication	VPN ハードウェア クライアントの背後にいるユーザに対して、接続前にセキュリティ アプライアンスに識別情報を示すように要求します。

log-adj-changes

OSPF 隣接ルータがアップ状態またはダウン状態になると syslog メッセージを送信するようにルータを設定するには、ルータ コンフィギュレーション モードで **log-adj-changes** コマンドを使用します。この機能をオフにするには、このコマンドの **no** 形式を使用します。

log-adj-changes [*detail*]

no log-adj-changes [*detail*]

シンタックスの説明

detail	（オプション）隣接ルータがアップ状態またはダウン状態になるときだけでなく、状態が変化するたびに syslog 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

log-adj-changes コマンドは、デフォルトでイネーブルになっており、コマンドの **no** 形式を使用して削除しない限り、実行コンフィギュレーションに表示されます。

例

次の例では、OSPF 隣接ルータがアップ状態またはダウン状態になったときに syslog メッセージを送信しないようにします。

```
hostname(config)# router ospf 5
hostname(config-router)# no log-adj-changes
```

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 ospf	OSPF ルーティング プロセスに関する一般情報を表示します。

login

ローカル ユーザ データベースを使用して特権 EXEC モードに入る場合や、ユーザ名を変更する場合は、ユーザ EXEC モードで **login** コマンドを使用します。

login

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
ユーザ 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

login コマンドを使用すると、ユーザ EXEC モードから特権 EXEC モードに、ローカル データベース内の任意のユーザ名としてログインできます。イネーブル認証をオンにした場合、**login** コマンドは **enable** コマンドと類似したものになります（**aaa authentication console** コマンドを参照）。ただし、イネーブル認証とは異なり、**login** コマンドはローカル ユーザ名データベースのみを使用できます。このコマンドでは、常に認証が要求されます。また、**login** コマンドを使用すると、任意の CLI モードからユーザを変更できます。

ユーザがログイン時に特権 EXEC モード（およびすべてのコマンド）にアクセスできるようにするには、ユーザの特権レベルを 2（デフォルト）～ 15 に設定します。ローカル コマンド認可を設定した場合、ユーザは、その特権レベル以下のレベルに割り当てられているコマンドのみを入力できます。詳細については、**aaa authorization コマンド**を参照してください。

注意　CLI にアクセスできるユーザや特権 EXEC モードに入らせないようにするユーザをローカル データベースに追加する場合は、コマンド認可を設定する必要があります。コマンド認可が設定されていない場合、ユーザは、特権レベルが 2 以上（2 がデフォルト）であれば、各自のパスワードを使用して CLI で特権 EXEC モード（およびすべてのコマンド）にアクセスできます。または、RADIUS または TACACS+ 認証を使用することもできます。あるいは、すべてのローカル ユーザをレベル 1 に設定して、システムのイネーブル パスワードを使用して特権 EXEC モードにアクセスできるユーザを制御することもできます。

例

次の例では、**login** コマンドを入力した後のプロンプトを示します。

```
hostname> login
Username:
```

関連コマンド

コマンド	説明
aaa authorization command	CLI アクセスのコマンド認可をイネーブルにします。
aaa authentication console	コンソール、Telnet、HTTP、SSH、または **enable** コマンド アクセスに対して認証を要求します。
logout	CLI からログアウトします。
username	ユーザをローカル データベースに追加します。

logging asdm

ASDM ログ バッファに syslog メッセージを送信するには、グローバル コンフィギュレーション モードで **logging asdm** コマンドを使用します。ASDM ログ バッファへのロギングをディセーブル にするには、このコマンドの **no** 形式を使用します。

logging asdm [*logging_list* | *level*]

no logging asdm [*logging_list* | *level*]

シンタックスの説明

level	システム ログ メッセージの最大レベルを設定します。たとえば、レベルを 3 に設定すると、セキュリティ アプライアンスはレベル 3、2、1、および 0 のシステム ログ メッセージを生成します。次の数値または名前で指定できます。 • **0** または **emergencies**：システムが使用不能 • **1** または **alerts**：ただちに処置が必要 • **2** または **critical**：クリティカルな状態 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：正常だが、注意が必要な状態 • **6** または **informational**：情報 • **7** または **debugging**:デバッグ メッセージ、ログ FTP コマンド、WWW URL
logging_list	ASDM ログ バッファに送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

デフォルト

ASDM のロギングは、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

ASDM ログ バッファにメッセージが送信される前に、**logging enable** コマンドを使用して、ロギングをイネーブルにしておく必要があります。

ASDM のログ バッファがいっぱいである場合、セキュリティ アプライアンスは最も古いメッセージを削除して、新しいメッセージ用の空き領域をバッファ内に確保します。ASDM のログ バッファに保持される syslog メッセージの数を制御するには、**logging asdm-buffer-size** コマンドを使用します。

ASDM のログ バッファは、**logging buffered** コマンドでイネーブルにするログ バッファとは別のバッファです。

例

次の例は、ロギングをイネーブルにして、ASDM ログ バッファに重大度 0、1、および 2 のメッセージを送信する方法を示しています。また、ASDM ログ バッファのサイズを 200 メッセージに設定する方法も示しています。

```
hostname(config)# logging enable
hostname(config)# logging asdm 2
hostname(config)# logging asdm-buffer-size 200
hostname(config)# show logging
Syslog logging: enabled
    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: level critical, 48 messages logged
```

関連コマンド

コマンド	説明
clear logging asdm	ASDM が保持しているすべてのメッセージの ASDM ログ バッファを消去します。
logging asdm-buffer-size	ASDM ログ バッファに保持される ASDM メッセージの数を指定します。
logging enable	ロギングをイネーブルにします。
logging list	再使用可能なメッセージ選択基準リストを作成します。
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	ロギングのコンフィギュレーションを表示します。

logging asdm-buffer-size

ASDM のログ バッファに保持される syslog メッセージの数を指定するには、グローバル コンフィギュレーション モードで **logging asdm-buffer-size** コマンドを使用します。ASDM ログ バッファをデフォルト サイズの 100 メッセージ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。

logging asdm-buffer-size *num_of_msgs*

no logging asdm-buffer-size *num_of_msgs*

シンタックスの説明

num_of_msgs	セキュリティ アプライアンスが ASDM ログ バッファに保持する syslog メッセージの数を指定します。

デフォルト

デフォルトの ASDM syslog バッファ サイズは 100 メッセージです。

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

ASDM のログ バッファがいっぱいである場合、セキュリティ アプライアンスは最も古いメッセージを削除して、新しいメッセージ用の空き領域をバッファ内に確保します。ASDM ログ バッファへのロギングをイネーブルにするかどうかを制御する場合や、ASDM ログ バッファに保持される syslog メッセージの種類を制御する場合は、**logging asdm** コマンドを使用します。

ASDM のログ バッファは、**logging buffered** コマンドでイネーブルにするログ バッファとは別のバッファです。

例

次の例は、ロギングをイネーブルにして、ASDM ログ バッファに重大度 0、1、および 2 のメッセージを送信する方法を示しています。また、ASDM ログ バッファのサイズを 200 メッセージに設定する方法も示しています。

```
hostname(config)# logging enable
hostname(config)# logging asdm 2
hostname(config)# logging asdm-buffer-size 200
hostname(config)# show logging
Syslog logging: enabled
    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: level critical, 48 messages logged
```

関連コマンド

コマンド	説明
clear logging asdm	ASDM が保持しているすべてのメッセージの ASDM ログ バッファを消去します。
logging asdm	ASDM ログ バッファへのロギングをイネーブルにします。
logging enable	ロギングをイネーブルにします。
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	現在動作しているロギング コンフィギュレーションを表示します。

logging buffered

セキュリティ アプライアンスが syslog メッセージをログ バッファに送信できるようにするには、グローバル コンフィギュレーション モードで **logging buffered** コマンドを使用します。ログ バッファへのロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

logging buffered [*logging_list* | *level*]

no logging buffered [*logging_list* | *level*]

シンタックスの説明

level	システム ログ メッセージの最大レベルを設定します。たとえば、レベルを 3 に設定すると、セキュリティ アプライアンスはレベル 3、2、1、および 0 のシステム ログ メッセージを生成します。次の数値または名前で指定できます。 • **0** または **emergencies**：システムが使用不能 • **1** または **alerts**：ただちに処置が必要 • **2** または **critical**：クリティカルな状態 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：正常だが、注意が必要な状態 • **6** または **informational**：情報 • **7** または **debugging**:デバッグ メッセージ、ログ FTP コマンド、WWW URL
logging_list	ログ バッファに送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

デフォルト

デフォルトは次のとおりです。

- バッファへのロギングはディセーブルです。
- バッファのサイズは 4 KB 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

ログ バッファにメッセージが送信される前に、**logging enable** コマンドを使用してロギングをイネーブルにしておく必要があります。

新しいメッセージは、バッファの最後に追加されます。バッファがいっぱいになると、セキュリティ アプライアンスはバッファを消去してから、メッセージの追加を続行します。ログ バッファがいっぱいである場合、セキュリティ アプライアンスは最も古いメッセージを削除して、新しいメッセージ用の空き領域をバッファ内に確保します。バッファの内容が「ラップ」されるたびにバッファの内容を自動的に保存することができます。これは、最後に保存されてから追加されたすべてのメッセージが新しいメッセージに置き換えられることを意味します。詳細については、**logging flash-bufferwrap** コマンドと **logging ftp-bufferwrap** コマンドを参照してください。

バッファの内容は、いつでもフラッシュ メモリに保存できます。詳細については、**logging savelog** コマンドを参照してください。

バッファに送信された syslog メッセージは、**show logging** コマンドで表示できます。

例

次の例では、レベル 0 およびレベル 1 のイベントに対して、バッファへのロギングを設定します。

```
hostname(config)# logging buffered alerts
hostname(config)#
```

次の例では、最大ロギング レベル 7 の notif-list というリストを作成し、notif-list リストで識別される syslog メッセージに対して、バッファへのロギングを設定します。

```
hostname(config)# logging list notif-list level 7
hostname(config)# logging buffered notif-list
hostname(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	保持しているすべての syslog メッセージのログ バッファを消去します。
logging buffer-size	ログ バッファのサイズを指定します。
logging enable	ロギングをイネーブルにします。
logging flash-bufferwrap	ログ バッファがいっぱいになったときに、ログ バッファをフラッシュ メモリに書き込みます。
logging ftp-bufferwrap	ログ バッファがいっぱいになったときに、ログ バッファを FTP サーバに送信します。
logging list	再使用可能なメッセージ選択基準リストを作成します。
logging savelog	ログ バッファの内容をフラッシュ メモリに保存します。
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	現在動作しているロギング コンフィギュレーションを表示します。

logging buffer-size

ログ バッファのサイズを指定するには、グローバル コンフィギュレーション モードで **logging buffer-size** コマンドを使用します。ログ バッファをデフォルト サイズの 4 KB 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。

logging buffer-size *bytes*

no logging buffer-size *bytes*

シンタックスの説明

bytes	ログ バッファに使用するメモリ量をバイト単位で設定します。たとえば、8,192 を指定した場合、セキュリティ アプライアンスはログ バッファに 8 KB のメモリを使用します。

デフォルト

ログ バッファのメモリ サイズは 4KB 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

セキュリティ アプライアンスが使用しているログ バッファのサイズがデフォルトのバッファ サイズと異なっているかどうかを確認するには、**show running-config logging** コマンドを使用します。**logging buffer-size** コマンドが表示されない場合、セキュリティ アプライアンスが使用するログ バッファのサイズは 4 KB です。

セキュリティ アプライアンスによるバッファの使用方法の詳細については、**logging buffered** コマンドを参照してください。

例

次の例では、ロギングとロギング バッファをイネーブルにし、セキュリティ アプライアンスがログ バッファ用に 16 KB のメモリを使用するように指定します。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging buffer-size 16384
hostname(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	保持しているすべての syslog メッセージのログ バッファを消去します。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging enable	ロギングをイネーブルにします。
logging flash-bufferwrap	ログ バッファがいっぱいになったときに、ログ バッファをフラッシュ メモリに書き込みます。
logging savelog	ログ バッファの内容をフラッシュ メモリに保存します。
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	現在動作しているロギング コンフィギュレーションを表示します。

logging class

メッセージ クラスに対して、ロギング先ごとの最大ロギング レベルを設定するには、グローバル コンフィギュレーション モードで **logging class** コマンドを使用します。メッセージ クラスのロギング レベル 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。

logging class *class destination level* [*destination level . . .*]

no logging class ***class***

シンタックスの説明

class	設定するロギング先ごとの最大ロギング レベルの対象となるメッセージ クラスを指定します。クラスの有効値については、後述する「使用上のガイドライン」の項を参照してください。
destination	*class* に対してロギング先を指定します。このロギング先についての、*destination* に送信される最大ロギング レベルは、*level* によって決まります。*destination* の有効値については、後述する「使用上のガイドライン」の項を参照してください。
level	システム ログ メッセージの最大レベルを設定します。たとえば、レベルを 3 に設定すると、セキュリティ アプライアンスはレベル 3、2、1、および 0 のシステム ログ メッセージを生成します。次の数値または名前で指定できます。 • **0** または **emergencies**：システムが使用不能 • **1** または **alerts**：ただちに処置が必要 • **2** または **critical**：クリティカルな状態 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：正常だが、注意が必要な状態 • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、WWW URL

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、ロギング先およびメッセージ クラスごとにロギング レベルを適用しないようになっています。代わりに、イネーブルになっている各ロギング先は、ロギング リストで指定されたロギング レベル、またはロギング先をイネーブルにするときに指定されたレベルで、すべてのクラスに対するメッセージを受信します。

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　*class* の有効値は、次のとおりです。

- **auth**：ユーザ認証
- **bridge**：透過ファイアウォール
- **ca**：PKI 認証局
- **config**：コマンド インターフェイス
- **email**：電子メール プロキシ
- **ha**：フェールオーバー
- **ids**：侵入検知システム
- **ip**：IP スタック
- **np**：ネットワーク プロセッサ
- **ospf**：OSPF ルーティング
- **rip**：RIP ルーティング
- **session**：ユーザ セッション
- **snmp**：SNMP
- **sys**：システム
- **vpn**：IKE および IPSec
- **vpnc**：VPN クライアント
- **vpnfo**：VPN フェールオーバー
- **vpnlb**：VPN ロードバランシング

有効なロギング先は、次のとおりです。

- **asdm**：このロギング先については、**logging asdm** コマンドを参照してください。
- **buffered**：このロギング先については、**logging buffered** コマンドを参照してください。
- **console**：このロギング先については、**logging console** コマンドを参照してください。
- **history**：このロギング先については、**logging history** コマンドを参照してください。
- **mail**：このロギング先については、**logging mail** コマンドを参照してください。
- **monitor**：このロギング先については、**logging monitor** コマンドを参照してください。
- **trap**：このロギング先については、**logging trap** コマンドを参照してください。

例

次の例では、フェールオーバー関連のメッセージに対して、ASDM ログ バッファの最大ロギング レベルが 2 で、システム ログ バッファの最大ロギング レベルが 7 であることを指定します。

```
hostname(config)# logging class ha asdm 2 buffered 7
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
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。

logging console

セキュリティ アプライアンスが syslog メッセージをコンソール セッションに表示できるようにするには、グローバル コンフィギュレーション モードで **logging console** コマンドを使用します。syslog メッセージをコンソール セッションに表示しないようにするには、このコマンドの **no** 形式を使用します。

logging console [*logging_list* | *level*]

no logging console

（注）　このコマンドを使用すると、バッファ オーバーフローによって多数の syslog メッセージがドロップされる可能性があるため、このコマンドの使用はお勧めできません。詳細については、後述する「使用上のガイドライン」の項を参照してください。

シンタックスの説明

level	システム ログ メッセージの最大レベルを設定します。たとえば、レベルを 3 に設定すると、セキュリティ アプライアンスはレベル 3、2、1、および 0 のシステム ログ メッセージを生成します。次の数値または名前で指定できます。 • **0** または **emergencies**：システムが使用不能 • **1** または **alerts**：ただちに処置が必要 • **2** または **critical**：クリティカルな状態 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：正常だが、注意が必要な状態 • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、WWW URL
logging_list	コンソール セッションに送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

デフォルト

セキュリティ アプライアンスは、デフォルトでは、syslog メッセージをコンソール セッションに表示しません。

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　コンソールにメッセージが送信される前に、**logging enable** コマンドを使用してロギングをイネーブルにしておく必要があります。

注意　**logging console** コマンドを使用すると、システム パフォーマンスが大幅に低下する可能性があります。代わりに、**logging buffered** を使用してロギングを開始し、**show logging** コマンドを使用してメッセージを表示してください。最新のメッセージをより簡単に表示するには、**clear logging *buffer*** コマンドを使用してバッファを消去します。

例　次の例は、レベル 0、1、2、および 3 の syslog メッセージをコンソール セッションに表示できるようにする方法を示しています。

```
hostname(config)# logging enable
hostname(config)# logging console errors
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging list	再使用可能なメッセージ選択基準リストを作成します。
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。

logging debug-trace

デバッグ メッセージを、重大度 7 で発行された syslog メッセージ 711011 としてログにリダイレクトするには、グローバル コンフィギュレーション モードで **logging debug-trace** コマンドを使用します。ログへのデバッグ メッセージの送信を停止するには、このコマンドの **no** 形式を使用します。

logging debug-trace

no logging debug-trace

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、セキュリティ アプライアンスはデバッグ出力を syslog メッセージに含めません。

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

デバッグ メッセージは、重大度 7 のメッセージとして生成されます。このメッセージは、syslog メッセージ番号 711011 と一緒にログに表示されます。

例

次の例は、ロギングをイネーブルにし、ログ メッセージをシステム ログ バッファに送信し、デバッグ出力をログにリダイレクトし、ディスク アクティビティのデバッグをオンにする方法を示しています。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging debug-trace
hostname(config)# debug disk filesystem
```

ログに表示できるデバッグ メッセージの例を次に示します。

```
%PIX-7-711001: IFS: Read: fd 3, bytes 4096
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
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。

logging device-id

EMBLEM 形式でない syslog メッセージにデバイス ID を含めるようにセキュリティ アプライアンスを設定するには、グローバル コンフィギュレーション モードで **logging device-id** コマンドを使用します。デバイス ID の使用をディセーブルにするには、このコマンドの **no** 形式を使用します。

logging device-id {***context-name*** | ***hostname*** | ***ipaddress*** *interface_name* | ***string*** *text*}

no logging device-id {***context-name*** | ***hostname*** | ***ipaddress*** *interface_name* | ***string*** *text*}

シンタックスの説明

context-name	デバイス ID として、現在のコンテキストの名前を使用します。
hostname	デバイス ID として、セキュリティ アプライアンスのホスト名を使用します。
ipaddress *interface_name*	デバイス ID として、*interface_name* で指定されたインターフェイスの IP アドレスを使用します。**ipaddress** キーワードを使用すると、セキュリティ アプライアンスがログ データを外部サーバに送信するために使用するインターフェイスに関係なく、外部サーバに送信される syslog メッセージに、指定されたインターフェイスの IP アドレスが含まれます。
string *text*	デバイス ID として、*text* に含まれている最大 16 文字の文字を使用します。*text* にスペースや次の文字は使用できません。 • &：アンパサンド • '：一重引用符 • "：二重引用符 • <：小なり • >：大なり • ?：疑問符

デフォルト

syslog メッセージにデフォルトのデバイス ID は使用されません。

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
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

ipaddress キーワードを使用すると、デバイス ID は、メッセージが送信されたインターフェイスに関係なく、指定したセキュリティ アプライアンス インターフェイスの IP アドレスとなります。このキーワードの使用により、そのデバイスから送信されるメッセージすべてに、1 つの同じデバイス ID が割り当てられます。

例

次の例は、secappl-1 というホストを設定する方法を示しています。

```
hostname(config)# logging device-id hostname
hostname(config)# show logging
Syslog logging: disabled
Facility: 20
Timestamp logging: disabled
Standby logging: disabled
Console logging: disabled
Monitor logging: disabled
Buffer logging: level informational, 991 messages logged
Trap logging: disabled
History logging: disabled
Device ID: hostname "secappl-1"
```

syslog メッセージでは、ホスト名 secappl-1 はメッセージの先頭に表示されます。メッセージの例を次に示します。

```
secappl-1 %PIX-5-111008: User 'enable_15' executed the 'logging buffer-size 4096'
command.
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
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。

logging emblem

syslog サーバ以外のロギング先に送信される syslog メッセージに EMBLEM 形式を使用するには、グローバル コンフィギュレーション モードで **logging emblem** コマンドを使用します。EMBLEM 形式の使用をディセーブルにするには、このコマンドの **no** 形式を使用します。

logging emblem

no logging emblem

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、セキュリティ アプライアンスは syslog メッセージに EMBLEM 形式を使用しません。

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
7.0(1)	このコマンドが **logging host** コマンドと無関係になるように変更されました。

使用上のガイドライン

logging emblem コマンドを使用すると、syslog サーバを除くすべてのロギング先に対して、EMBLEM 形式のロギングをイネーブルにできます。**logging timestamp** キーワードもイネーブルにすると、タイムスタンプ付きのメッセージが送信されます。

syslog サーバに対して EMBLEM 形式のロギングをイネーブルにするには、**logging host** コマンドに ***format emblem*** オプションを使用します。

例

次の例は、ロギングをイネーブルにし、syslog サーバを除くすべてのロギング先へのロギングに対して、EMBLEM 形式の使用をイネーブルにする方法を示しています。

```
hostname(config)# logging enable
hostname(config)# logging emblem
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
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。

logging enable

設定済みの出力場所すべてに対してロギングをイネーブルにするには、グローバル コンフィギュレーション モードで **logging enable** コマンドを使用します。ロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

logging enable

no logging enable

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

ロギングは、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 **logging on** コマンドから変更されました。

使用上のガイドライン

logging enable コマンドを使用すると、サポートされている任意のロギング先に対する syslog メッセージの送信をイネーブルまたはディセーブルにできます。すべてのロギングを停止するには、**no logging enable** コマンドを使用します。

個別のロギング先へのロギングをイネーブルにするには、次のコマンドを使用します。

- **logging asdm**
- **logging buffered**
- **logging console**
- **logging history**
- **logging mail**
- **logging monitor**
- **logging trap**

例

次の例は、ロギングをイネーブルにする方法を示しています。**show logging** コマンドの出力は、使用可能な各ロギング先を個別にイネーブルにする必要がある状況を示しています。

```
hostname(config)# logging enable
hostname(config)# show logging
Syslog logging: enabled
    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。

logging facility

syslog サーバに送信されるメッセージに使用するロギング ファシリティを指定するには、グローバル コンフィギュレーション モードで **logging facility** コマンドを使用します。ロギング ファシリティをデフォルトの 20 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。

logging facility *facility*

no logging facility

シンタックスの説明

facility	syslog ファシリティを指定します。有効値は 16 ～ 23 です。

デフォルト

デフォルト ファシリティは 20（LOCAL4）です。

コマンドのモード

次の表は、コマンドを入力できるモードを示しています。例外については、上記の「シンタックスの説明」の項を参照してください。

	ファイアウォール モード		セキュリティ 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

syslog サーバは、メッセージの *facility* 番号をもとに、メッセージをファイルします。使用可能なファシリティには、16（LOCAL0）～ 23（LOCAL7）の 8 つがあります。

例

次の例は、セキュリティ アプライアンスがロギング ファシリティを 16 として syslog メッセージに指定するように設定する方法を示しています。**show logging** コマンドの出力には、セキュリティ アプライアンスによって使用されているファシリティが含まれます。

```
hostname(config)# logging facility 16
hostname(config)# show logging
Syslog logging: enabled
    Facility: 16
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: level errors, facility 16, 3607 messages logged
        Logging to infrastructure 10.1.2.3
    History logging: disabled
    Device ID: 'inside' interface IP address "10.1.1.1"
    Mail logging: disabled
    ASDM logging: disabled
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging host	syslog サーバを定義します。
logging trap	syslog サーバへのロギングをイネーブルにします。
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。

logging flash-bufferwrap

バッファが未保存のメッセージでいっぱいになるたびに、セキュリティ アプライアンスがログ バッファをフラッシュ メモリに書き込めるようにするには、グローバル コンフィギュレーション モードで **logging flash-bufferwrap** コマンドを使用します。ログ バッファをフラッシュ メモリに書き込めないようにするには、このコマンドの **no** 形式を使用します。

logging flash-bufferwrap

no logging flash-bufferwrap

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　デフォルトは次のとおりです。

- バッファへのロギングはディセーブルです。
- フラッシュ メモリへのログ バッファの書き込みはディセーブルです。
- バッファのサイズは 4 KB です。
- フラッシュ メモリの最小空き容量は 3 MB です。
- バッファ ロギング用のフラッシュ メモリ最大割当量は、1 MB 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

セキュリティ アプライアンスがログ バッファをフラッシュ メモリに書き込めるようにするには、バッファへのロギングをイネーブルにする必要があります。このようにしないと、フラッシュ メモリに書き込むデータがログ バッファに保持されません。バッファへのロギングをイネーブルにするには、**logging buffered** コマンドを使用します。

セキュリティ アプライアンスは、ログ バッファの内容をフラッシュ メモリに書き込む間も、新しいイベント メッセージをログ バッファに継続的に格納します。

セキュリティ アプライアンスは、次のように、デフォルトのタイムスタンプ形式を使用した名前でログ ファイルを作成します。

LOG-*YYYY-MM-DD-HHMMSS*.TXT

YYYY は西暦年、*MM* は月、*DD* は日、*HHMMSS* は時刻の時、分、秒です。

フラッシュ メモリの可用性により、セキュリティ アプライアンスが **logging flash-bufferwrap** コマンドを使用して syslog メッセージを保存するときの方法が異なります。詳細については、**logging flash-maximum-allocation** コマンドと **logging flash-minimum-free** コマンドを参照してください。

例

次の例は、ロギングとログ バッファをイネーブルにし、セキュリティ アプライアンスがログ バッファをフラッシュ メモリに書き込めるようにする方法を示しています。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging flash-bufferwrap

hostname(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	保持しているすべての syslog メッセージのログ バッファを消去します。
copy	ファイルを、ある位置から TFTP サーバや FTP サーバなどの別の位置にコピーします。
delete	保存済みログ ファイルなどのファイルを、ディスク パーティションから削除します。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging buffer-size	ログ バッファのサイズを指定します。
logging enable	ロギングをイネーブルにします。
logging flash-maximum-allocation	フラッシュ メモリについて、ログ バッファの内容を書き込むために使用できる最大量を指定します。
logging flash-minimum-free	フラッシュ メモリへのログ バッファの書き込みを許可するときに、セキュリティ アプライアンスが使用できるようにしておく必要のある最小限のフラッシュ メモリ量を指定します。
show logging	イネーブルなロギング オプションを表示します。

logging flash-maximum-allocation

セキュリティ アプライアンスがログ データの格納に使用するフラッシュ メモリの最大量を指定するには、グローバル コンフィギュレーション モードで **logging flash-maximum-allocation** コマンドを使用します。このコマンドにより、**logging savelog** コマンドと **logging flash-bufferwrap** コマンドで使用できるフラッシュ メモリの最大量が決まります。この用途に使用するフラッシュ メモリの最大量をデフォルト サイズの 1 MB 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。

logging flash-maximum-allocation *kbytes*

no logging flash-maximum-allocation *kbytes*

シンタックスの説明

kbytes	セキュリティ アプライアンスがログ バッファ データの保存に使用できるフラッシュ メモリの最大量（KB 単位）。

デフォルト

ログ データ用のデフォルトのフラッシュ メモリ最大割当量は、1 MB 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

logging savelog または **logging flash-bufferwrap** によって保存されるログ ファイルが原因で、ログ ファイル用のフラッシュ メモリの使用量が、**logging flash-maximum-allocation** コマンドで指定された最大量を超える場合、セキュリティ アプライアンスは最も古いログ ファイルを削除して、新しいログ ファイル用に十分な量のメモリを開放します。削除するファイルがない場合や、古いファイルをすべて削除してもメモリの空き容量が新しいログ ファイル用には小さすぎる場合、セキュリティ アプライアンスは新しいログ ファイルを保存できません。

セキュリティ アプライアンスによるフラッシュ メモリの最大割当量がデフォルト サイズと異なっているかどうかを確認するには、**show running-config logging** コマンドを使用します。**logging flash-maximum-allocation** コマンドが表示されない場合、セキュリティ アプライアンスがログ バッファ データの保存に使用する最大サイズは 1 MB です。割り当てられたメモリは、**logging savelog** コマンドと **logging flash-bufferwrap** コマンドの両方に使用されます。

セキュリティ アプライアンスによるログ バッファの使用方法の詳細については、**logging buffered** コマンドを参照してください。

例

次の例は、ロギングとログ バッファをイネーブルにし、セキュリティ アプライアンスがログ バッファをフラッシュ メモリに書き込めるようにし、ログ ファイルの書き込みに使用するフラッシュ メモリの最大量を約 1.2 MB に設定する方法を示しています。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging flash-bufferwrap
hostname(config)# logging flash-maximum-allocation 1200
hostname(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	保持しているすべての syslog メッセージのログ バッファを消去します。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging enable	ロギングをイネーブルにします。
logging flash-bufferwrap	ログ バッファがいっぱいになったときに、ログ バッファをフラッシュ メモリに書き込みます。
logging flash-minimum-free	フラッシュ メモリへのログ バッファの書き込みを許可するときに、セキュリティ アプライアンスが使用できるようにしておく必要のある最小限のフラッシュ メモリ量を指定します。
logging savelog	ログ バッファの内容をフラッシュ メモリに保存します。
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	現在動作しているロギング コンフィギュレーションを表示します。

logging flash-minimum-free

セキュリティ アプライアンスが新しいログ ファイルを保存する前に確保しておく必要のあるフラッシュ メモリの最小空き容量を指定するには、グローバル コンフィギュレーション モードで **logging flash-minimum-free** コマンドを使用します。このコマンドにより、**logging savelog** コマンドと **logging flash-bufferwrap** コマンドで作成されたログファイルをセキュリティ アプライアンスが保存する前に確保しておく必要のあるフラッシュ メモリの空き容量が異なります。フラッシュ メモリの必要最小限の空き容量をデフォルト サイズの 3 MB 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。

logging flash-minimum-free *kbytes*

no logging flash-minimum-free *kbytes*

シンタックスの説明

kbytes	セキュリティ アプライアンスが新しいログ ファイルを保存する前に使用可能にしておく必要のあるフラッシュ メモリの最小量（KB 単位）。

デフォルト

デフォルトのフラッシュ メモリの最小空き容量は 3 MB 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

logging flash-minimum-free コマンドは、**logging savelog** コマンドと **logging flash-bufferwrap** コマンド用に常に確保しておく必要のあるフラッシュ メモリ量を指定します。

logging savelog または **logging flash-bufferwrap** によって保存されるログ ファイルが原因で、フラッシュ メモリの空き容量が、**logging flash-minimum-free** コマンドで指定された限度を下回る場合、セキュリティ アプライアンスは最も古いログ ファイルを削除して、新しいログ ファイルの保存後もメモリの最小空き容量が保持されることを保証します。削除するファイルがない場合や、古いファイルをすべて削除してもメモリの空き容量が限度を下回る場合、セキュリティ アプライアンスは新しいログ ファイルを保存できません。

例

次の例は、ロギングとログ バッファをイネーブルにし、セキュリティ アプライアンスがログ バッファをフラッシュ メモリに書き込めるようにし、フラッシュ メモリの最小空き容量を 4,000 KB にする必要があることを指定する方法を示しています。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging flash-bufferwrap
hostname(config)# logging flash-minimum-free 4000
hostname(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	保持しているすべての syslog メッセージのログ バッファを消去します。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging enable	ロギングをイネーブルにします。
logging flash-bufferwrap	ログ バッファがいっぱいになったときに、ログ バッファをフラッシュ メモリに書き込みます。
logging flash-maximum-allocation	フラッシュ メモリについて、ログ バッファの内容を書き込むために使用できる最大量を指定します。
logging savelog	ログ バッファの内容をフラッシュ メモリに保存します。
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	現在動作しているロギング コンフィギュレーションを表示します。

logging from-address

セキュリティ アプライアンスによって電子メールで送信される syslog メッセージの送信者の電子メール アドレスを指定するには、グローバル コンフィギュレーション モードで **logging from-address** コマンドを使用します。syslog メッセージ電子メールはすべて、指定したアドレスから送信されたように表示されます。送信者の電子メール アドレスを削除するには、このコマンドの **no** 形式を使用します。

logging from-address *from-email-address*

no logging from-address *from-email-address*

シンタックスの説明

from-email-address	送信元の電子メール アドレス（syslog 電子メールの送信元として表示される電子メール アドレス）。たとえば、cdb@example.com 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

syslog メッセージを電子メールで送信できるようにするには、**logging mail** コマンドを使用します。

このコマンドで指定するアドレスは、既存の電子メール アカウントに対応している必要はありません。

例

次の基準に従って、ロギングをイネーブルにし、syslog メッセージを電子メールで送信するようにセキュリティ アプライアンスを設定します。

- critical、alerts、および emergencies のメッセージを送信する。
- メッセージを送信するときに、ciscosecurityappliance@example.com を送信者のアドレスとして使用する。
- メッセージを admin@example.com に送信する。
- SMTP を使用して、メッセージをプライマリ サーバ pri-smtp-host およびセカンダリ サーバ sec-smtp-host に送信する。

次のコマンドを入力します。

```
hostname(config)# logging enable
hostname(config)# logging mail critical
hostname(config)# logging from-address ciscosecurityappliance@example.com
hostname(config)# logging recipient-address admin@example.com
hostname(config)# smtp-server pri-smtp-host sec-smtp-host
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging mail	セキュリティ アプライアンスが syslog メッセージを電子メールで送信できるようにし、どのメッセージを電子メールで送信するかを決定します。
logging recipient-address	syslog メッセージ電子メールの送信先となる電子メール アドレスを指定します。
smtp-server	SMTP サーバを設定します。
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	現在動作しているロギング コンフィギュレーションを表示します。

logging ftp-bufferwrap

バッファが未保存のメッセージでいっぱいになるたびに、セキュリティ アプライアンスがログ バッファを FTP サーバに送信できるようにするには、グローバル コンフィギュレーション モードで **logging ftp-bufferwrap** コマンドを使用します。ログ バッファを FTP サーバに送信しないようにするには、このコマンドの **no** 形式を使用します。

logging ftp-bufferwrap

no logging ftp-bufferwrap

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

デフォルトは次のとおりです。

- バッファへのロギングはディセーブルです。
- FTP サーバへのログ バッファの送信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
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

logging ftp-bufferwrap がイネーブルの場合、セキュリティ アプライアンスは、**logging ftp-server** コマンドで指定された FTP サーバにログ バッファ データを送信します。セキュリティ アプライアンスは、ログ データを FTP サーバに送信する間も、新しいイベント メッセージをログ バッファに継続的に格納します。

セキュリティ アプライアンスがログ バッファの内容を FTP サーバに送信できるようにするには、バッファへのロギングをイネーブルにする必要があります。このようにしないと、フラッシュ メモリに書き込むデータがログ バッファに保持されません。バッファへのロギングをイネーブルにするには、**logging buffered** コマンドを使用します。

セキュリティ アプライアンスは、次のように、デフォルトのタイムスタンプ形式を使用した名前でログ ファイルを作成します。

LOG-*YYYY-MM-DD-HHMMSS*.TXT

YYYY は西暦年、*MM* は月、*DD* は日、*HHMMSS* は時刻の時、分、秒です。

例

次の例は、ロギングとログ バッファをイネーブルにし、FTP サーバを指定し、セキュリティ アプライアンスがログ バッファを FTP サーバに書き込めるようにする方法を示しています。この例では、logserver-352 というホスト名の FTP サーバを指定しています。このサーバには、ユーザ名 logsupervisor とパスワード 1luvMy10gs を使用してアクセスできます。ログ ファイルは、/syslogs ディレクトリに保存されます。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging ftp-server logserver-352 /syslogs logsupervisor 1luvMy10gs
hostname(config)# logging ftp-bufferwrap
hostname(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	保持しているすべての syslog メッセージのログ バッファを消去します。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging buffer-size	ログ バッファのサイズを指定します。
logging enable	ロギングをイネーブルにします。
logging ftp-server	**logging ftp-bufferwrap** コマンドで使用する FTP サーバ パラメータを指定します。
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	現在動作しているロギング コンフィギュレーションを表示します。

logging ftp-server

logging ftp-bufferwrap がイネーブルの場合にセキュリティ アプライアンスがログ バッファ データを送信する FTP サーバについての詳細を指定するには、グローバル コンフィギュレーション モードで **logging ftp-server** コマンドを使用します。FTP サーバについての詳細をすべて削除するには、このコマンドの **no** 形式を使用します。

logging ftp-server *ftp-server ftp_server path username password*

no logging ftp-server *ftp-server ftp_server path username password*

シンタックスの説明

ftp-server	外部 FTP サーバの IP アドレスまたはホスト名。 **（注）** ホスト名を指定する場合は、ネットワーク上で DNS が正しく動作していることを確認してください。
path	ログ バッファ データの保存先となる FTP サーバ上のディレクトリ パス。このパスは、FTP ルート ディレクトリに対する相対パスです。次の例を参考にしてください。 `/security_appliances/syslogs/appliance107`
username	FTP サーバへのロギングに有効なユーザ名。
password	指定したユーザ名に対応するパスワード。

デフォルト

FTP サーバは、デフォルトでは指定されていません。

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

指定できる FTP サーバは 1 つのみです。ロギング FTP サーバがすでに指定されている場合、**logging ftp-server** コマンドを使用すると、その FTP サーバ コンフィギュレーションが、入力した新しいコンフィギュレーションに置き換えられます。

セキュリティ アプライアンスは、指定された FTP サーバ情報を確認しません。詳細を誤って設定した場合、セキュリティ アプライアンスはログ バッファ データを FTP サーバに送信できません。

例

次の例は、ロギングとログ バッファをイネーブルにし、FTP サーバを指定し、セキュリティ アプライアンスがログ バッファを FTP サーバに書き込めるようにする方法を示しています。この例では、logserver-352 というホスト名の FTP サーバを指定しています。このサーバには、ユーザ名 logsupervisor とパスワード 1luvMy10gs を使用してアクセスできます。ログ ファイルは、/syslogs ディレクトリに保存されます。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging ftp-server logserver-352 /syslogs logsupervisor 1luvMy10gs
hostname(config)# logging ftp-bufferwrap
hostname(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	保持しているすべての syslog メッセージのログ バッファを消去します。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging buffer-size	ログ バッファのサイズを指定します。
logging enable	ロギングをイネーブルにします。
logging ftp-bufferwrap	ログ バッファがいっぱいになったときに、ログ バッファを FTP サーバに送信します。
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	現在動作しているロギング コンフィギュレーションを表示します。

logging history

SNMP ロギングをイネーブルにし、SNMP サーバに送信されるメッセージを指定するには、グローバル コンフィギュレーション モードで **logging history** コマンドを使用します。SNMP ロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

logging history [*logging_list* | *level*]

no logging history

シンタックスの説明

level	システム ログ メッセージの最大レベルを設定します。たとえば、レベルを 3 に設定すると、セキュリティ アプライアンスはレベル 3、2、1、および 0 のシステム ログ メッセージを生成します。次の数値または名前で指定できます。 • **0** または **emergencies**：システムが使用不能 • **1** または **alerts**：ただちに処置が必要 • **2** または **critical**：クリティカルな状態 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：正常だが、注意が必要な状態 • **6** または **informational**：情報 • **7** または **debugging**:デバッグ メッセージ、ログ FTP コマンド、WWW URL
logging_list	SNMP サーバに送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

デフォルト

セキュリティ アプライアンスは、デフォルトでは SNMP サーバにロギングしません。

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

logging history コマンドを使用すると、SNMP サーバへのロギングをイネーブルにし、SNMP メッセージ レベルまたはイベント リストを設定することができます。

例

次の例は、SNMP ロギングをイネーブルにし、レベル 0、1、2、および 3 のメッセージが設定済みの SNMP サーバに送信されるよう指定する方法を示しています。

```
hostname(config)# logging enable
hostname(config)# snmp-server host infrastructure 10.2.3.7 trap community gam327
hostname(config)# snmp-server enable traps syslog
hostname(config)# logging history errors
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging list	再使用可能なメッセージ選択基準リストを作成します。
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。
snmp-server	SNMP サーバの詳細を指定します。

logging host

syslog サーバを定義するには、グローバル コンフィギュレーション モードで **logging host** コマンドを使用します。syslog サーバの定義を削除するには、このコマンドの **no** 形式を使用します。

logging host *interface_name syslog_ip* [***tcp****/port* | ***udp****/port*] [**format emblem**]

logging host *interface_name syslog_ip*

シンタックスの説明

format emblem	（オプション）syslog サーバに対して EMBLEM 形式のロギングをイネーブルにします。
interface_name	syslog サーバが常駐するインターフェイス。
syslog_ip	syslog サーバの IP アドレス。
tcp	メッセージを syslog サーバに送信するときに、セキュリティ アプライアンスが TCP を使用することを指定します。
udp	メッセージを syslog サーバに送信するときに、セキュリティ アプライアンスが TCP を使用することを指定します。
port	syslog サーバがメッセージをリスンするポート。有効となるポート値の範囲は、どちらのプロトコルの場合も 1025 ～ 65535 です。

デフォルト

デフォルトは次のとおりです。

- デフォルトのポート番号は次のとおりです。
  - UDP ポートは 514
  - TCP ポートは 1470
- デフォルト プロトコルは UDP 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

logging host *ip_address* **format emblem** コマンドを使用すると、各 syslog サーバに対して EMBLEM 形式のロギングをイネーブルにできます。EMBLEM 形式のロギングは、UDP syslog メッセージに対してだけ利用できます。EMBLEM 形式のロギングを特定の syslog ホストに対してイネーブルにすると、メッセージがそのホストに送信されます。**logging timestamp** キーワードもイネーブルにすると、タイムスタンプ付きのメッセージが送信されます。

複数の **logging host** コマンドを使用して複数の追加サーバを指定すると、追加したサーバすべてが syslogs メッセージを受信します。ただし、サーバは UDP か TCP のどちらか一方を受信するように指定でき、両方を受信するようには指定できません。

以前入力した *port* と *protocol* の値のみを表示するには、**show running-config logging** コマンドを使用して、リストでコマンドを見つけます（TCP プロトコルは 6、UDP プロトコルは 17 として示されます）。TCP ポートは、セキュリティ アプライアンス syslog サーバに対してのみ動作します。*port* は、syslog サーバがリスンするポートと一致している必要があります。

例

次の例は、内部インターフェイス上にあってデフォルトのプロトコルとポート番号を使用する syslog サーバに対して、レベル 0、1、2、および 3 の syslog メッセージを送信する方法を示しています。

```
hostname(config)# logging enable
hostname(config)# logging host inside 10.2.2.3
hostname(config)# logging trap errors
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging trap	syslog サーバへのロギングをイネーブルにします。
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。

logging list

各種の基準（ロギング レベル、イベント クラス、およびメッセージ ID）でメッセージを指定するため、他のコマンドで使用するロギング リストを作成するには、グローバル コンフィギュレーション モードで **logging list** コマンドを使用します。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。

logging list *name* {**level** *level* [**class** *event_class*] | **message** *start_id*[-*end_id*]}

no logging list *name*

シンタックスの説明

class *event_class*	（オプション）syslog メッセージのイベント クラスを設定します。指定されたレベルに対応する、指定されたクラスの syslog メッセージのみが、コマンドによって特定されます。クラス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。
level *level*	システム ログ メッセージの最大レベルを設定します。たとえば、レベルを 3 に設定すると、セキュリティ アプライアンスはレベル 3、2、1、および 0 のシステム ログ メッセージを生成します。次の数値または名前で指定できます。 • **0** または **emergencies**：システムが使用不能 • **1** または **alerts**：ただちに処置が必要 • **2** または **critical**：クリティカルな状態 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：正常だが、注意が必要な状態 • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、WWW URL
message *start_id*[-*end_id*]	メッセージ ID または ID の範囲を指定します。メッセージのデフォルト レベルを確認するには、**show logging** コマンドを使用するか、『*Cisco Security Appliance System Log Messages*』を参照してください。
name	ロギング リストの名前を設定します。

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　リストを使用できるロギング コマンドは、次のとおりです。

- **logging asdm**
- **logging buffered**
- **logging console**
- **logging history**
- **logging mail**
- **logging monitor**
- **logging trap**

event_class に指定できる値は、次のとおりです。

- **auth**：ユーザ認証
- **bridge**：透過ファイアウォール
- **ca**：PKI 認証局
- **config**：コマンド インターフェイス
- **email**：電子メール プロキシ
- **ha**：フェールオーバー
- **ids**：侵入検知システム
- **ip**：IP スタック
- **np**：ネットワーク プロセッサ
- **ospf**：OSPF ルーティング
- **rip**：RIP ルーティング
- **session**：ユーザ セッション
- **snmp**：SNMP
- **sys**：システム
- **vpn**：IKE および IPSec
- **vpnc**：VPN クライアント
- **vpnfo**：VPN フェールオーバー
- **vpnlb**：VPN ロードバランシング

例　次の例は、logging list コマンドを使用する方法を示しています。

```
hostname(config)# logging list my-list 100100-100110
hostname(config)# logging list my-list level critical
hostname(config)# logging list my-list level warning class vpn
hostname(config)# logging buffered my-list
```

上記の例は、指定された基準に一致する syslog メッセージがロギング バッファに送信されることを示しています。この例で指定されている基準は、次のとおりです。

1. 100100 ～ 100110 の範囲内にある syslog メッセージ ID
2. critical レベル以上（emergency、alert、または critical）にあるすべての syslog メッセージ
3. warning レベル以上（emergency、alert、critical、error、または warning）にある VPN クラスのすべての syslog メッセージ

syslog メッセージがこれらの条件のいずれかを満たしている場合、そのメッセージはバッファにロギングされます。

（注）　リストの基準を設計する場合、メッセージを重複して指定する基準にしてもかまいません。複数の基準に一致する syslog メッセージも正常にロギングされます。

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
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。

logging mail

セキュリティ アプライアンスが syslog メッセージを電子メールで送信したり、電子メールで送信するメッセージを判別したりできるようにするには、グローバル コンフィギュレーション モードで **logging mail** コマンドを使用します。syslog メッセージを電子メールで送信しないようにするには、このコマンドの **no** 形式を使用します。

logging mail [*logging_list* | *level*]

no logging mail [*logging_list* | *level*]

シンタックスの説明

level	システム ログ メッセージの最大レベルを設定します。たとえば、レベルを 3 に設定すると、セキュリティ アプライアンスはレベル 3、2、1、および 0 のシステム ログ メッセージを生成します。次の数値または名前で指定できます。 • **0** または **emergencies**：システムが使用不能 • **1** または **alerts**：ただちに処置が必要 • **2** または **critical**：クリティカルな状態 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：正常だが、注意が必要な状態 • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、WWW URL
logging_list	電子メールの受信者に送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

デフォルト

電子メールへのロギングは、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。

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

電子メールで送信された syslog メッセージは、送信済み電子メールの件名欄に表示されます。

例

次の基準に従って、syslog メッセージを電子メールで送信するようにセキュリティ アプライアンスを設定します。

- critical、alerts、および emergencies のメッセージを送信する。
- メッセージを送信するときに、ciscosecurityappliance@example.com を送信者のアドレスとして使用する。
- メッセージを admin@example.com に送信する。
- SMTP を使用して、メッセージをプライマリ サーバ pri-smtp-host およびセカンダリ サーバ sec-smtp-host に送信する。

次のコマンドを入力します。

```
hostname(config)# logging mail critical
hostname(config)# logging from-address ciscosecurityappliance@example.com
hostname(config)# logging recipient-address admin@example.com
hostname(config)# smtp-server pri-smtp-host sec-smtp-host
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging from-address	syslog メッセージ電子メールの送信元として表示する電子メール アドレスを指定します。
logging list	再使用可能なメッセージ選択基準リストを作成します。
logging recipient-address	syslog メッセージ電子メールの送信先となる電子メール アドレスを指定します。
smtp-server	SMTP サーバを設定します。
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	現在動作しているロギング コンフィギュレーションを表示します。

logging message

syslog メッセージのロギング レベルを指定するには、グローバル コンフィギュレーション モードで **logging message** コマンドを ***level*** キーワードと組み合せて使用します。メッセージのロギング レベルをデフォルト レベル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。セキュリティ アプライアンスが特定の syslog メッセージを生成しないようにするには、グローバル コンフィギュレーション モードで **logging message** コマンドの **no** 形式を使用します（***level*** キーワードは指定しません）。セキュリティ アプライアンスが特定の syslog メッセージを生成できるようにするには、**logging message** コマンドを使用します（***level*** キーワードは指定しません）。これら 2 つの用途の **logging message** コマンドは、並行して実行できます。後述する「例」の項を参照してください。

logging message *syslog_id* **level** *level*

no logging message *syslog_id* **level** *level*

logging message *syslog_id*

no logging message *syslog_id*

シンタックスの説明

level *level*	システム ログ メッセージの最大レベルを設定します。たとえば、レベルを 3 に設定すると、セキュリティ アプライアンスはレベル 3、2、1、および 0 のシステム ログ メッセージを生成します。次の数値または名前で指定できます。 • **0** または **emergencies**：システムが使用不能 • **1** または **alerts**：ただちに処置が必要 • **2** または **critical**：クリティカルな状態 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：正常だが、注意が必要な状態 • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、WWW URL
syslog_id	イネーブルまたはディセーブルにする syslog メッセージ、または重大度を変更する syslog メッセージの ID。メッセージのデフォルト レベルを確認するには、**show logging** コマンドを使用するか、『*Cisco Security Appliance System Log Messages*』を参照してください。

デフォルト

デフォルトでは、syslog メッセージはすべてイネーブルになっており、すべてのメッセージの重大度はデフォルト レベルに設定されています。

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
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

logging message コマンドは、次の 2 つの用途に使用できます。

- メッセージをイネーブルとディセーブルのどちらにするかを制御する。
- メッセージの重大度を制御する。

メッセージに現在割り当てられているレベルや、メッセージがイネーブルになっているかどうかを判別するには、**show logging** コマンドを使用します。

例

次の例にある一連のコマンドは、**logging message** コマンドを使用して、メッセージをイネーブルにするかどうか、およびメッセージの重大度の両方を制御する方法を示しています。

```
hostname(config)# show logging message 403503
syslog 403503: default-level errors (enabled)

hostname(config)# logging message 403503 level 1
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)

hostname(config)# no logging message 403503
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (disabled)

hostname(config)# logging message 403503
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)

hostname(config)# no logging message 403503 level 3
hostname(config)# show logging message 403503
syslog 403503: default-level errors (enabled)
```

関連コマンド

コマンド	説明
clear configure logging	ロギング コンフィギュレーションすべてまたはメッセージ コンフィギュレーションのみを消去します。
logging enable	ロギングをイネーブルにします。
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。

logging monitor

セキュリティ アプライアンスが syslog メッセージを SSH および Telnet セッションに表示できるようにするには、グローバル コンフィギュレーション モードで **logging monitor** コマンドを使用します。syslog メッセージを SSH および Telnet セッションに表示しないようにするには、このコマンドの **no** 形式を使用します。

logging monitor [*logging_list* | *level*]

no logging monitor

シンタックスの説明

level	システム ログ メッセージの最大レベルを設定します。たとえば、レベルを 3 に設定すると、セキュリティ アプライアンスはレベル 3、2、1、および 0 のシステム ログ メッセージを生成します。次の数値または名前で指定できます。 • **0** または **emergencies**：システムが使用不能 • **1** または **alerts**：ただちに処置が必要 • **2** または **critical**：クリティカルな状態 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：正常だが、注意が必要な状態 • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、WWW URL
logging_list	SSH または Telnet セッションに送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

デフォルト

セキュリティ アプライアンスは、デフォルトでは、syslog メッセージを SSH および Telnet セッションに表示しません。

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

logging monitor コマンドを使用すると、現在のコンテキスト内のセッションすべてに対して syslog メッセージをイネーブルにできます。ただし、セッションに syslog メッセージを表示するかどうかは、セッションごとに **terminal** コマンドで制御します。

例

次の例は、syslog メッセージをコンソール セッションに表示できるようにする方法を示しています。***errors*** キーワードを使用することは、レベル 0、1、2、および 3 のメッセージを SSH および Telnet セッションに表示する必要があることを示しています。**terminal** コマンドを使用すると、現在のセッションにメッセージを表示できます。

```
hostname(config)# logging enable
hostname(config)# logging monitor errors
hostname(config)# terminal monitor
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging list	再使用可能なメッセージ選択基準リストを作成します。
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。
terminal	端末回線のパラメータを設定します。

logging permit-hostdown

TCP ベースの syslog サーバの状態が新しいユーザ セッションとは無関係になるように指定するには、グローバル コンフィギュレーション モードで **logging permit-hostdown** コマンドを使用します。TCP ベースの syslog サーバが使用不能のときにセキュリティ アプライアンスが新しいユーザ セッションを拒否するように設定するには、このコマンドの **no** 形式を使用します。

logging permit-hostdown

no logging permit-hostdown

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、TCP 接続を使用する syslog サーバへのロギングをイネーブルにした場合、何らかの理由で syslog サーバが使用不能になったときは、セキュリティ アプライアンスは新しいネットワーク アクセス セッションを許可しません。

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
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

syslog サーバにメッセージを送信するためのロギング転送プロトコルとして TCP を使用する場合、セキュリティ アプライアンスは、syslog サーバに到達できないときは、セキュリティ保護手段として、新しいネットワーク アクセス セッションを拒否します。この制限を削除するには、**logging permit-hostdown** コマンドを使用します。

例

次の例では、TCP ベースの syslog サーバの状態が、セキュリティ アプライアンスが新しいセッションを許可するかどうかとは無関係になるように指定します。show running-config logging コマンドの出力に show running-config logging コマンドが含まれている場合、TCP ベースの syslog サーバの状態は新しいネットワーク アクセス セッションとは無関係になっています。

```
hostname(config)# logging permit-hostdown
hostname(config)# show running-config logging
logging enable
logging trap errors
logging host infrastructure 10.1.2.3 6/1470
logging permit-hostdown
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging host	syslog サーバを定義します。
logging trap	syslog サーバへのロギングをイネーブルにします。
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。

logging queue

セキュリティ アプライアンスがロギング コンフィギュレーションに従って処理する前に syslog キューに保持できる syslog メッセージの数を指定するには、グローバル コンフィギュレーション モードで **logging queue** コマンドを使用します。ロギング キューのサイズをデフォルトの 512 メッセージ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。

logging queue *queue_size*

no logging queue *queue_size*

シンタックスの説明

queue_size	処理前に格納するためのキューに入れることができる syslog メッセージの数。有効な値は 0 ～ 8,192 メッセージです。0 は、キューがブロック メモリの可用性による制限のみを受けることを意味します。

デフォルト

デフォルトのキュー サイズは 512 メッセージです。

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

トラフィックが重いためにキューがいっぱいになった場合、セキュリティ アプライアンスはメッセージを廃棄することがあります。

例

次の例は、**logging queue** コマンドと **show logging queue** コマンドの出力を表示する方法を示しています。

```
hostname(config)# logging queue 0
hostname(config)# show logging queue
Logging Queue length limit : Unlimited
Current 5 msg on queue, 3513 msgs most on queue, 1 msg discard.
```

この例では、**logging queue** コマンドは 0 に設定されています。これは、キューがブロック メモリの可用性によって許容されるだけのメッセージを保持できることを意味します。キュー内の syslog メッセージは、セキュリティ アプライアンスによって、ロギング コンフィギュレーションで示される方法で処理されます。この方法には、syslog メッセージを電子メール受信者に送信することや、フラッシュ メモリに保存することなどがあります。

この例における **show logging queue** コマンドの出力は、キューにあるメッセージが 5 つ、セキュリティ アプライアンスが最後にブートされてから同時にキューに存在したメッセージの最大数が 3,513、廃棄されたメッセージが 1 つであることを表示しています。キューは無制限になるように設定されていましたが、メッセージをキューに追加するためのブロック メモリが使用できなかったため、メッセージは廃棄されました。

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
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。

logging rate-limit

システム ログ メッセージの生成レートを制限するには、**logging rate-limit** コマンドを使用します。レート制限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。

logging rate-limit {***unlimited*** | {*num* [*interval*]}} ***message*** *syslog_id* | ***level*** *severity_level*

[no] logging rate-limit [***unlimited*** | {*num* [*interval*]}} ***message*** *syslog_id*] ***level*** *severity_level*

シンタックスの説明

unlimited	レート制限をディセーブルにします。これは、ロギング レートが制限されないことを意味します。
num	指定した時間間隔が経過するまでに生成できるシステム メッセージの数。*num* の有効値の範囲は 0 ～ 2,147,483,647 です。
interval	（オプション）メッセージの生成レートの測定に使用される時間間隔（秒単位）。*interval* の有効値の範囲は 0 ～ 2,147,483,647 です。
message	このシステム ログ メッセージのレポートを抑制します。
syslog_id	抑制するシステム ログ メッセージの ID。*syslog_id* の有効値の範囲は 100000 ～ 999999 です。
level *severity_level*	重大度を設定します。これを超えると、セキュリティ アプライアンスがメッセージを抑制します。*severity_level* の有効な範囲は 1 ～ 7 です。

デフォルト

interval のデフォルト設定は 1 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 EXEC	•	•	•	•	•

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

システム メッセージの重大度は次のとおりです。

•0：システムが使用不可

•1：ただちに処置が必要

•2：クリティカルな状態

•3：エラー メッセージ

•4：警告メッセージ

•5：正常だが、注意が必要な状態

•6：情報

•7：デバッグ メッセージ

例

次の例は、システム ログ メッセージの生成レートを制限する方法を示しています。

```
hostname(config)# logging rate-limit 5 message 106023
hostname(config)# logging rate-limit 10 60 level 7
```

関連コマンド

コマンド	説明
clear configure logging rate-limit	ロギング レート制限の設定をデフォルトにリセットします。
show logging	内部バッファ内の現在のメッセージ、またはロギング コンフィギュレーションの設定を表示します。
show running-config logging rate-limit	現在のロギング レート制限の設定を表示します。

logging recipient-address

セキュリティ アプライアンスによって電子メールで送信される syslog メッセージの受信者の電子メール アドレスを指定するには、グローバル コンフィギュレーション モードで **logging recipient-address** コマンドを使用します。受信者の電子メール アドレスを削除するには、このコマンドの **no** 形式を使用します。受信者のアドレスは最大 5 つまで設定できます。必要に応じて、受信者のアドレスごとに、**logging mail** コマンドで指定されたメッセージ レベルとは別のレベルを指定できます。

logging recipient-address *address* [**level** *level*]

no logging recipient-address *address* [**level** *level*]

シンタックスの説明

address	syslog メッセージを電子メールで送信する場合の受信者の電子メール アドレスを指定します。
level	この後にロギング レベルが続くことを示します。
level	システム ログ メッセージの最大レベルを設定します。たとえば、レベルを 3 に設定すると、セキュリティ アプライアンスはレベル 3、2、1、および 0 のシステム ログ メッセージを生成します。次の数値または名前で指定できます。 • **0** または **emergencies**：システムが使用不能 • **1** または **alerts**：ただちに処置が必要 • **2** または **critical**：クリティカルな状態 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：正常だが、注意が必要な状態 • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、WWW URL **（注）** **logging recipient-address** コマンドでは、3 より大きなレベルを使用することはお勧めできません。ロギング レベルを高くすると、バッファ オーバーフローによって syslog メッセージがドロップされることがあります。 **logging recipient-address** コマンドで指定されたメッセージ レベルは、**logging mail** コマンドで指定されたメッセージ レベルを上書きします。たとえば、**logging recipient-address** コマンドでレベル 7 が指定された場合、**logging mail** コマンドでレベル 3 が指定されていたときは、セキュリティ アプライアンスはレベル 4、5、6、および 7 のメッセージを含むすべてのメッセージを受信者に送信します。

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。

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
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

syslog メッセージを電子メールで送信できるようにするには、**logging mail** コマンドを使用します。

logging recipient-address コマンドは最大 5 つまで設定できます。コマンドごとに、別々のロギング レベルを指定できます。この方法は、緊急性の高いメッセージを緊急性の低いメッセージよりも多くの受信者に送信する場合に便利です。

例

次の基準に従って、syslog メッセージを電子メールで送信するようにセキュリティ アプライアンスを設定します。

- critical、alerts、および emergencies のメッセージを送信する。
- メッセージを送信するときに、ciscosecurityappliance@example.com を送信者のアドレスとして使用する。
- メッセージを admin@example.com に送信する。
- SMTP を使用して、メッセージをプライマリ サーバ pri-smtp-host およびセカンダリ サーバ sec-smtp-host に送信する。

次のコマンドを入力します。

```
hostname(config)# logging mail critical
hostname(config)# logging from-address ciscosecurityappliance@example.com
hostname(config)# logging recipient-address admin@example.com
hostname(config)# smtp-server pri-smtp-host sec-smtp-host
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging from-address	syslog メッセージ電子メールの送信元として表示する電子メール アドレスを指定します。
logging mail	セキュリティ アプライアンスが syslog メッセージを電子メールで送信できるようにし、どのメッセージを電子メールで送信するかを決定します。
smtp-server	SMTP サーバを設定します。
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	現在動作しているロギング コンフィギュレーションを表示します。

logging savelog

ログ バッファをフラッシュ メモリに保存するには、特権 EXEC モードで **logging savelog** コマンドを使用します。

logging savelog [*savefile*]

シンタックスの説明

savefile	（オプション）保存するフラッシュ メモリ ファイルの名前。ファイル名が指定されない場合、セキュリティ アプライアンスは、次のように、デフォルトのタイムスタンプ形式を使用してファイルを保存します。 `LOG-YYYY-MM-DD-HHMMSS.TXT` *YYYY* は西暦年、*MM* は月、*DD* は日、*HHMMSS* は時刻の時、分、秒です。

デフォルト

デフォルトは次のとおりです。

- バッファのサイズは 4 KB です。
- フラッシュ メモリの最小空き容量は 3 MB です。
- バッファ ロギング用のフラッシュ メモリ最大割当量は、1 MB です。
- デフォルトのログ ファイル名は、上記の表のとおりです。

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 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

ログ バッファをフラッシュ メモリに保存するには、事前にバッファへのロギングをイネーブルにしておく必要があります。このようにしないと、フラッシュ メモリに保存するデータがログ バッファに保持されません。バッファへのロギングをイネーブルにするには、**logging buffered** コマンドを使用します。

（注）　**logging savelog** コマンドは、バッファを消去しません。バッファを消去するには、**clear logging buffer** コマンドを使用します。

例

次の例では、ロギングとログ バッファをイネーブルにし、グローバル コンフィギュレーション モードを終了し、latest-logfile.txt というファイル名を使用してログ バッファをフラッシュ メモリに保存します。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# exit
hostname# logging savelog latest-logfile.txt
hostname#
```

関連コマンド

コマンド	説明
clear logging buffer	保持しているすべての syslog メッセージのログ バッファを消去します。
copy	ファイルを、ある位置から TFTP サーバや FTP サーバなどの別の位置にコピーします。
delete	保存済みログ ファイルなどのファイルを、ディスク パーティションから削除します。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。

logging standby

フェールオーバー スタンバイ セキュリティ アプライアンスがこのセキュリティ アプライアンスの syslog メッセージをロギング先に送信できるようにするには、グローバル コンフィギュレーション モードで **logging standby** コマンドを使用します。syslog および SNMP ロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

logging standby

no logging standby

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

logging standby 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
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

logging standby をイネーブルにすると、フェールオーバーが発生しても、フェールオーバー スタンバイ セキュリティ アプライアンスの syslog メッセージが同期されたままになることが保証されます。

（注） **logging standby** コマンドを使用すると、syslog サーバ、SNMP サーバ、および FTP サーバなどの共有ロギング先に対するトラフィックが 2 倍になります。

例

次の例では、セキュリティ アプライアンスが syslog メッセージをフェールオーバー スタンバイ セキュリティ アプライアンスに送信できるようにします。**show logging** コマンドの出力は、この機能がイネーブルになっていることを示しています。

```
hostname(config)# logging standby
hostname(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: enabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: disabled
    History logging: disabled
    Device ID: 'inside' interface IP address "10.1.1.1"
    Mail logging: disabled
    ASDM logging: disabled
```

関連コマンド

コマンド	説明
フェールオーバー	フェールオーバー機能をイネーブルにします。
logging enable	ロギングをイネーブルにします。
logging host	syslog サーバを定義します。
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。

logging timestamp

syslog メッセージにメッセージの生成日時を含めるよう指定するには、グローバル コンフィギュレーション モードで **logging timestamp** コマンドを使用します。syslog メッセージから日時を削除するには、このコマンドの **no** 形式を使用します。

logging timestamp

no logging timestamp

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

セキュリティ アプライアンスは、デフォルトでは、日時を syslog メッセージに含めません。

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

logging timestamp コマンドは、セキュリティ アプライアンスがすべての syslog メッセージにタイムスタンプを含めるように指定します。

例

次の例では、すべての syslog メッセージにタイムスタンプ情報を含めることをイネーブルにします。

```
hostname(config)# logging enable
hostname(config)# logging timestamp
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
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。

logging trap

セキュリティ アプライアンスが syslog サーバに送信する syslog メッセージを指定するには、グローバル コンフィギュレーション モードで **logging trap** コマンドを使用します。このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

logging trap [*logging_list* | *level*]

no logging trap

シンタックスの説明

level	システム ログ メッセージの最大レベルを設定します。たとえば、レベルを 3 に設定すると、セキュリティ アプライアンスはレベル 3、2、1、および 0 のシステム ログ メッセージを生成します。次の数値または名前で指定できます。 • **0** または **emergencies**：システムが使用不能 • **1** または **alerts**：ただちに処置が必要 • **2** または **critical**：クリティカルな状態 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：正常だが、注意が必要な状態 • **6** または **informational**：情報 • **7** または **debugging**:デバッグ メッセージ、ログ FTP コマンド、WWW URL
logging_list	syslog サーバに送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

デフォルト

デフォルトの syslog トラップは定義されていません。

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

ロギング転送プロトコルとして TCP を使用する場合、セキュリティ アプライアンスが syslog サーバに到達できないとき、syslog サーバが誤って設定されているとき、またはディスクがいっぱいのときは、セキュリティ アプライアンスはセキュリティ保護手段として、新しいネットワーク アクセス セッションを拒否します。

UDP ベースのロギングは、syslog サーバに障害が発生しても、セキュリティ アプライアンスによるトラフィックの送信を妨げません。

例

次の例は、内部インターフェイス上にあってデフォルトのプロトコルとポート番号を使用する syslog サーバに対して、レベル 0、1、2、および 3 の syslog メッセージを送信する方法を示しています。

```
hostname(config)# logging enable
hostname(config)# logging host inside 10.2.2.3
hostname(config)# logging trap errors
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging host	syslog サーバを定義します。
logging list	再使用可能なメッセージ選択基準リストを作成します。
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。

login-message

WebVPN ユーザにログインを求めるメッセージを作成するには、WebVPN モードで **login-message** コマンドを使用します。ログイン メッセージをコンフィギュレーションから削除してデフォルトにリセットするには、このコマンドの **no** 形式を使用します。ログイン メッセージを削除するには、引数を指定しないで **login-message** コマンドを使用します。

login-message [*string***]**

no login-message

シンタックスの説明

string	（オプション）ログイン メッセージの HTML 文字列を指定します。最大 255 文字です。7 ビットの ASCII 値、HTML タグ、およびエスケープ シーケンスを含めることができます。

デフォルト

デフォルトのログイン メッセージは「Please enter your username and password」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
WebVPN　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

次の例は、「Welcome to Our Company. Please enter your username and password」という WebVPN メッセージを作成する方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# login-message Welcome to Our Company. Please enter your
username and password.
```

logo

WebVPN ログイン ページおよびホーム ページに表示するロゴを指定するには、WebVPN モードで **logo** コマンドを使用します。ロゴをコンフィギュレーションから削除してデフォルトにリセットするには、このコマンドの **no** 形式を使用します。ロゴを削除するには、**logo none** コマンドを使用します。指定したファイル名が存在しない場合は、エラーが発生します。ロゴ ファイルを削除した場合、コンフィギュレーションが引き続きそのファイルを指していても、ロゴは表示されません。

logo {**file** *filename* | **none**}

no logo

シンタックスの説明

file *filename*	ロゴ イメージのファイル名を指定します。最大長は 255 文字です。ファイル タイプには JPG、PNG、または GIF を指定し、サイズは 100 KB 未満にする必要があります。
none	ロゴを使用しないことを指定します。ヌル値を設定して、ロゴを拒否します。ロゴを継承しないようにします。

デフォルト

デフォルトは、シスコのロゴです。

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
WebVPN　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

管理者がこのファイルをセキュリティ ゲートウェイにアップロードします。指定したファイルが存在しない場合、セキュリティ アプライアンスはエラーを生成します。

例

次の例は、MyCompanylogo.gif というファイル名で WebVPN ロゴを設定する方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# logo MyCompanylogo.gif
```

logout

CLI を終了するには、ユーザ EXEC モードで **logout** コマンドを使用します。

logout

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
ユーザ 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

logout コマンドを使用すると、セキュリティ アプライアンスからログアウトできます。ユーザ モードに戻るには、**exit** コマンドまたは **quit** コマンドを使用します。

例

次の例は、セキュリティ アプライアンスからログアウトする方法を示しています。

```
hostname> logout
```

関連コマンド

コマンド	説明
login	ログイン プロンプトを開始します。
exit	アクセス モードを終了します。
quit	コンフィギュレーション モードまたは特権モードを終了します。

logout-message

ログアウトするユーザに WebVPN が示すログアウト メッセージを作成するには、WebVPN モードで **logout-message** コマンドを使用します。ログアウト メッセージをコンフィギュレーションから削除してデフォルトにリセットするには、このコマンドの **no** 形式を使用します。ログアウト メッセージを削除するには、引数を指定しないで **logout-message** コマンドを使用します。

logout-message [*string*]

no logout-message

シンタックスの説明

string	（オプション）ログアウト メッセージの HTML 文字列を指定します。最大 255 文字です。7 ビットの ASCII 値、HTML タグ、およびエスケープ シーケンスを含めることができます。

デフォルト

デフォルトのログアウト メッセージは「Goodbye」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
WebVPN　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

次の例は、「Farewell! Be careful crossing the street!」という WebVPN ログアウト メッセージを作成する方法を示しています。

```
hostname(config)# logout-message Farewell!Be careful crossing the street!
```