icmp コマンド～ imap4s コマンド

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 14-1 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。しかし、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 メッセージも拒否します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド 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	変更内容
6.0	このコマンドが導入されました。

使用上のガイドライン

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。しかし、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 トラフィックに対しては、**access-list extended** 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 トラフィックを最初に照合し、そのインターフェイス上のそれ以外の 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 アプライアンスはその 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見なされます。

表 14-1 に、使用できる ICMP タイプ値を示します。

表 14-1　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

表 14-1　ICMP タイプのリテラル（続き）

ICMP タイプ	リテラル
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
```

ICMP トラフィックを拒否する追加インターフェイスそれぞれに対して、続けて **icmp deny any** *interface* コマンドを入力します。

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 モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド 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	変更内容
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**
9	**router-advertisement**
10	**router-solicitation**
11	**time-exceeded**
12	**parameter-problem**
13	**timestamp-request**
14	**timestamp-reply**
15	**information-request**

番号	ICMP タイプの名前
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 モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド 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	変更内容
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。

id-mismatch

過度の DNS ID ミスマッチのロギングをイネーブルにするには、パラメータ コンフィギュレーション モードで **id-mismatch** 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。

id-mismatch [**count** *number* **duration** *seconds*] **action log**

no id-mismatch [**count** *number* **duration** *seconds*] [**action log**]

シンタックスの説明

count *number*	システム メッセージ ログが送信される前のミスマッチ インスタンスの最大数。
duration *seconds*	監視する期間（秒）。

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。コマンドがイネーブルで、オプションが指定されていない場合、デフォルト レートは最大数が 30 で、期間は 3 秒間です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.2(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

ハイレートの DNS ID ミスマッチはキャッシュ ポイズニング攻撃を示す場合があります。このコマンドをイネーブルにすると、そうした試みを監視して警告します。ミスマッチ レートが設定値を超えると、システム メッセージの要約ログが出力されます。**id-mismatch** コマンドは通常のイベントベースのシステム メッセージ ログに関する詳細をシステム管理者に提供します。

例

次の例では、DNS 検査ポリシー マップで ID ミスマッチをイネーブルにする方法を示しています。

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# id-mismatch action log
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

id-randomization

DNS クエリーの DNS ID をランダム化するには、パラメータ コンフィギュレーション モードで **id-randomization** 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。

id-randomization

no id-randomization

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

デフォルトではディセーブルです。DNS クエリーからの DNS ID は変更されません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.2(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

ID のランダム化は、キャッシュ ポイズニング攻撃に対する保護に役立ちます。

例

次の例では、DNS 検査ポリシー マップで ID のランダム化をイネーブルにする方法を示しています。

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# id-randomization
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

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 モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド 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	変更内容
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ている受信者、および IGMP を通じてラーニングされた受信者を持つマルチキャスト 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。しかし、拡張アクセス リストを指定した場合、照合され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 モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド 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	変更内容
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 モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド 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	変更内容
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 モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド 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	変更内容
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 モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド 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	変更内容
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、インターフェイスにおける IGMP の状態の数を 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 モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド 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	変更内容
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 モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド 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	変更内容
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 モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド 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	変更内容
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 モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド 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	変更内容
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 モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド 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	変更内容
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 モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド 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	変更内容
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。

im

SIP 経由のインスタント メッセージをイネーブルにするには、パラメータ コンフィギュレーション モードで **im** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

im

no im

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 モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、SIP 検査ポリシー マップで SIP 経由のインスタント メッセージをイネーブルにする方法を示します。

```
hostname(config)# policy-map type inspect sip sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# im
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

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 モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド 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	変更内容
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。