CHAPTER 4

D ～ F のコマンド

debug aaa

AAA に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug aaa** コマンドを使用します。AAA メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug aaa [***accounting*** | ***authentication*** | ***authorization*** | ***internal*** | ***vpn*** [*level*]]

no debug aaa

シンタックスの説明

accounting	（オプション）アカウンティングに関するデバッグ メッセージだけを表示します。
authentication	（オプション）認証に関するデバッグ メッセージだけを表示します。
authorization	（オプション）認可に関するデバッグ メッセージだけを表示します。
internal	（オプション）ローカル データベースだけでサポートされる AAA 機能に関するデバッグ メッセージを表示します。
level	（オプション）デバッグ レベルを指定します。**vpn** キーワードと共に使用する場合だけ有効です。
vpn	（オプション）VPN 関連の AAA 機能に関するデバッグ メッセージだけを表示します。

デフォルト

デフォルトのレベルは、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	このコマンドは、新しいキーワードを含めるように修正されました。

使用上のガイドライン

debug aaa コマンドは、AAA アクティビティに関する詳細な情報を表示します。**no debug all** コマンドまたは **undebug all** コマンドは、イネーブルなデバッグをすべてオフにします。

例

次の例では、ローカル データベースでサポートされる AAA 機能のデバッグをイネーブルにします。

```
hostname(config)# debug aaa internal
debug aaa internal enabled at level 1
hostname(config)# uap allocated. remote address: 10.42.15.172, Session_id: 2147483841
uap freed for user . remote address: 10.42.15.172, session id: 2147483841
```

関連コマンド

コマンド	説明
show running-config aaa	AAA に関連する実行コンフィギュレーションを表示します。

debug arp

ARP に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug arp** コマンドを使用します。ARP に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug arp

no debug arp

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークのトラフィックが遅くなる可能性があります。

例

次の例では、ARP に関するデバッグ メッセージをイネーブルにします。

```
hostname# debug arp
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
show arp statistics	ARP 統計情報を表示します。
show debug	イネーブルなデバッガをすべて表示します。

debug arp-inspection

ARP 検査に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug arp-inspection** コマンドを使用します。ARP 検査に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug arp-inspection

no debug arp-inspection

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークのトラフィックが遅くなる可能性があります。

例

次の例では、ARP 検査に関するデバッグ メッセージをイネーブルにします。

```
hostname# debug arp-inspection
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
arp-inspection	透過 ファイアウォール モードで、ARP パケットを調べて ARP スプーフィングを防止します。
show debug	イネーブルなデバッガをすべて表示します。

debug asdm history

ASDM のデバッグ情報を表示するには、特権 EXEC モードで **debug asdm history** コマンドを使用します。

debug asdm history *level*

シンタックスの説明

level	（オプション）デバッグ レベルを指定します。

デフォルト

デフォルトのレベルは、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	このコマンドは、**debug pdm history** コマンドから **debug asdm history** コマンドに変更されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカルサポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、ASDM に関するレベル 1 のデバッグをイネーブルにします。

```
hostname# debug asdm history
debug asdm history enabled at level 1

hostname#
```

関連コマンド

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

debug cmgr

SSM カード マネージャに関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug cmgr** コマンドを使用します。カード マネージャに関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug cmgr [*level*]

no debug cmgr [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

デフォルトのレベルは、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	このコマンドが導入されました。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークのトラフィックが遅くなる可能性があります。

例

次の例では、カード マネージャに関するデバッグ メッセージをイネーブルにします。

```
hostname# debug cmgr
```

関連コマンド

コマンド	説明
hw-module module recover	TFTP サーバからリカバリ イメージをロードすることにより、AIP SSM を回復します。
hw-module module reset	AIP SSM をシャットダウンし、ハードウェア リセットを実行します。
hw-module module reload	AIP SSM ソフトウェアをリロードします。
hw-module module shutdown	コンフィギュレーション データを失わずに電源を切るため、AIP SSM ソフトウェアをシャットダウンします。
show module	SSM 情報を表示します。

debug context

セキュリティ コンテキストを追加または削除する際にデバッグ メッセージを表示するには、特権 EXEC モードで **debug context** コマンドを使用します。コンテキストに関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug context [*level*]

no debug context [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

デフォルトのレベルは、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	このコマンドが導入されました。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークのトラフィックが遅くなる可能性があります。

例

次の例では、コンテキスト管理に関するデバッグ メッセージをイネーブルにします。

```
hostname# debug context
```

関連コマンド

コマンド	説明
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードに入ります。
show context	コンテキスト情報を表示します。
show debug	イネーブルなデバッガをすべて表示します。

debug cplane

SSM に内部的に接続するコントロール プレーンに関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug cplane** コマンドを使用します。制御プレーンに関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug cplane [*level*]

no debug cplane [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

デフォルトのレベルは、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	このコマンドが導入されました。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークのトラフィックが遅くなる可能性があります。

例

次の例では、コントロール プレーンに関するデバッグ メッセージをイネーブルにします。

```
hostname# debug cplane
```

関連コマンド

コマンド	説明
hw-module module recover	TFTP サーバからリカバリ イメージをロードすることにより、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、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	コンフィギュレーション データを失わずに電源を切るため、SSM ソフトウェアをシャットダウンします。
show module	SSM 情報を表示します。

debug crypto ca

CA で使用する PKI アクティビティに関するデバッグ メッセージを表示するには、特権 EXEC モードで **ebug crypto ca** コマンドを使用します。PKI に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug crypto ca [**messages** | **transactions**] [*level*]

no debug crypto ca [**messages** | **transactions**] [*level*]

シンタックスの説明

messages	（オプション）PKI の入力および出力メッセージに関するデバッグ メッセージだけを表示します。
transactions	（オプション）PKI トランザクションに関するデバッグ メッセージだけを表示します。
level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。レベル 1（デフォルト）では、エラーが発生した場合にだけメッセージが表示されます。レベル 2 では、警告が表示されます。レベル 3 では、情報メッセージが表示されます。レベル 4 以上では、トラブルシューティングのための追加情報が表示されます。

デフォルト

デフォルトでは、このコマンドはすべてのデバッグ メッセージを表示します。デフォルトのレベルは、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
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

debug コマンドを使用すると、通信量の多いネットワークのトラフィックが遅くなる可能性があります。

例

次の例では、PKI に関するデバッグ メッセージをイネーブルにします。

```
hostname# debug crypto ca
```

関連コマンド

コマンド	説明
debug crypto engine	暗号化エンジンに関するデバッグ メッセージを表示します。
debug crypto ipsec	IPSec に関するデバッグ メッセージを表示します。
debug crypto isakmp	ISAKMP に関するデバッグ メッセージを表示します。

debug crypto engine

暗号化エンジンに関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug crypto engine** コマンドを使用します。暗号化エンジンに関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug crypto engine [*level*]

no debug crypto engine [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

デフォルトのレベルは、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	このコマンドが導入されました。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークのトラフィックが遅くなる可能性があります。

例

次の例では、暗号化エンジンに関するデバッグ メッセージをイネーブルにします。

```
hostname# debug crypto engine
```

関連コマンド

コマンド	説明
debug crypto ca	CA に関するデバッグ メッセージを表示します。
debug crypto ipsec	IPSec に関するデバッグ メッセージを表示します。
debug crypto isakmp	ISAKMP に関するデバッグ メッセージを表示します。

debug crypto ipsec

IPSec に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug crypto ipsec** コマンドを使用します。IPSec に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug crypto ipsec [*level*]

no debug crypto ipsec [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

デフォルトのレベルは、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
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

debug コマンドを使用すると、通信量の多いネットワークのトラフィックが遅くなる可能性があります。

例

次の例では、IPSec に関するデバッグ メッセージをイネーブルにします。

```
hostname# debug crypto ipsec
```

関連コマンド

コマンド	説明
debug crypto ca	CA に関するデバッグ メッセージを表示します。
debug crypto engine	暗号化エンジンに関するデバッグ メッセージを表示します。
debug crypto isakmp	ISAKMP に関するデバッグ メッセージを表示します。

debug crypto isakmp

ISAKMP に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug crypto isakmp** コマンドを使用します。ISAKMP に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug crypto isakmp [**timers**] [*level*]

no debug crypto isakmp [**timers**] [*level*]

シンタックスの説明

timers	（オプション）ISAKMP タイマーの期限切れに関するデバッグ メッセージを表示します。
level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。レベル 1（デフォルト）では、エラーが発生した場合にだけメッセージが表示されます。レベル 2 ～ 7 では、追加情報が表示されます。レベル 254 では、復号化された ISAKMP パケットが、読み取り可能な形式で表示されます。レベル で 255 は、復号化された ISAKMP パケットの 16 進形式のダンプが表示されます。

デフォルト

デフォルトのレベルは、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
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

debug コマンドを使用すると、通信量の多いネットワークのトラフィックが遅くなる可能性があります。

例

次の例では、ISAKMP に関するデバッグ メッセージをイネーブルにします。

```
hostname# debug crypto isakmp
```

関連コマンド

コマンド	説明
debug crypto ca	CA に関するデバッグ メッセージを表示します。
debug crypto engine	暗号化エンジンに関するデバッグ メッセージを表示します。
debug crypto ipsec	IPSec に関するデバッグ メッセージを表示します。

debug ctiqbe

CTIQBE アプリケーション検査に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug ctiqbe** コマンドを使用します。CTIQBE アプリケーション検査に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug ctiqbe [*level*]

no debug ctiqbe [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 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
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

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。デバッグ メッセージがすべて表示されないようにするには、**no debug all** コマンドを入力します。

（注）　**debug ctiqbe** コマンドをイネーブルにすると、通信量の多いネットワークでは、トラフィックの速度が遅くなります。

例

次の例では、CTIQBE アプリケーション検査に関するデバッグ メッセージをデフォルトのレベル（1）でイネーブルにします。

```
hostname# debug ctiqbe
```

関連コマンド

コマンド	説明
inspect ctiqbe	CTIQBE アプリケーション検査をイネーブルにします。
show ctiqbe	セキュリティ アプライアンスを介して確立された CTIQBE 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。

debug dhcpc

DHCP クライアントのデバッグをイネーブルにするには、特権 EXEC モードで **debug dhcpc** コマンドを使用します。デバッ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。

debug dhcpc {***detail*** | ***packet*** | ***error***} [*level*]

no debug dhcpc {***detail*** | ***packet*** | ***error***} [*level*]

シンタックスの説明

detail	DHCP クライアントに関連する詳細なイベント情報を表示します。
error	DHCP クライアントに関連するエラー メッセージを表示します。
level	（オプション）デバッグ レベルを指定します。有効な値は 1 ～ 255 です。
packet	DHCP クライアントに関連するパケット情報を表示します。

デフォルト

デフォルトのデバッグ レベルは、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
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

DHCP クライアントのデバッグ情報を表示します。

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカルサポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、DHCP クライアントに関するデバッグをイネーブルにする方法を示しています。

```
hostname# debug dhcpc detail 5
debug dhcpc detail enabled at level 5
```

関連コマンド

コマンド	説明
show ip address dhcp	インターフェイスの DHCP リースに関する詳細な情報を表示します。
show running-config interface	指定されたインターフェイスの実行コンフィギュレーションを表示します。

debug dhcpd

DHCP サーバのデバッグをイネーブルにするには、特権 EXEC モードで **debug dhcpd** コマンドを使用します。デバッ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。

debug dhcpd {***event*** | ***packet***} [*level*]

no debug dhcpd {***event*** | ***packet***} [*level*]

シンタックスの説明

event	DHCP サーバに関連するイベント情報を表示します。
level	（オプション）デバッグ レベルを指定します。有効な値は 1 ～ 255 です。
packet	DHCP サーバに関連するパケット情報を表示します。

デフォルト

デフォルトのデバッグ レベルは、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
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

debug dhcpd event コマンドは、DHCP サーバに関するイベント情報を表示します。**debug dhcpd packet** コマンドは、DHCP サーバに関するパケット情報を表示します。

debug dhcpd コマンドの **no** 形式を使用して、デバッグをディセーブルにします。

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカルサポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、DHCP イベント デバッグをイネーブルにします。

```
hostname# debug dhcpd event
debug dhcpd event enabled at level 1
```

関連コマンド

コマンド	説明
show dhcpd	DHCP のバインディング、統計情報、または状態情報を表示します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

debug dhcprelay

DHCP リレー サーバのデバッグをイネーブルにするには、特権 EXEC モードで **debug dhcpreleay** コマンドを使用します。デバッ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。

debug dhcprelay {***event*** | ***packet*** | ***error***} [*level*]

no debug dhcprelay {***event*** | ***packet*** | ***error***} [*level*]

シンタックスの説明

error	DHCP リレー エージェントに関連するエラー メッセージを表示します。
event	DHCP リレー エージェントに関連するイベント情報を表示します。
level	（オプション）デバッグ レベルを指定します。有効な値は 1 ～ 255 です。
packet	DHCP リレー エージェントに関連するパケット情報を表示します。

デフォルト

デフォルトのデバッグ レベルは、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
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

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカルサポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例は、DHCP リレー エージェントのエラー メッセージのデバッグをイネーブルにする方法を示しています。

```
hostname# debug dhcprelay error
debug dhcprelay error enabled at level 1
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
clear dhcprelay statistics	DHCP リレー エージェント統計情報カウンタをクリアします。
show dhcprelay statistics	DHCP リレー エージェントの統計情報を表示します。
show running-config dhcprelay	現在の DHCP リレー エージェント コンフィギュレーションを表示します。

debug disk

ファイル システムのデバッグ情報を表示するには、特権 EXEC モードで **debug disk** コマンドを使用します。デバッグ情報の表示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。

debug disk {***file*** | ***file-verbose*** | ***filesystem***} [*level*]

no debug disk {***file*** | ***file-verbose*** | ***filesystem***}

シンタックスの説明

file	ファイル レベルでのディスクのデバッグ メッセージをイネーブルにします。
file-verbose	ファイル レベルでの詳細なディスクのデバッグ メッセージをイネーブルにします。
filesystem	ファイル システムのデバッグ メッセージをイネーブルにします。
level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 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	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカルサポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、ファイル レベルでのディスクのデバッグ メッセージをイネーブルにします。**show debug** コマンドは、ファイル レベルでのディスク デバッグ メッセージがイネーブルになっていることを示します。**dir** コマンドを実行すると、いくつかのデバッグ メッセージが作成されます。

```
hostname# debug disk file
debug disk file enabled at level 1
hostname# show debug
debug vpn-sessiondb  enabled at level 1
hostname# dir
IFS: Opening: file flash:/, flags 1, mode 0
IFS: Opened: file flash:/ as fd 3
IFS: Getdent: fd 3
IFS: Getdent: fd 3
IFS: Getdent: fd 3
IFS: Getdent: fd 3

Directory of flash:/
IFS: Close: fd 3
IFS: Opening: file flash:/, flags 1, mode 0

4      -rw-  5124096     14:42:27 Apr 04 2005  cdisk.binIFS: Opened: file flash:/ as
fd 3

9      -rw-  5919340     14:53:39 Apr 04 2005  ASDMIFS: Getdent: fd 3

11     drw-  0           15:18:56 Apr 21 2005  syslog
IFS: Getdent: fd 3
IFS: Getdent: fd 3
IFS: Getdent: fd 3
IFS: Close: fd 3

16128000 bytes total (5047296 bytes free)
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug dns

DNS に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug dns** コマンドを使用します。DNS に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug dns [***resolver*** | ***all***] [*level*]

no debug dns [***resolver*** | ***all***] [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。
resolver	（オプション）DNS リゾルバ メッセージだけを表示します。
all	（デフォルト）DNS キャッシュに関するメッセージを含む、すべてのメッセージを表示します。

デフォルト

デフォルトのレベルは、1 です。キーワードを指定しない場合、セキュリティ アプライアンスはすべてのメッセージを表示します。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークのトラフィックが遅くなる可能性があります。

例

次の例では DNS のデバッグ メッセージをイネーブルにします。

```
hostname# debug dns
```

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。
inspect dns	DNS アプリケーション検査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。

debug entity

管理情報ベース（MIB）のデバッグ情報を表示するには、特権 EXEC モードで **debug entity** コマンドを使用します。デバッグ情報の表示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。

debug entity [*level*]

no debug entity

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 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	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカルサポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、MIB デバッグ メッセージをイネーブルにします。**show debug** コマンドは、MIB デバッグ メッセージがイネーブルになっていることを示します。

```
hostname# debug entity
debug entity  enabled at level 1
hostname# show debug
debug entity  enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug fixup

アプリケーション検査に関する詳細情報を表示するには、特権 EXEC モードで **debug fixup** コマンドを使用します。デバッ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。

debug fixup

no debug fixup

デフォルト

デフォルトでは、すべてのオプションが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
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

debug fixup コマンドは、アプリケーション検査に関する詳細情報を表示します。**no debug all** コマンドまたは **undebug all** コマンドは、イネーブルなデバッグをすべてオフにします。

例

次の例では、アプリケーション検査に関する詳細情報の表示をイネーブルにします。

```
hostname# debug fixup
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
inspect *protocol*	特定のプロトコルに関するアプリケーション検査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。

debug fover

フェールオーバーのデバッグ情報を表示するには、特権 EXEC モードで **debug fover** コマンドを使用します。デバッグ情報の表示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。

debug fover {***cable*** | ***fail*** | ***fmsg*** | ***ifc*** | ***open*** | ***rx*** | ***rxdmp*** | ***rxip*** | ***switch*** | ***sync*** | ***tx*** | ***txdmp*** | ***txip*** | ***verify***}

no debug fover {***cable*** | ***fail*** | ***fmsg*** | ***ifc*** | ***open*** | ***rx*** | ***rxdmp*** | ***rxip*** | ***switch*** | ***sync*** | ***tx*** | ***txdmp*** | ***txip*** | ***verify***}

シンタックスの説明

cable	フェールオーバーの LAN ステータスまたはシリアル ケーブル ステータス
fail	フェールオーバー内部例外
fmsg	フェールオーバー メッセージ
ifc	ネットワーク インターフェイス ステータス トレース
open	フェールオーバー デバイス オープン
rx	フェールオーバー メッセージ受信
rxdmp	フェールオーバー受信メッセージ ダンプ（シリアル コンソールのみ）
rxip	IP ネットワーク フェールオーバー パケット受信
switch	フェールオーバー スイッチング ステータス
sync	フェールオーバー コンフィギュレーション、またはコマンド複製
tx	フェールオーバー メッセージ送信
txdmp	フェールオーバー送信メッセージ ダンプ（シリアル コンソールのみ）
txip	IP ネットワーク フェールオーバー パケット送信
verify	フェールオーバー メッセージの確認

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	このコマンドが変更されました。このコマンドには、追加のデバッグ キーワードが含まれています。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカルサポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例は、フェールオーバー コマンド複製のデバッグ情報を表示する方法を示しています。

```
hostname# debug fover sync
fover event trace on
```

関連コマンド

コマンド	説明
show failover	フェールオーバー コンフィギュレーションに関する情報および動作統計情報を表示します。

debug fsm

FSM のデバッグ情報を表示するには、特権 EXEC モードで **debug fsm** コマンドを使用します。デバッグ情報の表示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。

debug fsm [*level*]

no debug fsm

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 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	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカルサポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、FSM デバッグ メッセージをイネーブルにします。**show debug** コマンドは、FSM デバッグ メッセージがイネーブルになっていることを示します。

```
hostname# debug fsm
debug fsm  enabled at level 1
hostname# show debug
debug fsm  enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug ftp client

FTP に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug ftp client** コマンドを使用します。FTP に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug ftp client [*level*]

no debug ftp client [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 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
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

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。デバッグ メッセージがすべて表示されないようにするには、**no debug all** コマンドを入力します。

（注）　**debug ftp client** コマンドをイネーブルにすると、通信量の多いネットワークでは、トラフィックの速度が遅くなります。

例

次の例では、FTP のデバッグ メッセージをデフォルトのレベル（1）でイネーブルにします。

```
hostname# debug ftp client
```

関連コマンド

コマンド	説明
copy	イメージ ファイルまたはコンフィギュレーション ファイルを FTP サーバとの間でアップロードまたはダウンロードします。
ftp mode passive	FTP セッションのモードを設定します。
show running-config ftp mode	FTP クライアントのコンフィギュレーションを表示します。

debug generic

その他のデバッグ情報を表示するには、特権 EXEC モードで **debug generic** コマンドを使用します。その他のデバッグ情報の表示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。

debug generic [*level*]

no debug generic

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 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	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカルサポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、その他のデバッグ メッセージをイネーブルにします。**show debug** コマンドは、その他のデバッグ メッセージがイネーブルになっていることを示します。

```
hostname# debug generic
debug generic  enabled at level 1
hostname# show debug
debug generic  enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug gtp

GTP 検査に関する詳細情報を表示するには、特権 EXEC モードで **debug gtp** コマンドを使用します。デバッ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。

debug gtp [**error** | **event** | **ha** | **parser**]

no debug gtp [**error** | **event** | **ha** | **parser**]

シンタックスの説明

error	（オプション）GTP メッセージの処理中に発生したエラーのデバッグ情報を表示します。
event	（オプション）GTP イベントのデバッグ情報を表示します。
ha option	（オプション）GTP HA イベントに関する情報をデバッグします。
parser	（オプション）GTP メッセージの解析のデバッグ情報を表示します。

デフォルト

デフォルトでは、すべてのオプションが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
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

使用上のガイドライン

debug gtp コマンドは、GTP 検査に関する詳細情報を表示します。**no debug all** コマンドまたは **undebug all** コマンドは、イネーブルなデバッグをすべてオフにします。

（注）　GTP 検査には、特別なライセンスが必要です。

例

次の例では、GTP 検査に関する詳細情報の表示をイネーブルにします。

```
hostname# debug gtp
```

関連コマンド

コマンド	説明
clear service-policy inspect gtp	グローバル GTP 統計情報を消去します。
gtp-map	GTP マップを定義し、GTP マップ コンフィギュレーション モードをイネーブルにします。
inspect gtp	アプリケーション検査用に GTP マップを適用します。
show service-policy inspect gtp	GTP コンフィギュレーションを表示します。
show running-config gtp-map	設定されている GTP マップを表示します。

debug h323

H.323 に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug h323** コマンドを使用します。H.323 に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug h323 {h225 | h245 | ras} [asn | event]

no debug h323 {h225 | h245 | ras} [asn | event]

シンタックスの説明

h225	H.225 シグナリングを指定します。
h245	H.245 シグナリングを指定します。
ras	登録、許可、およびステータスのプロトコルを指定します。
asn	（オプション）デコードされたプロトコル データ ユニット（PDU）の出力を表示します。
event	（オプション）H.245 シグナリングのイベントを表示するか、両方のトレースをオンにします。

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
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

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。デバッグ メッセージがすべて表示されないようにするには、**no debug all** コマンドを入力します。

（注）　**debug h323** コマンドをイネーブルにすると、通信量の多いネットワークでは、トラフィックの速度が遅くなります。

例

次の例では、H.225 シグナリングのデバッグ メッセージをデフォルトのレベル（1）でイネーブルにします。

```
hostname# debug h323 h225
```

関連コマンド

コマンド	説明
inspect h323	H.323 アプリケーション検査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。

debug http

HTTP トラフィックに関する詳細情報を表示するには、特権 EXEC モードで **debug http** コマンドを使用します。デバッ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。

debug http [*level*]

no debug http [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 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	このコマンドが導入されました。

使用上のガイドライン

debug http コマンドは、HTTP トラフィックに関する詳細情報を表示します。**no debug all** コマンドまたは **undebug all** コマンドは、イネーブルなデバッグをすべてオフにします。

例

次の例では、HTTP トラフィックに関する詳細情報の表示をイネーブルにします。

```
hostname# debug http
```

関連コマンド

コマンド	説明
http	セキュリティ アプライアンスの内部の HTTP サーバにアクセス可能なホストを指定します。
http-proxy	HTTP プロキシ サーバを設定します。
http redirect	HTTP トラフィックを HTTPS にリダイレクトします。
http server enable	セキュリティ アプライアンス HTTP サーバをイネーブルにします。

debug http-map

HTTP アプリケーション検査マップに関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug http-map** コマンドを使用します。HTTP アプリケーション検査に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug http-map

no debug http-map

デフォルト

level のデフォルト値は 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	このコマンドが導入されました。

使用上のガイドライン

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。デバッグ メッセージがすべて表示されないようにするには、**no debug all** コマンドを入力します。

（注）　**debug http-map** コマンドをイネーブルにすると、通信量の多いネットワークでは、トラフィックの速度が遅くなります。

例

次の例では、HTTP アプリケーション検査のデバッグ メッセージをデフォルトのレベル（1）でイネーブルにします。

```
hostname# debug http-map
```

関連コマンド

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

debug icmp

ICMP 検査に関する詳細情報を表示するには、特権 EXEC モードで **debug icmp** コマンドを使用します。デバッ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。

debug icmp trace [*level*]

no debug icmp trace [*level*]

シンタックスの説明

trace	ICMP トレース アクティビティのデバッグ情報を表示します。
level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

すべてのオプションが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
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

使用上のガイドライン

debug icmp コマンドは、ICMP 検査に関する詳細情報を表示します。**no debug all** コマンドまたは **undebug all** コマンドは、イネーブルなデバッグをすべてオフにします。

例

次の例では、ICMP 検査に関する詳細情報の表示をイネーブルにします。

```
hostname# debug icmp
```

関連コマンド

コマンド	説明
clear configure icmp	ICMP コンフィギュレーションを消去します。
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。
show conn	さまざまなプロトコルおよびセッション タイプの、セキュリティ アプライアンスを介した接続状態を表示します。
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。

debug igmp

IGMP のデバッグ情報を表示するには、特権 EXEC モードで **debug igmp** コマンドを使用します。デバッグ情報の表示を停止するには、このコマンドの **no** 形式を使用します。

debug igmp [***group*** *group_id* | ***interface*** *if_name*]

no debug igmp [***group*** *group_id* | ***interface*** *if_name*]

シンタックスの説明

group *group_id*	指定されたグループの IGMP デバッグ情報を表示します。
interface *if_name*	指定されたインターフェイスの IGMP デバッグ情報を表示します。

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
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

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカルサポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次に、**debug igmp** コマンドの出力例を示します。

```
hostname#debug igmp

IGMP debugging is on
IGMP: Received v2 Query on outside from 192.168.3.2
IGMP: Send v2 general Query on dmz
IGMP: Received v2 Query on dmz from 192.168.4.1
IGMP: Send v2 general Query on outside
IGMP: Received v2 Query on outside from 192.168.3.1
IGMP: Send v2 general Query on inside
IGMP: Received v2 Query on inside from 192.168.1.1
IGMP: Received v2 Report on inside from 192.168.1.6 for 224.1.1.1
IGMP: Updating EXCLUDE group timer for 224.1.1.1
```

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。

debug ils

ILS に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug ils** コマンドを使用します。ILS に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug ils [*level*]

no debug ils [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 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
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

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。デバッグ メッセージがすべて表示されないようにするには、**no debug all** コマンドを入力します。

（注）　**debug ils**　コマンドをイネーブルにすると、通信量の多いネットワークでは、トラフィックの速度が遅くなります。

例

次の例では、ILS アプリケーション検査のデバッグ メッセージをデフォルトのレベル（1）でイネーブルにします。

```
hostname# debug ils
```

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。
inspect ils	ILS アプリケーション検査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。

debug imagemgr

Image Manager のデバッグ情報を表示するには、特権 EXEC モードで **debug imagemgr** コマンドを使用します。デバッグ情報の表示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。

debug imagemgr [*level*]

no debug imagemgr

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 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	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカルサポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、Image Manager デバッグ メッセージをイネーブルにします。**show debug** コマンドは、Image Manager のデバッグ メッセージがイネーブルになっていることを示します。

```
hostname# debug imagemgr
debug imagemgr  enabled at level 1
hostname# show debug
debug imagemgr  enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug ipsec-over-tcp

IPSec-over-TCP のデバッグ情報を表示するには、特権 EXEC モードで **debug ipsec-over-tcp** コマンドを使用します。デバッグ情報の表示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。

debug ipsec-over-tcp [*level*]

no debug ipsec-over-tcp

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 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	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカルサポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、IPSec-over-TCP のデバッグ メッセージをイネーブルにします。**show debug** コマンドは、IPSec-over-TCP のデバッグ メッセージがイネーブルになっていることを示します。

```
hostname# debug ipsec-over-tcp
debug ipsec-over-tcp  enabled at level 1
hostname# show debug
debug ipsec-over-tcp  enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug ipv6

ipv6 のデバッグ メッセージを表示するには、特権 EXEC モードで **debug ipv6** コマンドを使用します。デバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug ipv6 {***icmp*** | ***interface*** | ***nd*** | ***packet*** | ***routing***}

no debug ipv6 {***icmp*** | ***interface*** | ***nd*** | ***packet*** | ***routing***}

シンタックスの説明

icmp	ICMPv6 近隣探索トランザクションを除外した、IPv6 ICMP トランザクションに関するデバッグ メッセージを表示します。
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。
nd	ICMPv6 近隣探索トランザクションに関するデバッグ メッセージを表示します。
packet	IPv6 パケットに関するデバッグ メッセージを表示します。
routing	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。

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	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカルサポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次に、**debug ipv6 icmp** コマンドの出力例を示します。

```
hostname# debug ipv6 icmp
13:28:40:ICMPv6:Received ICMPv6 packet from 2000:0:0:3::2, type 136
13:28:45:ICMPv6:Received ICMPv6 packet from FE80::203:A0FF:FED6:1400, type 135
13:28:50:ICMPv6:Received ICMPv6 packet from FE80::203:A0FF:FED6:1400, type 136
13:28:55:ICMPv6:Received ICMPv6 packet from FE80::203:A0FF:FED6:1400, type 135
```

関連コマンド

コマンド	説明
ipv6 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 メッセージのアクセス規則を設定します。
ipv6 address	IPv6 アドレスに対するインターフェイスを設定します。
ipv6 nd dad attempts	重複アドレスの検出中に実行される、近隣探索の試行回数を定義します。
ipv6 route	IPv6 ルーティング テーブルにスタティック エントリを定義します。

debug iua-proxy

個々のユーザ認証（IUA）プロキシのデバッグ情報を表示するには、特権 EXEC モードで **debug iua-proxy** コマンドを使用します。デバッグ情報の表示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。

debug iua-proxy [*level*]

no debug iua-proxy

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 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	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカルサポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、IUA プロキシのデバッグ メッセージをイネーブルにします。**show debug** コマンドは、IUA プロキシのデバッグ メッセージがイネーブルになっていることを示します。

```
hostname# debug iua-proxy
debug iua-proxy  enabled at level 1
hostname# show debug
debug iua-proxy  enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug kerberos

Kerberos 認証のデバッグ情報を表示するには、特権 EXEC モードで **debug kerberos** コマンドを使用します。デバッグ情報の表示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。

debug kerberos [*level*]

no debug kerberos

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 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	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカルサポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、Kerberos のデバッグ メッセージをイネーブルにします。**show debug** コマンドは、Kerberos のデバッグ メッセージがイネーブルになっていることを示します。

```
hostname# debug kerberos
debug kerberos  enabled at level 1
hostname# show debug
debug kerberos  enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug ldap

LDAP のデバッグ情報を表示するには、特権 EXEC モードで **debug ldap** コマンドを使用します。デバッグ情報の表示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。

debug ldap [*level*]

no debug ldap

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 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	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカルサポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、LDAP のデバッグ メッセージをイネーブルにします。**show debug** コマンドは、LDAP のデバッグ メッセージがイネーブルになっていることを示します。

```
hostname# debug ldap
debug ldap  enabled at level 1
hostname# show debug
debug ldap  enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug mac-address-table

MAC アドレス テーブルに関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug mac-address-table** コマンドを使用します。MAC アドレス テーブルに関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug mac-address-table [*level*]

no debug mac-address-table [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

デフォルトのレベルは、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	このコマンドが導入されました。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークのトラフィックが遅くなる可能性があります。

例

次の例では、MAC アドレス テーブルのデバッグ メッセージをイネーブルにします。

```
hostname# debug mac-address-table
```

関連コマンド

コマンド	説明
mac-address-table aging-time	ダイナミック MAC アドレス エントリのタイムアウトを設定します。
mac-address-table static	MAC アドレス テーブルにスタティック MAC アドレス エントリを追加します。
mac-learn	MAC アドレス ラーニングをディセーブルにします。
show debug	イネーブルなデバッガをすべて表示します。
show mac-address-table	MAC アドレス テーブルのエントリを表示します。

debug menu

特定機能の詳細なデバッグ情報を表示するには、特権 EXEC モードで **debug menu** コマンドを使用します。

debug menu

注意　**debug menu** コマンドは、シスコのテクニカルサポート スタッフの指導の下で使用する必要があります。

シンタックスの説明

このコマンドは、シスコ テクニカルサポート スタッフの指導の下で使用する必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカルサポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

このコマンドは、シスコ テクニカルサポート スタッフの指導の下で使用する必要があります。

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug mfib

MFIB のデバッグ情報を表示するには、特権 EXEC モードで **debug mfib** コマンドを使用します。デバッグ情報の表示を停止するには、このコマンドの **no** 形式を使用します。

debug mfib {***db*** | ***init*** | ***mrib*** | ***pak*** | ***ps*** | ***signal***} [*group*]

no debug mfib {***db*** | ***init*** | ***mrib*** | ***pak*** | ***ps*** | ***signal***} [*group*]

シンタックスの説明

db	（オプション）ルート データベース動作のデバッグ情報を表示します。
group	（オプション）マルチキャスト グループの IP アドレス。
init	（オプション）システムの初期化アクティビティを表示します。
mrib	（オプション）MRIB との通信のデバッグ情報を表示します。
pak	（オプション）パケット フォワーディング動作のデバッグ情報を表示します。
ps	（オプション）プロセス スイッチング動作のデバッグ情報を表示します。
signal	（オプション）ルーティング プロトコルへの MFIB シグナリングのデバッグ情報を表示します。

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
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカルサポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、MFIB データベース動作のデバッグ情報を表示します。

```
hostname# debug mfib db
MFIB IPv4 db debugging enabled
```

関連コマンド

コマンド	説明
show mfib	MFIB の転送エントリおよびインターフェイスを表示します。

debug mgcp

MGCP アプリケーション検査に関する詳細情報を表示するには、特権 EXEC モードで **debug mgcp** コマンドを使用します。デバッ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。

debug mgcp {**messages** | **parser** | **sessions**}

no debug mgcp {**messages** | **parser** | **sessions**}

シンタックスの説明

messages	MGCP メッセージのデバッグ情報を表示します。
parser	MGCP メッセージ解析のデバッグ情報を表示します。
sessions	MGCP セッションに関するデバッグ情報を表示します。

デフォルト

すべてのオプションが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
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

使用上のガイドライン

debug mgcp コマンドは、mgcp 検査に関する詳細情報を表示します。**no debug all** コマンドまたは **undebug all** コマンドは、イネーブルなデバッグをすべてオフにします。

例

次の例では、MGCP アプリケーション検査に関する詳細情報の表示をイネーブルにします。

```
hostname# debug mgcp
```

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。
inspect mgcp	MGCP アプリケーション検査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。
show conn	さまざまな接続タイプの接続状態を表示します。

debug module-boot

SSM ブーティング プロセスに関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug module-boot** コマンドを使用します。SSM ブーティング プロセスに関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug module-boot [*level*]

no debug module-boot [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

デフォルトのレベルは、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	このコマンドが導入されました。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークのトラフィックが遅くなる可能性があります。

例

次の例では、SSM ブーティング プロセスに関するデバッグ メッセージをイネーブルにします。

```
hostname# debug module-boot
```

関連コマンド

コマンド	説明
hw-module module recover	TFTP サーバからリカバリ イメージをロードすることにより、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、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	コンフィギュレーション データを失わずに電源を切るため、SSM ソフトウェアをシャットダウンします。
show module	SSM 情報を表示します。

debug mrib

MRIB のデバッグ情報を表示するには、特権 EXEC モードで **debug mrib** コマンドを使用します。デバッグ情報の表示を停止するには、このコマンドの **no** 形式を使用します。

debug mrib {***client*** | ***io*** | ***route*** [*group*] | ***table***}

no debug mrib {***client*** | ***io*** | ***route*** [*group*] | ***table***}

シンタックスの説明

client	MRIB クライアント管理アクティビティのデバッグをイネーブルにします。
io	MRIB I/O イベントのデバッグをイネーブルにします。
route	MRIB ルーティング エントリ アクティビティのデバッグをイネーブルにします。
group	指定グループでの MRIB ルーティング エントリ アクティビティのデバッグをイネーブルにします。
table	MRIB テーブル管理アクティビティのデバッグをイネーブルにします。

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
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカルサポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、MRIB I/O イベントのデバッグをイネーブルにする方法を示しています。

```
hostname# debug mrib io
IPv4 MRIB io debugging is on
```

関連コマンド

コマンド	説明
show mrib client	MRIB クライアント接続に関する情報を表示します。
show mrib route	MRIB テーブル のエントリを表示します。

debug ntdomain

NT ドメイン認証のデバッグ情報を表示するには、特権 EXEC モードで **debug ntdomain** コマンドを使用します。NT ドメインのデバッグ情報の表示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。

debug ntdomain [*level*]

no debug ntdomain

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 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	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカルサポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、NT ドメインのデバッグ メッセージをイネーブルにします。**show debug** コマンドは、NT ドメインのデバッグ メッセージがイネーブルになっていることを示します。

```
hostname# debug ntdomain
debug ntdomain  enabled at level 1
hostname# show debug
debug ntdomain  enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug ntp

NTP に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug ntp** コマンドを使用します。NTP に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug ntp {***adjust*** | ***authentication*** | ***events*** | ***loopfilter*** | ***packets*** | ***params*** | ***select*** | ***sync*** | ***validity***}

no debug ntp {***adjust*** | ***authentication*** | ***events*** | ***loopfilter*** | ***packets*** | ***params*** | ***select*** | ***sync*** | ***validity***}

シンタックスの説明

adjust	NTP クロック調整に関するメッセージを表示します。
authentication	NTP 認証に関するメッセージを表示します。
events	NTP イベントに関するメッセージを表示します。
loopfilter	NTP ループ フィルタに関するメッセージを表示します。
packets	NTP パケットに関するメッセージを表示します。
params	NTP クロック パラメータに関するメッセージを表示します。
select	NTP クロック セレクションに関するメッセージを表示します。
sync	NTP クロック同期に関するメッセージを表示します。
validity	NTP ピア クロックの有効性に関するメッセージを表示します。

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
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

debug コマンドを使用すると、通信量の多いネットワークのトラフィックが遅くなる可能性があります。

例

次の例では NTP に関するデバッグ メッセージをイネーブルにします。

```
hostname# debug ntp events
```

関連コマンド

コマンド	説明
ntp authenticate	NTP 認証をイネーブルにします。
ntp server	NTP サーバを指定します。
show debug	イネーブルなデバッガをすべて表示します。
show ntp associations	セキュリティ アプライアンスが関連付けられている NTP サーバを表示します。
show ntp status	NTP アソシエーションのステータスを表示します。

debug ospf

OSPF ルーティング プロセスのデバッグ情報を表示するには、特権 EXEC モードで **debug ospf** コマンドを使用します。

debug ospf [*adj* | *database-timer* | *events* | *flood* | *lsa-generation* | *packet* | *retransmission* | *spf* [*external* | *inter* | *intra*] | *tree*]

no debug ospf [*adj* | *database-timer* | *events* | *flood* | *lsa-generation* | *packet* | *retransmission* | *spf* [*external* | *inter* | *intra*] | *tree*]

シンタックスの説明

adj	（オプション）OSPF 隣接イベントのデバッグをイネーブルにします。
database-timer	（オプション）OSPF タイマー イベントのデバッグをイネーブルにします。
events	（オプション）OSPF イベントのデバッグをイネーブルにします。
external	（オプション）SPF デバッグを外部イベントに制限します。
flood	（オプション）OSPF フラッディングのデバッグをイネーブルにします。
inter	（オプション）SPF デバッグをエリア間イベントに制限します。
intra	（オプション）SPF デバッグをエリア内イベントに制限します。
lsa-generation	（オプション）OSPF 集約 LSA 生成のデバッグをイネーブルにします。
packet	（オプション）受信した OSPF パケットのデバッグをイネーブルにします。
retransmission	（オプション）OSPF 再送信イベントのデバッグをイネーブルにします。
spf	（オプション）OSPF 最短パス優先計算のデバッグをイネーブルにします。SPF デバッグ情報は、*external*、*inter*、および *intra* のキーワードを使用することで制限できます。
tree	（オプション）OSPF データベース イベントのデバッグをイネーブルにします。

デフォルト

キーワードが提供されないときに、すべての OSPF デバッグ情報が表示されます。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカルサポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次に、**debug ospf events** コマンドの出力例を示します。

```
hostname# debug ospf events
ospf event debugging is on

OSPF:hello with invalid timers on interface Ethernet0
hello interval received 10 configured 10
net mask received 255.255.255.0 configured 255.255.255.0
dead interval received 40 configured 30
```

関連コマンド

コマンド	説明
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。

debug parser cache

CLI パーサーのデバッグ情報を表示するには、特権 EXEC モードで **debug parser cache** コマンドを使用します。CLI パーサーのデバッグ情報の表示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。

debug parser cache [*level*]

no debug parser cache

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 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	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカルサポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、CLI パーサーのデバッグ メッセージをイネーブルにします。**show debug** コマンドは、現在のデバッグ コンフィギュレーションを表示します。CLI パーサーのデバッグ メッセージは、**show debug** コマンドの出力の前後に表示されます。

```
hostname# debug parser cache
debug parser cache enabled at level 1
hostname# show debug
parser cache: try to match 'show debug' in exec mode
debug parser cache enabled at level 1
parser cache: hit at index 8
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug pim

PIM のデバッグ情報を表示するには、特権 EXEC モードで **debug pim** コマンドを使用します。デバッグ情報の表示を停止するには、このコマンドの **no** 形式を使用します。

debug pim [***df-election*** [***interface*** *if_name* | ***rp*** *rp*] | ***group*** *group* | ***interface*** *if_name* | ***neighbor***]

no debug pim [***df-election*** [***interface*** *if_name* | ***rp*** *rp*] | ***group*** *group* | ***interface*** *if_name* | ***neighbor***]

シンタックスの説明

df-election	（オプション）PIM の双方向 DF 選定メッセージ プロセスに関するデバッグ メッセージを表示します。
group *group*	（オプション）指定されたグループのデバッグ情報を表示します。*group* の値は、次のいずれかです。 • マルチキャスト グループの名前。DNS の hosts テーブルに定義されているものか、ドメインの **ipv4 host** コマンドで定義したものです。 • マルチキャスト グループの IP アドレス。これは、4 分割ドット 10 進表記のマルチキャスト IP アドレスです。
interface *if_name*	（オプション）***df-election*** キーワードと共に使用する場合は、DF 選定のデバッグ表示を、指定したインターフェイスに関する情報に制限します。 ***df-election*** キーワードと共に使用しない場合は、指定されたインターフェイスの PIM エラー メッセージを表示します。 （注）　**debug pim** ***interface*** コマンドは、PIM プロトコル アクティビティ メッセージを表示せず、エラー メッセージだけを表示します。PIM プロトコル アクティビティのデバッグ情報を表示するには、***interface*** キーワードを使用せずに **debug pim** コマンドを使用します。***group*** キーワードを使用して、指定されたマルチキャスト グループに表示を制限することができます。
neighbor	（オプション）送信、または受信された PIM の HELLO メッセージだけを表示します。
rp *rp*	（オプション）次のいずれかを指定できます。 • RP の名前。ドメイン ネーム システム（DNS）の hosts テーブルに定義されているものか、ドメインの **ipv4 host** コマンドで定義したものです。 • RP の IP アドレス。これは、4 分割ドット 10 進表記のマルチキャスト IP アドレスです。

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	このコマンドが導入されました。

使用上のガイドライン

受信および送信された PIM パケットおよび PIM 関連のイベントを記録します。

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカルサポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次に、**debug pim** コマンドの出力例を示します。

```
hostname# debug pim
PIM: Received Join/Prune on Ethernet1 from 172.24.37.33
PIM: Received Join/Prune on Ethernet1 from 172.24.37.33
PIM: Received Join/Prune on Tunnel0 from 10.3.84.1
PIM: Received Join/Prune on Ethernet1 from 172.24.37.33
PIM: Received Join/Prune on Ethernet1 from 172.24.37.33
PIM: Received RP-Reachable on Ethernet1 from 172.16.20.31
PIM: Update RP expiration timer for 224.2.0.1
PIM: Forward RP-reachability packet for 224.2.0.1 on Tunnel0
PIM: Received Join/Prune on Ethernet1 from 172.24.37.33
PIM: Prune-list (10.221.196.51/32, 224.2.0.1)
PIM: Set join delay timer to 2 seconds for (10.221.0.0/16, 224.2.0.1) on Ethernet1
PIM: Received Join/Prune on Ethernet1 from 172.24.37.6
PIM: Received Join/Prune on Ethernet1 from 172.24.37.33
PIM: Received Join/Prune on Tunnel0 from 10.3.84.1
PIM: Join-list: (*, 224.2.0.1) RP 172.16.20.31
PIM: Add Tunnel0 to (*, 224.2.0.1), Forward state
PIM: Join-list: (10.0.0.0/8, 224.2.0.1)
PIM: Add Tunnel0 to (10.0.0.0/8, 224.2.0.1), Forward state
PIM: Join-list: (10.4.0.0/16, 224.2.0.1)
PIM: Prune-list (172.24.84.16/28, 224.2.0.1) RP-bit set RP 172.24.84.16
PIM: Send Prune on Ethernet1 to 172.24.37.6 for (172.24.84.16/28, 224.2.0.1), RP
PIM: For RP, Prune-list: 10.9.0.0/16
PIM: For RP, Prune-list: 10.16.0.0/16
PIM: For RP, Prune-list: 10.49.0.0/16
PIM: For RP, Prune-list: 10.84.0.0/16
PIM: For RP, Prune-list: 10.146.0.0/16
PIM: For 10.3.84.1, Join-list: 172.24.84.16/28
PIM: Send periodic Join/Prune to RP via 172.24.37.6 (Ethernet1)
```

関連コマンド

コマンド	説明
show pim group-map	グループからプロトコルへのマッピング テーブルを表示します。
show pim interface	PIM インターフェイス固有の情報を表示します。
show pim neighbor	PIM ネイバーテーブルのエントリを表示します。

debug pix pkt2pc

uauth コードに送信されたパケットをトレースし、uauth プロキシ セッションがデータ パスにカットスルーしたイベントをトレースするデバッグ メッセージを表示するには、特権 EXEC モードで **debug pix pkt2pc** コマンドを使用します。デバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug pix pkt2pc

no debug pix pkt2pc

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークのトラフィックが遅くなる可能性があります。

例

次の例では、uauth コードに送信されたパケットをトレースし、uauth プロキシ セッションがデータ パスにカットスルーしたイベントをトレースするデバッグ メッセージをイネーブルにします。

```
hostname# debug pix pkt2pc
```

関連コマンド

コマンド	説明
debug pix process	xlate およびセカンダリ接続プロセスに関するデバッグ メッセージを表示します。
show debug	イネーブルなデバッガをすべて表示します。

debug pix process

xlate およびセカンダリ接続プロセスに関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug pix process** コマンドを使用します。デバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug pix process

no debug pix process

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークのトラフィックが遅くなる可能性があります。

例

次の例では、xlate およびセカンダリ接続プロセスのデバッグ メッセージをイネーブルにします。

```
hostname# debug pix process
```

関連コマンド

コマンド	説明
debug pix pkt2pc	uauth コードに送信されたパケットをトレースし、uauth プロキシ セッションがデータ パスにカットスルーしたイベントをトレースするデバッグ メッセージを表示します。
show debug	イネーブルなデバッガをすべて表示します。

debug pptp

PPTP に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug pptp** コマンドを使用します。PPTP に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug pptp [*level*]

no debug pptp [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 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
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

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。デバッグ メッセージがすべて表示されないようにするには、**no debug all** コマンドを入力します。

（注）　**debug pptp** コマンドをイネーブルにすると、通信量の多いネットワークでは、トラフィックの速度が遅くなります。

例

次の例では、PPTP アプリケーション検査に対するデバッグ メッセージをデフォルトのレベル（1）でイネーブルにします。

```
hostname# debug pptp
```

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。
inspect pptp	PPTP アプリケーション検査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。

debug radius

AAA に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug radius** コマンドを使用します。RADIUS メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug radius [***all*** | ***decode*** | ***session*** | ***user*** *username*]]

no debug radius

シンタックスの説明

all	（オプション）デコードされた RADIUS メッセージを含む、すべてのユーザおよびセッションに関する RADIUS デバッグ メッセージを表示します。
decode	（オプション）RADIUS メッセージのデコードされたコンテンツを表示します。16 進値と、それらの値をデコードした読み取り可能なバージョンを含む、すべての RADIUS パケットのコンテンツが表示されます。
session	（オプション）セッション関連の RADIUS メッセージを表示します。送信および受信された RADIUS メッセージのパケット タイプは表示されますが、パケット コンテンツは表示されません。
user	（オプション）特定のユーザに関する RADIUS デバッグ メッセージを表示します。
username	メッセージを表示する対象のユーザを指定します。**user** キーワードと共に使用する場合だけ有効です。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

debug radius コマンドは、セキュリティ アプライアンスと RADIUS AAA サーバの間の RADIUS メッセージに関する詳細情報を表示します。**no debug all** コマンドまたは **undebug all** コマンドは、イネーブルなデバッグをすべてオフにします。

例

次の例は、デコードされた RADIUS メッセージを示しています。これはアカウンティング パケットです。

```
hostname(config)# debug radius decode
hostname(config)# RADIUS packet decode (accounting request)

--------------------------------------
Raw packet data (length = 216).....
i
Parsed packet data.....
Radius: Code = 4 (0x04)
Radius: Identifier = 105 (0x69)
Radius: Length = 216 (0x00D8)
Radius: Vector: 842E0E99F44C00C05A0A19AB88A81312
Radius: Type = 40 (0x28) Acct-Status-Type
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x2
Radius: Type = 5 (0x05) NAS-Port
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x1
Radius: Type = 4 (0x04) NAS-IP-Address
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 10.1.1.1 (0x0A010101)
Radius: Type = 14 (0x0E) Login-IP-Host
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 10.2.0.50 (0xD0FE1291)
Radius: Type = 16 (0x10) Login-TCP-Port
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x50
Radius: Type = 44 (0x2C) Acct-Session-Id
Radius: Length = 12 (0x0C)
Radius: Value (String) =
30 78 31 33 30 31 32 39 66 65                       |  0x130129fe
Radius: Type = 1 (0x01) User-Name
Radius: Length = 9 (0x09)
Radius: Value (String) =
62 72 6f 77 73 65 72                                |  browser
Radius: Type = 46 (0x2E) Acct-Session-Time
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x0
Radius: Type = 42 (0x2A) Acct-Input-Octets
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x256D
Radius: Type = 43 (0x2B) Acct-Output-Octets
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x3E1
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 30 (0x1E)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 24 (0x18)
Radius: Value (String) =
69 70 3a 73 6f 75 72 63 65 2d 69 70 3d 31 30 2e     |  ip:source-ip=10.
31 2e 31 2e 31 30                                   |  1.1.10
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 27 (0x1B)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 21 (0x15)
Radius: Value (String) =
69 70 3a 73 6f 75 72 63 65 2d 70 6f 72 74 3d 33     |  ip:source-port=3
34 31 33                                            |  413
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 40 (0x28)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 34 (0x22)
Radius: Value (String) =
69 70 3a 64 65 73 74 69 6e 61 74 69 6f 6e 2d 69     |  ip:destination-i
```

```
70 3d 32 30 38 2e 32 35 34 2e 31 38 2e 31 34 35    |  p=10.2.0.50
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 30 (0x1E)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 24 (0x18)
Radius: Value (String) =
69 70 3a 64 65 73 74 69 6e 61 74 69 6f 6e 2d 70    |  ip:destination-p
6f 72 74 3d 38 30                                  |  ort=80
```

関連コマンド

コマンド	説明
show running-config	セキュリティ アプライアンス上で実行されている設定を表示します。

debug rip

RIP のデバッグ情報を表示するには、特権 EXEC モードで **debug rip** コマンドを使用します。デバッグ情報の表示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。

debug ***rip***

no debug ***rip***

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカルサポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、RIP のレベル 1 デバッグをイネーブルにします。

```
hostname# debug rip
debug rip enabled at level 1

hostname#
```

関連コマンド

コマンド	説明
clear configure rip	実行コンフィギュレーションからすべての RIP コマンドを消去します。
rip	指定したインターフェイスに RIP を設定します。
show running-config rip	実行コンフィギュレーション内の RIP コマンドを表示します。

debug rtsp

RTSP アプリケーション検査に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug rtsp** コマンドを使用します。RTSP アプリケーション検査に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug rtsp [*level*]

no debug rtsp [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 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
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

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。デバッグ メッセージがすべて表示されないようにするには、**no debug all** コマンドを入力します。

（注）　**debug rtsp** コマンドをイネーブルにすると、通信量の多いネットワークでは、トラフィックの速度が遅くなります。

例

次の例では、RTSP アプリケーション検査のデバッグ メッセージをデフォルトのレベル（1）でイネーブルにします。

```
hostname# debug rtsp
```

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。
inspect rtsp	RTSP アプリケーション検査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。

debug sdi

SDI 認証のデバッグ情報を表示するには、特権 EXEC モードで **debug sdi** コマンドを使用します。SDI デバッグ情報の表示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。

debug sdi [*level*]

no debug sdi

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 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	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカルサポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、SDI デバッグ メッセージをイネーブルにします。**show debug** コマンドは、SDI デバッグ メッセージがイネーブルになっていることを示します。

```
hostname# debug sdi
debug sdi  enabled at level 1
hostname# show debug
debug sdi  enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug sequence

すべてのデバッグ メッセージの最初にシーケンス番号を追加するには、特権 EXEC モードで **debug sequence** コマンドを使用します。デバッグ シーケンス番号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。

debug sequence [*level*]

no debug sequence

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

デフォルトは次のとおりです。

- デバッグ メッセージのシーケンス番号はディセーブルになっています。
- *level* のデフォルト値は 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	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカルサポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、デバッグ メッセージのシーケンス番号をイネーブルにします。**debug parser cache** コマンドは、CLI パーサー デバッグ メッセージをイネーブルにします。**show debug** コマンドは、現在のデバッグ コンフィギュレーションを表示します。表示されている CLI パーサー デバッグ メッセージには、各メッセージの前にシーケンス番号が含まれます。

```
hostname# debug sequence
debug sequence  enabled at level 1
hostname# debug parser cache
debug parser cache enabled at level 1
hostname# show debug
0: parser cache: try to match 'show debug' in exec mode
debug parser cache enabled at level 1
debug sequence  enabled at level 1
1: parser cache: hit at index 8
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug session-command

SSM へのセッションに対するデバッグ メッセージを表示するには、特権 EXEC モードで **debug session-command** コマンドを使用します。セッションに関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug session-command [*level*]

no debug session-command [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

デフォルトのレベルは、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	このコマンドが導入されました。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークのトラフィックが遅くなる可能性があります。

例

次の例では、セッションのデバッグ メッセージをイネーブルにします。

```
hostname# debug session-command
```

関連コマンド

コマンド	説明
session	SSM へのセッションです。

debug sip

SIP アプリケーション検査に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug sip** コマンドを使用します。SIP アプリケーション検査に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug sip [*level*]

no debug sip [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 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
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

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。デバッグ メッセージがすべて表示されないようにするには、**no debug all** コマンドを入力します。

（注）　**debug sip** コマンドをイネーブルにすると、通信量の多いネットワークでは、トラフィックの速度が遅くなります。

例

次の例では、SIP アプリケーション検査に対するデバッグ メッセージをデフォルトのレベル（1）でイネーブルにします。

```
hostname# debug sip
```

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。
inspect sip	SIP アプリケーション検査をイネーブルにします。
show conn	さまざまな接続タイプの接続状態を表示します。
show 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。
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。

debug skinny

SCCP（Skinny）アプリケーション検査に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug skinny** コマンドを使用します。SCCP アプリケーション検査に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug skinny [*level*]

no debug skinny [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 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
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

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。デバッグ メッセージがすべて表示されないようにするには、**no debug all** コマンドを入力します。

（注） **debug skinny** コマンドをイネーブルにすると、通信量の多いネットワークでは、トラフィックの速度が遅くなります。

例

次の例では、SCCP アプリケーション検査に関するデバッグ メッセージをデフォルトのレベル（1）でイネーブルにします。

```
hostname# debug skinny
```

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。
inspect skinny	SCCP アプリケーション検査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。

debug smtp

SMTP/ESMTP アプリケーション検査に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug smtp** コマンドを使用します。SMTP/ESMTP アプリケーション検査に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug smtp [*level*]

no debug smtp [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 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
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

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。デバッグ メッセージがすべて表示されないようにするには、**no debug all** コマンドを入力します。

（注）　**debug smtp** コマンドをイネーブルにすると、通信量の多いネットワークでは、トラフィックの速度が遅くなります。

例

次の例では、SMTP/ESMTP アプリケーション検査に対するデバッグ メッセージをデフォルトのレベル（1）でイネーブルにします。

```
hostname# debug smtp
```

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。
inspect esmtp	ESMTP アプリケーション検査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。

debug sqlnet

SQL*Net アプリケーション検査に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug sqlnet** コマンドを使用します。SQL*Net アプリケーション検査に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug sqlnet [*level*]

no debug sqlnet [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 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
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

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。デバッグ メッセージがすべて表示されないようにするには、**no debug all** コマンドを入力します。

（注）　**debug sqlnet** コマンドをイネーブルにすると、通信量の多いネットワークでは、トラフィックの速度が遅くなります。

例

次の例では、SQL*Net アプリケーション検査に対するデバッグ メッセージをデフォルトのレベル（1）でイネーブルにします。

```
hostname# debug sqlnet
```

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。
inspect sqlnet	SQL*Net アプリケーション検査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。

debug ssh

SSH に関連するデバッグ情報およびエラー メッセージを表示するには、特権 EXEC モードで **debug ssh** コマンドを使用します。デバッグ情報の表示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。

debug *ssh* [*level*]

no debug *ssh* [*level*]

シンタックスの説明

level	（オプション）デバッグのオプション レベルを指定します。

デフォルト

デフォルトのレベルは、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
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

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカルサポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次に、**debug ssh *255*** コマンドの出力例を示します。

```
hostname# debug ssh 255
debug ssh  enabled at level 255
SSH2 0: send: len 64 (includes padlen 17)
SSH2 0: done calc MAC out #239
SSH2 0: send: len 32 (includes padlen 7)
SSH2 0: done calc MAC out #240
SSH2 0: send: len 64 (includes padlen 15)
SSH2 0: done calc MAC out #241
SSH2 0: send: len 32 (includes padlen 16)
SSH2 0: done calc MAC out #242
SSH2 0: send: len 64 (includes padlen 7)
SSH2 0: done calc MAC out #243
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #244
SSH2 0: send: len 64 (includes padlen 8)
SSH2 0: done calc MAC out #245
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #246
SSH2 0: send: len 64 (includes padlen 7)
SSH2 0: done calc MAC out #247
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #248
SSH2 0: send: len 64 (includes padlen 7)
SSH2 0: done calc MAC out #249
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #250
SSH2 0: send: len 64 (includes padlen 8)
SSH2 0: done calc MAC out #251
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #252
SSH2 0: send: len 64 (includes padlen 7)
SSH2 0: done calc MAC out #253
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #254
SSH2 0: send: len 64 (includes padlen 8)
SSH2 0: done calc MAC out #255
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #256
SSH2 0: send: len 64 (includes padlen 7)
SSH2 0: done calc MAC out #257
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #258
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションからすべての SSH コマンドを消去します。
show running-config ssh	実行コンフィギュレーション内の現在の SSH コマンドを表示します。
show ssh sessions	セキュリティ アプライアンス上のアクティブな SSH セッションに関する情報を表示します。
ssh	指定したクライアントまたはネットワークからセキュリティ アプライアンスへの SSH 接続を許可します。

debug ssl

SSL のデバッグ情報を表示するには、特権 EXEC モードで **debug ssl** コマンドを使用します。SSL デバッグ情報の表示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。

debug ssl {***cipher*** | ***device***} [*level*]

no debug ssl {***cipher*** | ***device***}

シンタックスの説明

cipher	HTTP サーバとクライアント間の暗号ネゴシエーションに関する情報を表示します。
device	セッションの開始と進行中のステータスを含む SSL デバイスに関する情報を表示します。
level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 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
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

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカルサポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、特に暗号ネゴシエーションに対する SSL デバッグ メッセージをイネーブルにします。**show debug** コマンドは、SSL デバッグ メッセージがイネーブルになっていることを示します。

```
hostname# debug ssl cipher
debug ssl cipher enabled at level 1
hostname# show debug
debug ssl cipher enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug sunrpc

RPC アプリケーション検査に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug sunrpc** コマンドを使用します。RPC アプリケーション検査に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug sunrpc [*level*]

no debug sunrpc [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 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
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

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。デバッグ メッセージがすべて表示されないようにするには、**no debug all** コマンドを入力します。

（注）　**debug sunrpc** コマンドをイネーブルにすると、通信量の多いネットワークでは、トラフィックの速度が遅くなります。

例

次の例では、RPC アプリケーション検査に対するデバッグ メッセージをデフォルトのレベル（1）でイネーブルにします。

```
hostname# debug sunrpc
```

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。
inspect sunrpc	Sun RPC アプリケーション検査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。
show conn	RPC など、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。

debug tacacs

TACACS+ のデバッグ情報を表示するには、特権 EXEC モードで **debug tacacs** コマンドを使用します。TACACS+ デバッグ情報の表示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。

debug tacacs [***session*** | ***user*** *username*]

no debug tacacs [***session*** | ***user*** *username*]

シンタックスの説明

session	セッション関連の TACACS+ デバッグ メッセージを表示します。
user	ユーザ固有の TACACS+ デバッグ メッセージを表示します。一度に 1 人のユーザの TACACS+ デバッグ メッセージだけ表示できます。
username	TACACS+ デバッグ メッセージを表示するユーザを指定します。

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
7.0	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカルサポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、TACACS+ デバッグ メッセージをイネーブルにします。**show debug** コマンドは、TACACS+ デバッグ メッセージがイネーブルになっていることを示します。

```
hostname# debug tacacs user admin342
hostname# show debug
debug tacacs user admin342
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug tcp-map

TCP アプリケーション検査マップに関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug tcp-map** コマンドを使用します。TCP アプリケーション検査に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug tcp-map

no debug tcp-map

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカルサポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、TCP アプリケーション検査マップに対するデバッグ メッセージをイネーブルにします。**show debug** コマンドは、TCP アプリケーション検査マップのデバッグ メッセージがイネーブルになっていることを示します。

```
hostname# debug tcp-map
debug tcp-map enabled at level 1.
hostname# show debug
debug tcp-map enabled at level 1.
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug timestamps

すべてのデバッグ メッセージの最初にタイムスタンプ情報を追加するには、特権 EXEC モードで **debug timestamps** コマンドを使用します。デバッグ タイムスタンプ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。

debug timestamps [*level*]

no debug timestamps

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

デフォルトは次のとおりです。

- デバッグ タイムスタンプ情報はディセーブルです。
- *level* のデフォルト値は 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	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカルサポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、デバッグ メッセージのタイムスタンプをイネーブルにします。**debug parser cache** コマンドは、CLI パーサー デバッグ メッセージをイネーブルにします。**show debug** コマンドは、現在のデバッグ コンフィギュレーションを表示します。表示されている CLI パーサー デバッグ メッセージには、各メッセージの前にタイムスタンプが含まれています。

```
hostname# debug timestamps
debug timestamps  enabled at level 1
hostname# debug parser cache
debug parser cache enabled at level 1
hostname# show debug
1982769.770000000: parser cache: try to match 'show debug' in exec mode
1982769.770000000: parser cache: hit at index 8
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug vpn-sessiondb

VPN セッション データベースのデバッグ情報を表示するには、特権 EXEC モードで **debug vpn-sessiondb** コマンドを使用します。VPN セッション データベースに関するデバッグ情報の表示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。

debug vpn-sessiondb [*level*]

no debug vpn-sessiondb

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 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	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカルサポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、VPN セッション データベースのデバッグ メッセージをイネーブルにします。**show debug** コマンドは、VPN セッション データベースのデバッグ メッセージがイネーブルになっていることを示します。

```
hostname# debug vpn-sessiondb
debug vpn-sessiondb  enabled at level 1
hostname# show debug
debug vpn-sessiondb  enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug xdmcp

XDMCP アプリケーション検査に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug xdmcp** コマンドを使用します。XDMCP アプリケーション検査に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug xdmcp [*level*]

no debug xdmcp [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 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
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

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。デバッグ メッセージがすべて表示されないようにするには、**no debug all** コマンドを入力します。

（注）　**debug xdmcp** コマンドをイネーブルにすると、通信量の多いネットワークでは、トラフィックの速度が遅くなります。

例

次の例では、XDMCP アプリケーション検査に対するデバッグ メッセージをデフォルトのレベル（1）でイネーブルにします。

```
hostname# debug xdmcp
```

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。
inspect xdmcp	XDMCP アプリケーション検査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。

default

time-range コマンドの ***absolute*** キーワードおよび ***periodic*** キーワードのデフォルト設定を復元するには、時間範囲コンフィギュレーション モードで ***default*** コマンドを使用します。

default {**absolute** | **periodic** *days-of-the-week time* **to** [*days-of-the-week*] *time*}

シンタックスの説明

absolute	時間範囲が有効である絶対時間を定義します。
days-of-the-week	（オプション）最初の days-of-the-week 引数は、関連付けられている時間範囲が有効になる日または曜日です。2 番目の days-of-the-week 引数は、関連付けられている文の有効期間が終了する日または曜日です。 この引数は、任意の 1 つの曜日または曜日の組み合せです（monday（月曜日）、tuesday（火曜日）、wednesday（水曜日）、thursday（木曜日）、friday（金曜日）、saturday（土曜日）、および sunday（日曜日））。他に指定できる値は、次のとおりです。 • daily：月曜日～日曜日 • weekdays：月曜日～金曜日 • weekend：土曜日と日曜日 終了の曜日が開始の曜日と同じ場合は、終了の曜日を省略できます。
periodic	時間範囲機能をサポートする機能に対して、定期的な（週単位の）時間範囲を指定します。
time	時刻を HH:MM 形式で指定します。たとえば、午前 8 時は 8:00、午後 8 時は 20:00 とします。
to	「開始時刻から終了時刻まで」の範囲を完成させるには、***to*** キーワードを入力する必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

使用上のガイドライン

終了の days-of-the-week 値が開始の days-of-the-week 値と同じである場合は、終了の days-of-the-week 値を省略できます。

time-range コマンドに ***absolute*** 値と ***periodic*** 値の両方が指定されている場合、***periodic*** コマンドは ***absolute start*** 時刻に達した後にだけ評価され、***absolute end*** 時刻に達した後はそれ以上評価されません。

time-range 機能はセキュリティ アプライアンスのシステム クロックに依存しています。ただし、この機能は、NTP 同期化により最適に動作します。

例

次の例は、***absolute*** キーワードのデフォルト動作を復元する方法を示しています。

```
hostname(config-time-range)# default absolute
```

関連コマンド

コマンド	説明
absolute	時間範囲が有効である絶対時間を定義します。
periodic	時間範囲機能をサポートする機能に対して、定期的な（週単位の）時間範囲を指定します。
time-range	時間に基づいてセキュリティ アプライアンスのアクセス コントロールを定義します。

default (crl configure)

すべての CRL パラメータをシステムのデフォルト値に戻すには、crl 設定コンフィギュレーション モードで **default** コマンドを使用します。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。

default

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
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	このコマンドが導入されました。

使用上のガイドライン

このコマンドの呼び出しは、アクティブなコンフィギュレーションの一部になりません。

例

次の例では、ca-crl コンフィギュレーション モードに入り、CRL コマンド値をデフォルトに戻します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# default
hostname(ca-crl)#
```

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	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。

default (time-range)

absolute および ***periodic*** コマンドのデフォルト設定を復元するには、時間範囲コンフィギュレーション モードで ***default*** コマンドを使用します。

default {**absolute** | **periodic** *days-of-the-week time* **to** [*days-of-the-week*] *time*}

シンタックスの説明

absolute	時間範囲が有効である絶対時間を定義します。
days-of-the-week	最初の days-of-the-week 引数は、関連付けられている時間範囲が有効になる日または曜日です。2 番目の days-of-the-week 引数は、関連付けられている文の有効期間が終了する日または曜日です。 この引数は、任意の 1 つの曜日または曜日の組み合せです（monday（月曜日）、tuesday（火曜日）、wednesday（水曜日）、thursday（木曜日）、friday（金曜日）、saturday（土曜日）、および sunday（日曜日））。他に指定できる値は、次のとおりです。 • daily：月曜日～日曜日 • weekdays：月曜日～金曜日 • weekend：土曜日と日曜日 終了の曜日が開始の曜日と同じ場合は、終了の曜日を省略できます。
periodic	時間範囲機能をサポートする機能に対して、定期的な（週単位の）時間範囲を指定します。
time	時刻を HH:MM 形式で指定します。たとえば、午前 8 時は 8:00、午後 8 時は 20:00 とします。
to	「開始時刻から終了時刻まで」の範囲を完成させるには、***to*** キーワードを入力する必要があります。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

使用上のガイドライン

終了の days-of-the-week 値が開始の days-of-the-week 値と同じである場合は、終了の days-of-the-week 値を省略できます。

time-range コマンドに ***absolute*** 値と ***periodic*** 値の両方が指定されている場合、***periodic*** コマンドは ***absolute start*** 時刻に達した後にだけ評価され、***absolute end*** 時刻に達した後はそれ以上評価されません。

time-range 機能はセキュリティ アプライアンスのシステム クロックに依存しています。ただし、この機能は、NTP 同期化により最適に動作します。

例

次の例は、***absolute*** キーワードのデフォルト動作を復元する方法を示しています。

```
hostname(config-time-range)# default absolute
```

関連コマンド

コマンド	説明
absolute	時間範囲が有効である絶対時間を定義します。
periodic	時間範囲機能をサポートする機能に対して、定期的な（週単位の）時間範囲を指定します。
time-range	時間に基づいてセキュリティ アプライアンスのアクセス コントロールを定義します。

default enrollment

すべての登録パラメータをシステムのデフォルト値に戻すには、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 **default enrollment** コマンドを使用します。

default enrollment

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの呼び出しは、アクティブなコンフィギュレーションの一部になりません。

例

次の例では、トラストポイント central の暗号 CA トラストポイント コンフィギュレーション モードに入り、すべての登録パラメータをトラストポイント central 内のデフォルト値に戻します。

```
hostname<config># crypto ca trustpoint central
hostname<ca-trustpoint># default enrollment
hostname<ca-trustpoint>#
```

関連コマンド

コマンド	説明
clear configure crypto ca trustpoint	すべてのトラストポイントを削除します。
crl configure	crl コンフィギュレーション モードに入ります。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。

default-domain

グループポリシーのユーザに対してデフォルトのドメイン名を設定するには、グループポリシー コンフィギュレーション モードで **default-domain** コマンドを使用します。ドメイン名を削除するには、このコマンドの **no** 形式を使用します。

ユーザがドメイン名を継承しないようにするには、**default-domain none** コマンドを使用します。

セキュリティ アプライアンスは、ドメイン フィールドを省略した DNS クエリーに付加するために、デフォルト ドメイン名を IPSec クライアントに渡します。このドメイン名は、トンネル パケットにだけ適用されます。デフォルト ドメイン名がない場合、ユーザはデフォルト グループポリシーのデフォルト ドメイン名を継承します。

default-domain {value *domain-name* **| none}**

no default-domain [*domain-name***]**

シンタックスの説明

none	デフォルト ドメイン名がないことを指定します。デフォルト ドメイン名にヌル値を設定して、デフォルト ドメイン名を拒否します。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デフォルトのドメイン名を継承しないようにします。
value *domain-name*	グループのデフォルト ドメイン名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

使用上のガイドライン

デフォルトのドメイン名に使用できるのは、英数字、ハイフン（-）、およびピリオド（.）だけです。

例

次の例は、FirstGroup という名前のグループポリシーに対して FirstDomain のデフォルト ドメイン名を設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# default-domain value FirstDomain
```

関連コマンド

コマンド	説明
split-dns	スプリット トンネルを介して解決されるドメインのリストを提供します。
split-tunnel-network-list	トンネリングが必要なネットワークと不要なネットワークを区別するために、セキュリティ アプライアンスが使用するアクセスリストを指定します。
split-tunnel-policy	IPSec クライアントが、条件に応じて、パケットを暗号化された形式で IPSec トンネルを介して誘導したり、クリアテキスト形式でネットワーク インターフェイスに誘導したりできるようにします。

default-group-policy

デフォルトでユーザが継承するアトリビュートのセットを指定するには、トンネルグループ一般アトリビュート コンフィギュレーション モードで **default-group-policy** コマンドを使用します。デフォルトのグループポリシー名を削除するには、このコマンドの ***no*** 形式を使用します。

default-group-policy *group-name*

no default-group-policy *group-name*

シンタックスの説明

group-name	デフォルト グループの名前を指定します。

デフォルト

デフォルト グループ名は、DfltGrpPolicy 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
トンネルグループ一般アトリビュート 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	このコマンドが導入されました。

使用上のガイドライン

デフォルトのグループポリシー DfltGrpPolicy では、セキュリティ アプライアンスが初期設定されています。すべてのトンネルグループ タイプにこのアトリビュートを適用できます。

例

次の例では、Config-general コンフィギュレーション モードに入り、standard-policy という名前の IPSec LAN-to-LAN トンネルグループで、ユーザがデフォルトで継承するアトリビュートのセットを指定します。このコマンドのセットは、アカウンティング サーバ、認証サーバ、認可サーバおよびアドレス プールを定義します。

```
hostname(config)# tunnel-group standard-policy type ipsec-ra
hostname(config)# tunnel-group standard-policy general-attributes
hostname(config-general)# default-group-policy first-policy
hostname(config-general)# accounting-server-group aaa-server123
hostname(config-general)# address-pool (inside) addrpool1 addrpool2 addrpool3
hostname(config-general)# authentication-server-group aaa-server456
hostname(config-general)# authorization-server-group aaa-server78
hostname(config-general)#
```

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。
group-policy	グループポリシーを作成または編集します。
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。

default-group-policy (webvpn)

WebVPN または電子メールのプロキシ コンフィギュレーションがグループポリシーを指定していない場合に、使用するグループポリシー名を指定するには、**default-group-policy** コマンドを使用します。WebVPN、IMAP4S、POP3S、および SMTPS セッションは、指定されたグループポリシーまたはデフォルトのグループポリシーのいずれかを必要とします。WebVPN の場合、このコマンドは webvpn モードで使用します。電子メールの場合、このコマンドは、該当する電子メール プロキシ モードで使用します。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。

default-group-policy *groupname*

no default-group-policy

シンタックスの説明

groupname	デフォルトのグループポリシーとして使用する設定済みのグループポリシーを指定します。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、グループポリシーを設定します。

デフォルト

DfltGrpPolicy という名前のデフォルト グループポリシーは、常にセキュリティ アプライアンスに存在します。**default-group-policy** コマンドを使用すると、作成したグループポリシーを、WebVPN および電子メール プロキシ セッション用のデフォルトのグループポリシーとして代用できます。別の方法として、DfltGrpPolicy を編集することもできます。

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
Webvpn	•	—	•	—	—
Imap4s	•	—	•	—	—
Pop3s	•	—	•	—	—
Smtps	•	—	•	—	—

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

使用上のガイドライン

システムの DefaultGroupPolicy は編集できますが、削除できません。DefaultGroupPolicy の AVP は次のとおりです。

アトリビュート	デフォルト値
wins-server	none
dns-server	none
dhcp-network-scope	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	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	0
backup-servers	keep-client-config
split-tunnel-policy	tunnelall
split-tunnel-network-list	none
default-domain	none
split-dns	none
intercept-dhcp	disable
client-firewall	none
secure-unit-authentication	disabled
user-authentication	disabled
user-authentication-idle-timeout	none
ip-phone-bypass	disabled
leap-bypass	disabled
nem	disabled
webvpn アトリビュート：	
filter	none
functions	disabled
homepage	none
html-content-filter	none
port-forward	disabled
port-forward-name	none
url-list	mpme

例

次の例は、WebVPN に WebVPN7 という名前のデフォルト グループポリシーを指定する方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# default-group-policy WebVPN7
```

default-idle-timeout

WebVPN ユーザに対するデフォルトのアイドル タイムアウトを設定するには、webvpn モードで **default-idle-timeout** コマンドを使用します。デフォルトのアイドル タイムアウト値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。

デフォルトのアイドル タイムアウトを使用すると、古いセッションが発生するのを防ぐことができます。

default-idle-timeout *seconds*

no default-idle-timeout

シンタックスの説明

seconds	アイドル タイムアウトの秒数を指定します。最小値は 60 秒、最大値は 1 日（86,400 秒）です。

デフォルト

1,800 秒（30 分）です。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

使用上のガイドライン

ユーザのアイドル タイムアウトが定義されていない場合、値が 0 の場合、または値が有効な範囲外である場合、セキュリティ アプライアンスはここで設定された値を使用します。

このコマンドに、短い時間を設定することをお勧めします。理由は、クッキーがディセーブルにされている（またはクッキーを要求され、それを拒否する）設定のブラウザにより、ユーザが接続していなくてもセッション データベースに表示される場合があるからです。許容する接続の最大数が 1 に設定されている場合は（**vpn-simultaneous-logins** コマンド）、すでに接続の最大数に達していることをデータベースが示すため、ユーザはログインし直すことができません。アイドル タイムアウトを低く設定すると、そのような実体のないセッションを迅速に削除し、ユーザは再度ログインできます。

例

次の例は、デフォルトのアイドル タイムアウトを 1,200 秒（20 分）に設定する方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# default-idle-timeout 1200
```

関連コマンド

コマンド	説明
vpn-simultaneous-logins	許容する同時 VPN セッションの最大数を設定します。グループ ポリシーまたはユーザ名モードで使用します。

default-information originate

OSPF ルーティング ドメインへのデフォルトの外部ルートを生成するには、ルータ コンフィギュレーション モードで **default-information originate** 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。

default-information originate [***always***] [***metric*** *value*] [***metric-type*** {***1*** | ***2***}] [***route-map*** *name*]

no default-information originate [[***always***] [***metric*** *value*] [***metric-type*** {***1*** | ***2***}] [***route-map*** *name*]]

シンタックスの説明

always	（オプション）ソフトウェアでデフォルト ルートが設定されているかどうかかかわらず、常にデフォルト ルートをアドバタイズします。
metric *value*	（オプション）OSPF デフォルト メトリック値を指定します（0 ～ 16777214）。
metric-type {1 | 2}	（オプション）OSPF ルーティング ドメインにアドバタイズされたデフォルト ルートに関連する外部リンク タイプです。有効な値は次のとおりです。 • ***1***：タイプ 1 外部ルート。 • ***2***：タイプ 2 外部ルート。
route-map *name*	（オプション）適用するルートマップの名前。

デフォルト

デフォルト値は次のとおりです。

- ***metric*** *value* は 1 です。
- ***metric-type*** は 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
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

このコマンドの **no** 形式をオプションのキーワードおよび引数と共に使用すると、コマンドからオプションの情報だけが削除されます。たとえば、**no default-information originate** ***metric 3*** を入力すると、実行コンフィギュレーションのコマンドから ***metric 3*** オプションが削除されます。実行コンフィギュレーションからコマンド全体を削除するには、このコマンドの **no** 形式をオプションなしで使用します。つまり **no default-information originate** となります。

例

次の例は、オプションのメトリックおよびメトリック タイプと共に **default-information originate** コマンドを使用する方法を示しています。

```
hostname(config-router)# default-information originate always metric 3 metric-type 2
hostname(config-router)#
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

delete

ディスク パーティションのファイルを削除するには、特権 EXEC モードで **delete** コマンドを使用します。

delete [**/noconfirm**] [**/recursive**] [**disk0: | disk1: | flash:**]*filename*

シンタックスの説明

/noconfirm	（オプション）確認のためのプロンプトを表示しないように指定します。
/recursive	（オプション）指定されたファイルをすべてのサブディレクトリで再帰的に削除します。
disk0:	（オプション）内部フラッシュ メモリを指定し、続けてコロン（:）を入力します。
disk1:	（オプション）外部フラッシュ メモリ カードを指定し、続けてコロン（:）を入力します。
filename	削除するファイルの名前を指定します。
flash:	取り外しできない内部フラッシュを指定して、続けてコロン（:）を入力します。ASA 5500 シリーズでは、***flash*** キーワードは ***disk0*** のエイリアスです。

デフォルト

ディレクトリを指定しない場合のデフォルトのディレクトリは、現在の作業ディレクトリです。

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
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

パスを指定しない場合、ファイルは現在の作業ディレクトリから削除されます。ファイルの削除では、ワイルドカードがサポートされています。ファイルを削除する場合、ファイル名のプロンプトが表示され、削除を確認する必要があります。

次の例は、現在の作業ディレクトリにある *test.cfg* という名前のファイルを削除する方法を示しています。

```
hostname# delete test.cfg
```

関連コマンド

コマンド	説明
cd	現在の作業ディレクトリから、指定したディレクトリに移動します。
rmdir	ファイルまたはディレクトリを削除します。
show file	指定されたファイルを表示します。

deny version

SNMP トラフィックの特定のバージョンを拒否するには、グローバル コンフィギュレーション モードから snmp-map コマンドを入力することによりアクセスできる 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。このコマンドをディセーブルにするには、このコマンドの **no** 形式を使用します。

deny version *version*

deny version *version*

シンタックスの説明

version	セキュリティ アプライアンスがドロップする SNMP トラフィックのバージョンを指定します。許可される値は **1**、**2**、**2c**、および **3** 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
SNMP 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	このコマンドが導入されました。

使用上のガイドライン

deny version コマンドを使用して、SNMP トラフィックを、SNMP の特定のバージョンに制限します。SNMP の以前のバージョンはセキュリティが低いため、セキュリティ ポリシーで SNMP トラフィックを Version 2 に制限することができます。**snmp-map** コマンドを使用して設定する SNMP マップ内で **deny version** コマンドを使用します。SNMP マップを作成した後で、**inspect snmp** コマンドを使用してマップをイネーブルにし、次にそれを **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適用します。

例

次の例は、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 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
hostname(config-pmap)# exit
hostname(config)# service-policy inbound_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。
inspect snmp	SNMP アプリケーション検査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。
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。
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。

description

指定したコンフィギュレーション ユニット（たとえば、コンテキストまたはオブジェクト グループ）に対する説明を追加するには、さまざまなコンフィギュレーション モードで **description** コマンドを使用します。この説明を削除するには、このコマンドの **no** 形式を使用します。説明により、役立つ情報がコンフィギュレーションに追加されます。

description *text*

no description

シンタックスの説明

text	説明に、最大 200 文字のテキスト文字列を設定します。文字列に疑問符（?）を含める場合は、不注意から CLI ヘルプを呼び出さないように、疑問符を入力する前に **Ctrl+V** を入力する必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラスマップ コンフィギュレーション	•	•	•	•	—
コンテキスト コンフィギュレーション	•	•	—	—	•
Gtp マップ コンフィギュレーション	•	•	•	•	—
インターフェイス コンフィギュレーション	•	•	•	•	•
オブジェクト グループ コンフィギュレーション	•	•	•	•	—
ポリシーマップ 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	このコマンドが、複数の新しいコンフィギュレーション モードに追加されました。

例

次の例は、「アドミニストレーション」コンテキスト コンフィギュレーションに説明を追加したものです。

```
hostname(config)# context administrator
hostname(config-context)# description This is the admin context.
hostname(config-context)# allocate-interface gigabitethernet0/0.1
hostname(config-context)# allocate-interface gigabitethernet0/1.1
hostname(config-context)# config-url flash://admin.cfg
```

関連コマンド

コマンド	説明
class-map	**policy-map** コマンドでアクションを適用するトラフィックを指定します。
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードに入ります。
gtp-map	GTP 検査エンジンのパラメータを制御します。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
object-group	**access-list** コマンドに含めるトラフィックを指定します。
policy-map	**class-map** コマンドで指定されたトラフィックに適用するアクションを指定します。

dhcp-network-scope

セキュリティ アプライアンス DHCP サーバが、このグループポリシーのユーザにアドレスを割り当てるために使用する IP アドレスの範囲を指定するには、グループポリシー コンフィギュレーション モードで **dhcp-network-scope** コマンドを使用します。この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。値を継承しないようにするには、**dhcp-network-scope none** コマンドを使用します。

dhcp-network-scope {*ip_address*} | none

no dhcp-network-scope

シンタックスの説明

ip_address	このグループポリシーのユーザに IP アドレスを割り当てるときに使用する、DHCP サーバの IP サブネットワークを指定します。
none	DHCP サブネットワークに、ヌル値を設定して IP アドレスを許可しません。デフォルトのグループポリシーまたは指定されているグループポリシーから値を継承しないようにします。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

例

次の例は、First Group という名前のグループポリシーに対して 10.10.85.0 という IP サブネットワー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)# dhcp-network-scope 10.10.85.0
```

dhcp-server

VPN トンネルが確立されると IP アドレスをクライアントに割り当てる DHCP サーバへのサポートを設定するには、トンネルグループ一般アトリビュート コンフィギュレーション モードで **dhcp-server** コマンドを使用します。このコマンドをデフォルトに戻すには、このコマンドの ***no*** 形式を使用します。

dhcp-server *hostname1* [*...hostname10*]

no dhcp-server *hostname*

シンタックスの説明

hostname1 ...hostname10	DHCP サーバの IP アドレスを指定します。最大 10 個の DHCP サーバを指定できます。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネルグループ一般アトリビュート 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	このコマンドが導入されました。

使用上のガイドライン

このアトリビュートは、IPSec リモートアクセス トンネルグループ タイプだけに適用できます。

例

Config-general コンフィギュレーション モードで入力された次のコマンドは、3 つの DHCP サーバ（dhcp1、dhcp2、および dhcp3）を IPSec リモートアクセス トンネルグループ remotegrp に追加します。

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp general
hostname(config-general)# default-group-policy remotegrp
hostname(config-general)# dhcp-server dhcp1 dhcp2 dhcp3
hostname(config-general)
```

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。

dhcpd address

DHCP サーバで使用される IP アドレス プールを定義するには、グローバル コンフィギュレーション モードで **dhcpd address** コマンドを使用します。既存の DHCP 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。

dhcpd address *IP_address1*[*-IP_address2*] *interface_name*

no dhcpd address *interface_name*

シンタックスの説明

interface_name	アドレス プールの割り当て先のインターフェイスです。
IP_address1	DHCP アドレス プールの開始アドレスです。
IP_address2	DHCP アドレス プールの終了アドレスです。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

dhcpd address *ip1*[*-ip2*] *interface_name* コマンドは、DHCP サーバのアドレス プールを指定します。セキュリティ アプライアンス DHCP サーバのアドレス プールは、それがイネーブルにされたセキュリティ アプライアンス インターフェイスと同じサブネット内にある必要があり、*interface_name* を使用して関連する セキュリティ アプライアンス インターフェイスを指定する必要があります。

アドレス プールのサイズは、セキュリティ アプライアンスでプールあたり 256 に制限されています。アドレス プールの範囲が 253 アドレスよりも大きい場合、セキュリティ アプライアンス インターフェイスのネットマスクは、クラス C アドレス（たとえば、255.255.255.0）にはできないため、それよりいくらか大きく、たとえば、255.255.254.0 にする必要があります。

DHCP クライアントは、物理的に セキュリティ アプライアンス DCHP サーバ インターフェイスのサブネットに接続されている必要があります。

dhcpd address コマンドでは、「-」記号がオブジェクト名の一部ではなく範囲指定子と解釈されるため、「-」（ダッシュ）文字を含むインターフェイス名は使用できません。

no dhcpd address *interface_name* コマンドは、指定されたインターフェイスに設定されている DHCP サーバ アドレス プールを削除します。

DHCP サーバ機能をセキュリティ アプライアンスに実装する方法については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

例

次の例は、セキュリティ アプライアンスの **dmz** インターフェイスに DHCP クライアントに対するアドレス プールおよび DNS サーバを設定するため、**dhcpd address**、**dhcpd dns**、および **dhcpd enable** *interface_name* コマンドを使用する方法を示しています。

```
hostname(config)# dhcpd address 10.0.1.100-10.0.1.108 dmz
hostname(config)# dhcpd dns 209.165.200.226
hostname(config)# dhcpd enable dmz
```

次の例は、内部インターフェイスに DHCP サーバを設定する方法を示しています。内部インターフェイスの DHCP サーバに 10 個の IP アドレスのプールを割り当てるため、**dhcpd address** コマンドを使用します。

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 198.162.1.2 198.162.1.3
hostname(config)# dhcpd wins 198.162.1.4
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd ping_timeout 1000
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	DHCP サーバの設定をすべて削除します。
dhcpd enable	指定したインターフェイス上で、DHCP サーバをイネーブルにします。
show dhcpd	DHCP のバインディング、統計情報、または状態情報を表示します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd auto_config

DHCP クライアントで実行されているインターフェイスから取得した値に基づいて、セキュリティ アプライアンスが DHCP サーバに対して DNS、WINS およびドメイン名を自動的に設定すること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 **dhcpd auto_config** コマンドを使用します。DHCP パラメータの自動設定を解除するには、このコマンドの **no** 形式を使用します。

dhcpd auto_config *client_if_name*

no dhcpd auto_config *client_if_name*

シンタックスの説明

client_if_name	DNS、WINS、およびドメイン名パラメータを提供する DHCP クライアントを実行している、インターフェイスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

CLI コマンドを使用して DNS、WINS、またはドメイン名パラメータを指定した場合、自動設定によって取得されたパラメータは、CLI により設定されたパラメータに上書きされます。

例

次の例は、内部インターフェイス上で DHCP を設定する方法を示しています。外部インターフェイス上の DHCP クライアントから取得した DNS、WINS、およびドメイン情報を、内部インターフェイス上の DHCP クライアントに渡すには **dhcpd auto_config** コマンドを使用します。

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd autoconfig outside
hostname(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	DHCP サーバの設定をすべて削除します。
dhcpd enable	指定したインターフェイス上で、DHCP サーバをイネーブルにします。
show ip address dhcp server	DHCP クライアントとして動作するインターフェイスに DHCP サーバから提供される、DHCP オプションに関する詳細情報を表示します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd dns

DHCP クライアントに対して DNS 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 **dhcpd dns** コマンドを使用します。定義されたサーバをクリアするには、このコマンドの **no** 形式を使用します。

dhcpd dns *dnsip1* [*dnsip2*]

no dhcpd dns [*dnsip1* [*dnsip2*]]

シンタックスの説明

dnsip1	DHCP クライアントに対するプライマリ DNS サーバの IP アドレスです。
dnsip2	（オプション）DHCP クライアントの代替 DNS サーバの IP アドレスです。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

dhcpd dns コマンドは、DNS サーバの IP アドレスまたはアドレスを DHCP クライアントに指定します。2 つの DNS サーバを指定できます。**no dhcpd dns** コマンドは、コンフィギュレーションから DNS IP アドレスを削除します。

例

次の例は、セキュリティ アプライアンスの **dmz** インターフェイスに DHCP クライアントに対するアドレス プールおよび DNS サーバを設定するため、**dhcpd address**、**dhcpd dns**、および **dhcpd enable** *interface_name* コマンドを使用する方法を示しています。

```
hostname(config)# dhcpd address 10.0.1.100-10.0.1.108 dmz
hostname(config)# dhcpd dns 192.168.1.2
hostname(config)# dhcpd enable dmz
```

関連コマンド

コマンド	説明
clear configure dhcpd	DHCP サーバの設定をすべて削除します。
dhcpd address	指定したインターフェイス上で DHCP サーバが使用するアドレス プールを指定します。
dhcpd enable	指定したインターフェイス上で、DHCP サーバをイネーブルにします。
dhcpd wins	DHCP クライアントに対して WINS サーバを定義します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd domain

DHCP クライアントに対して DNS ドメイン名を定義するには、グローバル コンフィギュレーション モードで **dhcpd domain** コマンドを使用します。DNS ドメイン名をクリアするには、このコマンドの **no** 形式を使用します。

dhcpd domain *domain_name*

no dhcpd domain [*domain_name*]

シンタックスの説明

domain_name	example.com などの DNS ドメイン名。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
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

dhcpd domain コマンドは、DHCP クライアントに対する DNS ドメイン名を指定します。**no dhcpd domain** コマンドは、コンフィギュレーションから DNS ドメイン サーバを削除します。

例

次の例は、セキュリティ アプライアンスで DHCP サーバにより DHCP クライアントに提供されるドメイン名を設定するために **dhcpd domain** コマンドを使用する方法を示しています。

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 198.162.1.2 198.162.1.3
hostname(config)# dhcpd wins 198.162.1.4
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd ping_timeout 1000
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	DHCP サーバの設定をすべて削除します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd enable

DHCP 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 **dhcpd enable** コマンドを使用します。DHCP 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。DHCP サーバには、DHCP クライアントへのネットワーク コンフィギュレーション パラメータがあります。セキュリティ アプライアンス内で DHCP サーバをサポートすることは、セキュリティ アプライアンス が DHCP を使用して、接続されているクライアントを設定できることを意味します。

dhcpd enable *interface*

no dhcpd enable *interface*

シンタックスの説明

interface	DHCP サーバをイネーブルにするインターフェイスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

dhcpd enable *interface* コマンドを使用すると、DHCP デーモンが DHCP イネーブル インターフェイス上で DHCP クライアントの要求のリスンを開始します。**no dhcpd enable** コマンドは、指定したインターフェイス上の DHCP サーバ機能をディセーブルにします。

（注） マルチ コンテキスト モードの場合、複数のコンテキストにより使用されているインターフェイス（共有 VLAN）で DHCP サーバをイネーブルにすることはできません。

セキュリティ アプライアンスが DHCP クライアント要求に応答する場合、要求が受信されたインターフェイスの IP アドレスとサブネット マスクを、デフォルト ゲートウェイの IP アドレスとサブネット マスクとして応答で使用します。

（注） セキュリティ アプライアンス DHCP サーバ デーモンは、直接セキュリティ アプライアンス インターフェイスに接続されていないクライアントをサポートしていません。

DHCP サーバ機能をセキュリティ アプライアンスに実装する方法については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

例

次の例は、DHCP サーバを内部インターフェイス上でイネーブルにするために **dhcpd enable** コマンドを使用する方法を示しています。

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 198.162.1.2 198.162.1.3
hostname(config)# dhcpd wins 198.162.1.4
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd ping_timeout 1000
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
debug dhcpd	DHCP サーバに対するデバッグ情報を表示します。
dhcpd address	指定したインターフェイス上で DHCP サーバが使用するアドレス プールを指定します。
show dhcpd	DHCP のバインディング、統計情報、または状態情報を表示します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd lease

DHCP リース期間を指定するには、グローバル コンフィギュレーション モードで **dhcpd lease** コマンドを使用します。リースの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。

dhcpd lease *lease_length*

no dhcpd lease [*lease_length*]

シンタックスの説明

lease_length	DHCP サーバから DHCP クライアントに与えられる、秒単位の、IP アドレスのリース期間です。有効値は 300 ～ 1,048,575 秒です。

デフォルト

デフォルトの *lease_length* は 3,600 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
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

dhcpd lease コマンドは、DHCP クライアントに与えたリース期間を秒単位で指定します。このリース期間は、DHCP サーバが割り当てた IP アドレスを DHCP クライアントが使用できる期間を示します。

no dhcpd lease コマンドは、コンフィギュレーションから指定したリース長を削除して、この値をデフォルト値の 3,600 秒に置き換えます。

例

次の例は、DHCP クライアントに対する DHCP 情報のリース期間を指定するために **dhcpd lease** コマンドを使用する方法を示しています。

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 198.162.1.2 198.162.1.3
hostname(config)# dhcpd wins 198.162.1.4
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd ping_timeout 1000
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	DHCP サーバの設定をすべて削除します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd option

DHCP オプ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 **dhcpd option** コマンドを使用します。オプションをクリアするには、このコマンドの **no** 形式を使用します。**dhcpd option** コマンドを使用して、TFTP サーバ情報を Cisco IP Phones およびルータに提供することができます。

dhcpd option *code* {***ascii*** *string*} | {***ip*** *IP_address* [*IP_address*]} | {***hex*** *hex_string*}

no dhcpd option *code*

シンタックスの説明

ascii	オプション パラメータが ASCII 文字列であることを指定します。
code	設定された DHCP オプションの番号を表します。有効値は、0 ～ 255 です。
hex	オプション パラメータが 16 進文字列であることを指定します。
hex_string	16 進文字列を、スペースのない偶数桁で指定します。0x プレフィックスを使用する必要はありません。
ip	オプション パラメータが IP アドレスであることを指定します。最大 2 つの IP アドレスを ***ip*** キーワードに指定できます。
IP_address	10 進数の IP アドレスを指定します。
string	スペースなしの ASCII 文字列を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

DHCP オプション要求がセキュリティ アプライアンス DHCP サーバに到着すると、セキュリティ アプライアンスは **dhcpd option** コマンドで指定された値を、クライアントに対する応答に入れます。

dhcpd option 66 および **dhcpd option 150** コマンドは、Cisco IP Phones およびルータがコンフィギュレーション ファイルをダウンロードするときに使用する TFTP サーバを指定します。次のようにコマンドを使用します。

- **dhcpd option 66 ascii** *string*。ここで、*string* は IP アドレスまたは TFTP サーバのホスト名です。オプション 66 には、TFTP サーバを 1 つだけ指定できます。
- **dhcpd option 150 ip** *IP_address* [*IP_address*]。ここで、*IP_address* は TFTP サーバの IP アドレスです。オプション 150 には、最大 2 つの IP アドレスを指定できます。

（注）　**dhcpd option 66** コマンドは ***ascii*** パラメータのみ受け付け、**dhcpd option 150** コマンドは ***ip*** パラメータのみ受け付けます。

dhcpd option 66 | 150 コマンドに IP アドレスを指定するときには、次のガイドラインに従ってください。

- TFTP サーバが DHCP サーバ インターフェイス上にある場合、TFTP サーバのローカル IP アドレスを使用します。
- TFTP サーバが DHCP サーバ インターフェイスよりもセキュリティが低いインターフェイス上にある場合は、一般の発信規則が適用されます。DHCP クライアント用の NAT エントリ、グローバル エントリ、および **access-list** エントリを作成し、TFTP サーバの実際の IP アドレスを使用します。
- TFTP　サーバがよりセキュリティの高いインターフェイス上にある場合は、一般の受信規則が適用されます。TFTP サーバ用のスタティック文と **access-list** 文のグループを作成し、TFTP サーバのグローバル IP アドレスを使用します。

その他の DHCP オプションの詳細については、RFC2132 を参照してください。

例

次の例は、DHCP オプション 66 に TFTP サーバを指定する方法を示しています。

```
hostname(config)# dhcpd option 66 ascii MyTftpServer
```

関連コマンド

コマンド	説明
clear configure dhcpd	DHCP サーバの設定をすべて削除します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd ping_timeout

DHCP PING のデフォルト タイムアウトを変更するには、グローバル コンフィギュレーション モードで **dhcpd ping_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。アドレスの競合を避けるため、DHCP サーバは、アドレスを DHCP クライアントに割り当てる前に 2 つの ICMP PING パケットをアドレスに送信します。このコマンドは、PING タイムアウトをミリ秒で指定します。

dhcpd ping_timeout *number*

no dhcpd ping_timeout

シンタックスの説明

number	ミリ秒単位の PING タイムアウト値です。最小値は 10、最大値は 10,000 です。デフォルトは 50 です。

デフォルト

number のデフォルトのミリ秒は 50 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

セキュリティ アプライアンスは、DHCP クライアントに IP アドレスを割り当てる前に、両方の ICMP PING パケットがタイムアウトになるのを待ちます。たとえば、デフォルト値が使用された場合、セキュリティ アプライアンスは IP アドレスを割り当てる前に、1,500 ミリ秒（各 ICMP PING パケットに対して 750 ミリ秒）待ちます。

PING のタイムアウト値が長いと、DHCP サーバのパフォーマンスに悪影響を及ぼす場合があります。

例

次の例は、**dhcpd ping_timeout** コマンドを使用して、DHCP サーバの PING タイムアウト値を変更する方法を示しています。

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 198.162.1.2 198.162.1.3
hostname(config)# dhcpd wins 198.162.1.4
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd ping_timeout 1000
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	DHCP サーバの設定をすべて削除します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd wins

DHCP クライアントに対して WINS 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 **dhcpd wins** コマンドを使用します。DHCP サーバから WINS サーバを削除するには、このコマンドの **no** 形式を使用します。

dhcpd wins *server1* [*server2*]

no dhcpd wins [*server1* [*server2*]]

シンタックスの説明

server1	プライマリの Microsoft NetBIOS ネーム サーバ（WINS サーバ）の IP アドレスを指定します。
server2	（オプション）代替の Microsoft NetBIOS ネーム サーバ（WINS サーバ）の IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

dhcpd wins コマンドは、WINS サーバのアドレスを DHCP クライアントに指定します。**no dhcpd wins** コマンドは、コンフィギュレーションから WINS サーバの IP アドレスを削除します。

例

次の例は、dhcpd wins コマンドを使用して、DHCP クライアントに送信された WINS サーバ情報を指定する方法を示しています。

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 198.162.1.2 198.162.1.3
hostname(config)# dhcpd wins 198.162.1.4
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd ping_timeout 1000
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	DHCP サーバの設定をすべて削除します。
dhcpd address	指定したインターフェイス上で DHCP サーバが使用するアドレス プールを指定します。
dhcpd dns	DHCP クライアントに対して DNS サーバを定義します。
show dhcpd	DHCP のバインディング、統計情報、または状態情報を表示します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcprelay enable

DHCP リレー エージェント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 **dhcprelay enable** コマンドを使用します。DHCP リレー エージェ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。DHCP リレー エージェントを使用すると、指定したセキュリティ アプライアンス インターフェイスから指定した DHCP サーバに DHCP 要求を転送できます。

dhcprelay enable *interface_name*

no dhcprelay enable *interface_name*

シンタックスの説明

interface_name	DHCP リレー エージェントがクライアント要求を受け入れるインターフェイス名です。

デフォルト

DHCP リレー エージェン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
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

dhcprelay enable *interface_name* コマンドによってセキュリティ アプライアンスが DHCP リレー エージェントを開始するようにするには、**dhcprelay server** コマンドがコンフィギュレーションにすでに存在している必要があります。そのコマンドがなければ、セキュリティ アプライアンスは次に示すようなエラー メッセージを表示します。

```
DHCPRA: Warning - There are no DHCP servers configured!
        No relaying can be done without a server!
        Use the 'dhcprelay server <server_ip> <server_interface>' command
```

次の条件下では、DHCP リレーをイネーブルにできません。

- 同じインターフェイス上で DHCP リレーと DHCP リレー サーバをイネーブルにすることはできません。
- 同じインターフェイス上で DHCP リレーと DHCP サーバ（**dhcpd enable**）をイネーブルにすることはできません。
- 1 つのコンテキストの DHCP リレーを、DHCP サーバと同時にイネーブルにすることはできません。
- マルチ コンテキスト モードの場合、複数のコンテキストにより使用されているインターフェイス（共有 VLAN）で DHCP リレーをイネーブルにすることはできません。

no dhcprelay enable *interface_name* コマンドは、*interface_name* で指定されたインターフェイスの DHCP リレー エージェント コンフィギュレーションだけを削除します。

例

次の例は、10.1.1.1 という IP アドレスを持つ DHCP サーバ用の DHCP リレー エージェントをセキュリティ アプライアンスの外部インターフェイス上に設定し、クライアント要求をセキュリティ アプライアンスの内部インターフェイス上に設定して、さらにタイムアウト値を 90 秒に設定する方法を示しています。

```
hostname(config)# dhcprelay server 10.1.1.1 outside
hostname(config)# dhcprelay timeout 90
hostname(config)# dhcprelay enable inside
hostname(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay enable inside
dhcprelay timeout 90
```

次の例は、DHCP リレー エージェントをディセーブルにする方法を示しています。

```
hostname(config)# no dhcprelay enable inside
hostname(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay timeout 90
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
debug dhcp relay	DHCP リレー エージェントに関するデバッグ情報を表示します。
dhcprelay server	DHCP リレー エージェントが、DHCP 要求の転送先にする DHCP サーバを指定します。
dhcprelay setroute	DHCP リレー エージェントが、DHCP 応答でデフォルト ルータ アドレスとして使用する IP アドレスを定義します。
show running-config dhcprelay	現在の DHCP リレー エージェント コンフィギュレーションを表示します。

dhcprelay server

DHCP 要求が転送される DHCP サーバを指定するには、グローバル コンフィギュレーション モードで **dhcpreplay server** コマンドを使用します。DHCP リレー コンフィギュレーションから DHCP サーバを削除するには、このコマンドの **no** 形式を使用します。DHCP リレー エージェントを使用すると、指定したセキュリティ アプライアンス インターフェイスから指定した DHCP サーバに DHCP 要求を転送できます。

dhcprelay server *IP_address interface_name*

no dhcprelay server *IP_address* [*interface_name*]

シンタックスの説明

interface_name	DHCP サーバが常駐するセキュリティ アプライアンス インターフェイス名です。
IP_address	DHCP リレー エージェントがクライアント DHCP 要求を転送する DHCP サーバの IP アドレスです。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

インターフェイスあたり最大 4 つの DHCP リレー サーバを追加できます。**dhcprelay enable** コマンドを入力する前に、少なくとも 1 つの **dhcprelay server** コマンドをセキュリティ アプライアンス コンフィギュレーションに追加する必要があります。DHCP リレー サーバが設定されているインターフェイス上に、DHCP クライアントを設定することはできません。

dhcprelay server コマンドは、指定したインターフェイスにある UDP ポート 67 を開き、**dhcprelay enable** コマンドがコンフィギュレーションに追加されるとすぐに DHCP リレー タスクを開始します。コンフィギュレーション内に **no dhcprelay enable** コマンドがあれば、ソケットは開かれず、DHCP リレー タスクは開始しません。

no dhcprelay server *IP_address* [*interface_name*] コマンドを使用すると、インターフェイスは DHCP パケットのサーバへの転送を停止します。

no dhcprelay server *IP_address* [*interface_name*] コマンドを使用すると、*IP_address* [*interface_name*] で指定された DHCP サーバ用の DHCP リレー エージェント コンフィギュレーションだけが削除されます。

例

次の例は、10.1.1.1 という IP アドレスを持つ DHCP サーバ用の DHCP リレー エージェントをセキュリティ アプライアンスの外部インターフェイス上に設定し、クライアント要求をセキュリティ アプライアンスの内部インターフェイス上に設定して、さらにタイムアウト値を 90 秒に設定する方法を示しています。

```
hostname(config)# dhcprelay server 10.1.1.1 outside
hostname(config)# dhcprelay timeout 90
hostname(config)# dhcprelay enable inside
hostname(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay enable inside
dhcprelay timeout 90
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
dhcprelay enable	指定したインターフェイス上で、DHCP リレー エージェントをイネーブルにします。
dhcprelay setroute	DHCP リレー エージェントが、DHCP 応答でデフォルト ルータ アドレスとして使用する IP アドレスを定義します。
dhcprelay timeout	DHCP リレー エージェントのタイムアウト値を指定します。
show running-config dhcprelay	現在の DHCP リレー エージェント コンフィギュレーションを表示します。

dhcprelay setroute

DHCP 応答にデフォルト ゲートウェイ アドレスを設定するには、グローバル コンフィギュレーション モードで **dhcprelay setroute** コマンドを使用します。デフォルト ルータを削除するには、このコマンドの **no** 形式を使用します。このコマンドを使用すると、DHCP 応答のデフォルト IP アドレスは、指定されたセキュリティ アプライアンス インターフェイスのアドレスに置き換えられます。

dhcprelay setroute *interface*

no dhcprelay setroute *interface*

シンタックスの説明

interface	最初のデフォルト IP アドレス（DHCP サーバから送信されるパケット内にある）を *interface* のアドレスに変更するように DHCP リレー エージェントを設定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

dhcprelay setroute *interface* コマンドを使用すると、DHCP リレー エージェントが最初のデフォルト ルータ アドレス（DHCP サーバから送信されるパケット内にある）を *interface* のアドレスに変更するように設定できます。

パケット内にデフォルトのルータ オプションがなければ、セキュリティ アプライアンスは、*interface* アドレスを含んでいるデフォルト ルータを追加します。その結果、クライアントは自分のデフォルト ルートがセキュリティ アプライアンスに向かうように設定できます。

dhcprelay setroute *interface* コマンドを設定しない場合（かつパケット内にデフォルトのルータ オプションがある場合）、パケットは、ルータ アドレスが変更されないままセキュリティ アプライアンスを通過します。

例

次の例は、**dhcprelay setroute** コマンドを使用して、DHCP 応答のデフォルト ゲートウェイを外部 DHCP サーバからセキュリティ アプライアンスの内部インターフェイスに設定する方法を示しています。

```
hostname(config)# dhcprelay server 10.1.1.1 outside
hostname(config)# dhcprelay timeout 90
hostname(config)# dhcprelay setroute inside
hostname(config)# dhcprelay enable inside
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
dhcprelay enable	指定したインターフェイス上で、DHCP リレー エージェントをイネーブルにします。
dhcprelay server	DHCP リレー エージェントが、DHCP 要求の転送先にする DHCP サーバを指定します。
dhcprelay timeout	DHCP リレー エージェントのタイムアウト値を指定します。
show running-config dhcprelay	現在の DHCP リレー エージェント コンフィギュレーションを表示します。

dhcprelay timeout

DHCP リレー エージェントのタイムアウト値を設定するには、グローバル コンフィギュレーション モードで **dhcprelay timeout** コマンドを使用します。タイムアウト値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。

dhcprelay timeout *seconds*

no dhcprelay timeout

シンタックスの説明

seconds	DHCP リレー アドレス ネゴシエーション用に許可されている時間（秒）を指定します。

デフォルト

dhcprelay タイムアウトのデフォルト値は 60 秒です。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
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

dhcprelay timeout コマンドは、DHCP サーバからの応答がリレー バインディング構造を通して DHCP クライアントに進むことが許されている時間の合計を秒単位で設定します。

例

次の例は、10.1.1.1 という IP アドレスを持つ DHCP サーバ用の DHCP リレー エージェントをセキュリティ アプライアンスの外部インターフェイス上に設定し、クライアント要求をセキュリティ アプライアンスの内部インターフェイス上に設定して、さらにタイムアウト値を 90 秒に設定する方法を示しています。

```
hostname(config)# dhcprelay server 10.1.1.1 outside
hostname(config)# dhcprelay timeout 90
hostname(config)# dhcprelay enable inside
hostname(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay enable inside
dhcprelay timeout 90
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
dhcprelay enable	指定したインターフェイス上で、DHCP リレー エージェントをイネーブルにします。
dhcprelay server	DHCP リレー エージェントが、DHCP 要求の転送先にする DHCP サーバを指定します。
dhcprelay setroute	DHCP リレー エージェントが、DHCP 応答でデフォルト ルータ アドレスとして使用する IP アドレスを定義します。
show running-config dhcprelay	現在の DHCP リレー エージェント コンフィギュレーションを表示します。

dir

ディレクトリの内容を表示するには、特権 EXEC モードで **dir** コマンドを使用します。

dir /[all] [*all-filesystems*] [**/recursive**] [**disk0: | disk1: | flash:** | **system:**] [*path*]

シンタックスの説明

/all	（オプション）すべてのファイルを表示します。
all-filesystems	（オプション）すべてのファイル システムのファイルを表示します。
disk0:	（オプション）内部フラッシュ メモリを指定し、続けてコロン（:）を入力します。
disk1:	（オプション）外部フラッシュ メモリ カードを指定し、続けてコロン（:）を入力します。
/recursive	（オプション）ディレクトリの内容を再帰的に表示します。
system:	（オプション）ファイル システムのディレクトリの内容を表示します。
flash:	（オプション）デフォルト フラッシュ パーティションのディレクトリの内容を表示します。
path	（オプション）特定のパスを指定します。

デフォルト

ディレクトリを指定しない場合のデフォルトのディレクトリは、現在の作業ディレクトリです。

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	このコマンドが導入されました。

使用上のガイドライン

キーワードまたは引数のない **dir** コマンドは、現在のディレクトリの内容を表示します。

例

次の例は、ディレクトリの内容を表示する方法を示しています。

```
hostname# dir
Directory of disk0:/

1      -rw-  1519        10:03:50 Jul 14 2003    my_context.cfg
2      -rw-  1516        10:04:02 Jul 14 2003    my_context.cfg
3      -rw-  1516        10:01:34 Jul 14 2003    admin.cfg
60985344 bytes total (60973056 bytes free)
```

次の例は、ファイル システム全体の内容を再帰的に表示する方法を示しています。

```
hostname# dir /recursive disk0:
Directory of disk0:/*
1      -rw-  1519        10:03:50 Jul 14 2003    my_context.cfg
2      -rw-  1516        10:04:02 Jul 14 2003    my_context.cfg
3      -rw-  1516        10:01:34 Jul 14 2003    admin.cfg
60985344 bytes total (60973056 bytes free)
```

次の例は、フラッシュ パーティションの内容を表示する方法を示しています。

```
hostname# dir flash:
Directory of disk0:/*
1      -rw-  1519        10:03:50 Jul 14 2003    my_context.cfg
2      -rw-  1516        10:04:02 Jul 14 2003    my_context.cfg
3      -rw-  1516        10:01:34 Jul 14 2003    admin.cfg
60985344 bytes total (60973056 bytes free)
```

関連コマンド

コマンド	説明
cd	現在の作業ディレクトリから、指定したディレクトリに移動します。
pwd	現在の作業ディレクトリを表示します。
mkdir	ディレクトリを作成します。
rmdir	ディレクトリを削除します。

disable

特権 EXEC モードを終了してユーザ EXEC モードに戻るには、特権 EXEC モードで **disable** コマンドを使用します。

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

enable コマンドを使用して、特権モードに入ります。**disable** コマンドは、特権モードを終了して、ユーザ モードに戻ります。

例

次の例は、特権モードに入る方法を示しています。

```
hostname> enable
hostname#
```

次の例は、特権モードを終了する方法を示しています。

```
hostname# disable
hostname>
```

関連コマンド

コマンド	説明
enable	特権 EXEC モードをイネーブルにします。

distance ospf

ルート タイプに基づいて OSPF ルートの管理ディスタンスを定義するには、ルータ コンフィギュレーション モードで **distance ospf** 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。

distance ospf [***intra-area*** *d1*] [***inter-area*** *d2*] [***external*** *d3*]

no distance ospf

シンタックスの説明

d1、*d2*、*d3*	各ルート タイプの距離です。有効な値は 1 ～ 255 です。
external	（オプション）再配布によって取得した他のルーティング ドメインからのルートに距離を設定します。
inter-area	（オプション）あるエリアから別のエリアまでのルートすべての距離を設定します。
intra-area	（オプション）あるエリア内のすべてのルートの距離を設定します。

デフォルト

d1、*d2*、および *d3* のデフォルト値は 110 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
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

少なくとも 1 つのキーワードと引数を指定する必要があります。管理ディスタンスのタイプごとにコマンドを個別に入力することができますが、コンフィギュレーションでは 1 つのコマンドとして表示されます。管理ディスタンスを再入力する場合、対象ルート タイプの管理ディスタンスだけが変更されます。その他のルート タイプの管理ディスタンスは影響されません。

コマンドの **no** 形式には、キーワードも引数もありません。コマンドの **no** 形式を使用すると、すべてのルート タイプの管理ディスタンスがデフォルトに戻されます。複数のルート タイプを設定している場合、1 つのルートタイプをデフォルトの管理ディスタンスに戻すには、次のいずれかを実行します。

- ルート タイプを、手動でデフォルト値に設定します。
- コマンドの **no** 形式を使用してコンフィギュレーション全体を削除してから、保持するルート タイプのコンフィギュレーションを再入力します。

例

次の例では、外部ルートの管理ディスタンスを 150 に設定します。

```
hostname(config-router)# distance ospf external 105
hostname(config-router)#
```

次の例は、各ルート タイプに入力した個別のコマンドが、ルータ コンフィギュレーションで 1 つのコマンドとして表示される方法を示しています。

```
hostname(config-router)# distance ospf intra-area 105 inter-area 105
hostname(config-router)# distance ospf intra-area 105
hostname(config-router)# distance ospf external 105
hostname(config-router)# exit
hostname(config)# show running-config router ospf 1
!
router ospf 1
 distance ospf intra-area 105 inter-area 105 external 105
!
hostname(config)#
```

次の例では、各管理ディスタンスを 105 に設定し、次に外部管理ディスタンスだけを 150 に変更する方法を示しています。**show running-config router ospf** コマンドは、どのように外部ルート タイプの値だけが変更され、その他のルート タイプが以前に設定された値を保持するかを示しています。

```
hostname(config-router)# distance ospf external 105 intra-area 105 inter-area 105
hostname(config-router)# distance ospf external 150
hostname(config-router)# exit
hostname(config)# show running-config router ospf 1
!
router ospf 1
 distance ospf intra-area 105 inter-area 105 external 150
!
hostname(config)#
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

dns domain-lookup

サポートされるコマンドに対してネーム ルックアップを実行するために、セキュリティ アプライアンスが DNS サーバに DNS 要求を送信すること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 **dns domain-lookup** コマンドを使用します。DNS lookup 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。

dns domain-lookup *interface_name*

no dns domain-lookup *interface_name*

シンタックスの説明

interface_name	DNS lookup をイネーブルにするインターフェイスを指定します。このコマンドを入力して、DNS lookup を複数のインターフェイス上でイネーブルにする場合、セキュリティ アプライアンスは応答を受信するまで各インターフェイスを順番に試します。

デフォルト

デフォルトでは、DNS lookup 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	このコマンドが導入されました。

使用上のガイドライン

DNS 要求を送信する DNS サーバ アドレスを設定するには、**dns name-server** コマンドを使用します。DNS lookup をサポートするコマンドのリストについては、**dns name-server** コマンドを参照してください。

セキュリティ アプライアンスは、ダイナミックにラーニングされたエントリで構成される名前解決のキャッシュを管理します。セキュリティ アプライアンスは、ホスト名から IP アドレスへの変換が必要になるたびに外部 DNS サーバにクエリーする代わりに、外部 DNS 要求から返された情報をキャッシュします。セキュリティ アプライアンスは、キャッシュにない名前に対してのみ要求を実行します。キャッシュのエントリは、DNS レコードの期限切れ、または 72 時間後のいずれか早い方に自動的にタイムアウトします。

例

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

```
hostname(config)# dns domain-lookup inside
```

関連コマンド

コマンド	説明
dns name-server	DNS サーバのアドレスを設定します。
dns retries	セキュリティ アプライアンスが応答を受信しないときに、一連の DNS サーバへのアクセスを再試行する回数を指定します。
dns timeout	次の DNS サーバを試すまでに待つ時間を指定します。
domain-name	デフォルトのドメイン名を設定します。
show dns-hosts	DNS キャッシュを表示します。

dns name-server

1 つまたは複数の DNS サーバを指定するには、グローバル コンフィギュレーション モードで **dns name-server** コマンドを使用します。サーバを削除するには、このコマンドの **no** 形式を使用します。セキュリティ アプライアンスは、WebVPN コンフィギュレーションまたは証明書コンフィギュレーションのサーバ名を解決するために DNS を使用します（サポートされるコマンド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）。サーバ名を定義するその他の機能は（AAA など）、DNS 解決をサポートしていません。IP アドレスを入力するか、**name** コマンドを使用して手動により名前を IP アドレスに解決する必要があります。

dns name-server *ip_address* [*ip_address2*] [*...*] [*ip_address6*]

no dns name-server *ip_address* [*ip_address2*] [*...*] [*ip_address6*]

シンタックスの説明

ip_address	DNS サーバの IP アドレスを指定します。最大 6 個のアドレスを個別のコマンドとして指定するか、利便性のために、1 つのコマンド内で 6 つまでのアドレスをスペースで分けて指定できます。1 つのコマンドに複数のサーバを入力する場合、セキュリティ アプライアンスは、各サーバをコンフィギュレーションの個別のコマンドに保存します。セキュリティ アプライアンスは、応答を受信するまで各 DNS サーバを順番に試します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

使用上のガイドライン

DNS lookup をイネーブルにするには、**dns domain-lookup** コマンドを設定します。DNS lookup をイネーブルにしない場合、DNS サーバは使用されません。

DNS 解決をサポートする WebVPN コマンドには、次のコマンドが含まれます。

- **server (pop3s)**
- **server (imap4s)**
- **server (smtps)**
- **port-forward**
- **url-list**

DNS 解決をサポートする certificate コマンドには、次のコマンドが含まれます。

- **enrollment url**
- **url**

name コマンドを使用すると、名前と IP アドレスを手動で入力できます。

セキュリティ アプライアンスが 一連の DNS サーバを再試行する回数を設定するには、**dns retries** コマンドを参照してください。

例

次の例では、3 つの DNS サーバを追加します。

```
hostname(config)# dns name-server 10.1.1.1 10.2.3.4 192.168.5.5
```

セキュリティ アプライアンスは、次のようにコンフィギュレーションを個別のコマンドとして保存します。

```
dns name-server 10.1.1.1
dns name-server 10.2.3.4
dns name-server 192.168.5.5
```

2 つのサーバを追加するには、それらを 1 つのコマンドとして入力できます。

```
hostname(config)# dns name-server 10.5.1.1 10.8.3.8
hostname(config)# show running-config dns
dns name-server 10.1.1.1
dns name-server 10.2.3.4
dns name-server 192.168.5.5
dns name-server 10.5.1.1
dns name-server 10.8.3.8
...
```

それらを 2 つのコマンドとして入力することもできます。

```
hostname(config)# dns name-server 10.5.1.1
hostname(config)# dns name-server 10.8.3.8
```

複数のサーバを削除するには、それらのサーバを、次のように複数のコマンドとして、または 1 つのコマンドとして入力できます。

```
hostname(config)# no dns name-server 10.5.1.1 10.8.3.8
```

関連コマンド

コマンド	説明
dns domain-lookup	セキュリティ アプライアンスがネーム ルックアップを実行できるようにします。
dns retries	セキュリティ アプライアンスが応答を受信しないときに、一連の DNS サーバへのアクセスを再試行する回数を指定します。
dns timeout	次の DNS サーバを試すまでに待つ時間を指定します。
domain-name	デフォルトのドメイン名を設定します。
show dns-hosts	DNS キャッシュを表示します。

dns retries

セキュリティ アプライアンスが応答を受信しないときに、一連の DNS サーバへのアクセスを再試行する回数を指定するには、グローバル コンフィギュレーション モードで **dns retries** 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。

dns retries *number*

no dns retries [*number*]

シンタックスの説明

number	再試行の回数を 0 ～ 10 の間で指定します。デフォルトは 2 です。

デフォルト

デフォルトでは、再試行の回数は 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
7.0	このコマンドが導入されました。

使用上のガイドライン

dns name-server コマンドを使用して DNS サーバを追加します。

例

次の例では、再試行の回数を 0 に設定します。セキュリティ アプライアンスは各サーバを 1 回ずつ試します。

```
hostname(config)# dns retries 0
```

関連コマンド

コマンド	説明
dns domain-lookup	セキュリティ アプライアンスがネーム ルックアップを実行できるようにします。
dns name-server	DNS サーバのアドレスを設定します。
dns timeout	次の DNS サーバを試すまでに待つ時間を指定します。
domain-name	デフォルトのドメイン名を設定します。
show dns-hosts	DNS キャッシュを表示します。

dns timeout

次の DNS サーバを試すまで待機する時間を指定するには、グローバル コンフィギュレーション モードで **dns timeout** コマンドを使用します。デフォルトのタイムアウトに戻すには、このコマンドの **no** 形式を使用します。

dns timeout *seconds*

no dns timeout [*seconds*]

シンタックスの説明

seconds	タイムアウトを 1 ～ 30 の間の秒単位で指定します。デフォルトは 2 秒です。セキュリティ アプライアンスが一連のサーバを試すたびに、このタイムアウトは倍増します。試行回数を設定するには、**dns retries** コマンドを参照してください。

デフォルト

デフォルトのタイムアウトは 2 秒です。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

例

次の例では、タイムアウトを 1 秒に設定します。

```
hostname(config)# dns timeout 1
```

関連コマンド

コマンド	説明
dns name-server	DNS サーバのアドレスを設定します。
dns retries	セキュリティ アプライアンスが応答を受信しないときに、一連の DNS サーバへのアクセスを再試行する回数を指定します。
dns domain-lookup	セキュリティ アプライアンスがネーム ルックアップを実行できるようにします。
domain-name	デフォルトのドメイン名を設定します。
show dns-hosts	DNS キャッシュを表示します。

dns-server

プライマリおよびセカンダリの DNS サーバの IP アドレスを設定するには、グループポリシー モードで **dns-server** コマンドを使用します。この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、DNS サーバを別のグループポリシーから継承できます。サーバを継承しないようにするには、**dns-server none** コマンドを使用します。

dns-server {**value** *ip_address* [*ip_address*] | none}

no dns-server

シンタックスの説明

none	dns サーバに、ヌル値を設定して DNS サーバを許可しません。デフォルトのグループポリシーまたは指定されているグループポリシーから値を継承しないようにします。
value *ip_address*	プライマリおよびセカンダリ DNS サーバの IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

使用上のガイドライン

dns-server コマンドを実行するたびに、既存の設定が上書きされます。たとえば、DNS サーバ x.x.x.x を設定し、次に DNS サーバ y.y.y.y を設定した場合、2 番目のコマンドは最初のコマンドを上書きし、y.y.y.y が唯一の DNS サーバになります。サーバを複数設定する場合も同様です。以前に設定された DNS サーバを上書きする代わりにサーバを追加するには、このコマンドを入力するときにすべての DNS サーバの IP アドレスを含めます。

例

次の例は、FirstGroup という名前のグループポリシーで、IP アドレスが 10.10.10.15、10.10.10.30、および 10.10.10.45 の DNS サーバを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# dns-server value 10.10.10.15 10.10.10.30 10.10.10.45
```

domain-name

デフォルトのドメイン名を設定するには、グローバル コンフィギュレーション モードで **domain-name** コマンドを使用します。ドメイン名を削除するには、このコマンドの **no** 形式を使用します。セキュリティ アプライアンスは、修飾子を持たない名前の拡張子として、ドメイン名を付加します。 たとえば、ドメイン名を「example.com」と設定し、syslog サーバを、修飾子を持たない「jupiter」という名前で　指定した場合、名前は、セキュリティ　アプライアンスにより「jupiter.example.com.」と修飾されます。

domain-name *name*

no domain-name [*name*]

シンタックスの説明

name	ドメイン名を設定します。最大長は 63 文字です。

デフォルト

デフォルト ドメイン名は、default.domain.invalid です。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
既存	このコマンドは既存のものです。

使用上のガイドライン

マルチ コンテキスト モードの場合、システム実行スペース内だけでなく、各コンテキストでもドメイン名を設定できます。

例

次の例では、ドメインを example.com に設定します。

```
hostname(config)# domain-name example.com
```

関連コマンド

コマンド	説明
dns domain-lookup	セキュリティ アプライアンスがネーム ルックアップを実行できるようにします。
dns name-server	DNS サーバのアドレスを設定します。
hostname	セキュリティ アプライアンスのホスト名を設定します。
show running-config domain-name	ドメイン名のコンフィギュレーションを表示します。

downgrade

オペレーティング システム ソフトウェア（ソフトウェア イメージ）の以前のバージョンにダウングレードするには、特権 EXEC モードで ***downgrade*** コマンドを使用します。

注意　PIX セキュリティ アプライアンスが現在 PIX Version 7.0 以降を実行している場合は、以前のバージョンのソフトウェアをロードしないでください。PIX Version 7.0 ファイル システムがインストールされている PIX セキュリティ アプライアンスに、モニタ モードからソフトウェア イメージをロードすることは、予測できない動作を発生させるため、サポートされていません。ダウングレード プロセスを簡単に行うために用意された、実行中の PIX Version 7.0 イメージから、***downgrade*** コマンドを使用することをお勧めします。

downgrade *image_url* **[activation-key [flash** | *4-part_key* | *file***]] [config** *start_config_url***]**

シンタックスの説明

4-part_key	（オプション）イメージに書き込むための 4 分割アクティベーション キーを指定します。 5 分割キーを使用する場合、4 分割キーに戻ることにより失われる可能性がある機能のリストと共に、警告が生成されます。 システム フラッシュが再フォーマットまたは消去された場合、ダウングレード用のデフォルト キーは使用できなくなります。その場合、CLI はコマンドラインにアクティベーション キーを入力するように求めます。これは、***activation-key*** のキーワードがコマンドラインで指定されていない場合のデフォルトの動作です。
activation-key	（オプション）ダウングレードされたソフトウェア イメージで使用するアクティベーション キーを指定します。
config	（オプション）スタートアップ コンフィギュレーション ファイルを指定します。
file	（オプション）ダウングレード手順が完了した後で使用するパス /URL およびアクティベーション キー ファイルの名前を指定します。アップグレード プロセス中にフラッシュに保存されたファイルが、ソースのイメージ ファイルだった場合、このファイル内のアクティベーション キーがダウングレードで使用されます。
flash	（オプション）フラッシュ メモリで 5 分割アクティベーション キーを使用する前にデバイスで使用されていた、4 分割アクティベーション キーを検索するように指定します。これは、***activation-key*** のキーワードがコマンドラインで指定されていない場合のデフォルトの動作です。
image_url	ダウングレードするソフトウェア イメージのパス/URL および名前を指定します。ソフトウェア イメージは、7.0 以前のバージョンである必要があります。
start_config_url	（オプション）ダウングレード手順が完了した後で使用するパス /URL およびコンフィギュレーション ファイルの名前を指定します。

デフォルト

activation-key のキーワードが指定されていない場合、セキュリティ アプライアンスは最後に使用された 4 分割アクティベーション キーを試します。セキュリティ アプライアンスがフラッシュで 4 分割アクティベーション キーを検出できなかった場合、コマンドは拒否され、エラー メッセージが表示されます。この場合、次回にコマンドラインで有効な 4 分割アクティベーション キーを指定する必要があります。デフォルトのアクティベーション キーまたはユーザ指定のアクティベーション キーが、現在有効なアクティベーション キーと比較されます。選択されたアクティベーション キーを使用することで、機能を損失する可能性がある場合、ダウングレード後に、損失する可能性のある機能のリストと共に警告が表示されます。

スタートアップ コンフィギュレーション ファイルが指定されていない場合、セキュリティ アプライアンスはデフォルトで downgrade.cfg を使用します。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、ソフトウェア リリース 7.0 以降を実行している Cisco PIX Firewall シリーズのセキュリティ アプライアンスに限り使用できます。このコマンドは、Cisco ASA 5500 シリーズのセキュリティ アプライアンスではサポートされていません。

注意

ダウングレード プロセス中に電源障害が発生すると、フラッシュ メモリが破損する場合があります。予防策として、ダウングレード プロセスを開始する前に、フラッシュ メモリ上のすべてのデータを外部デバイスにバックアップしてください。

破損したフラッシュ メモリを回復するには、コンソールへの直接アクセスが必要です。詳細については、***format*** コマンドを参照してください。

例

次の例では、ソフトウェアをリリース 6.3.3 にダウングレードします。

```
hostname# downgrade tftp://17.13.2.25//tftpboot/mananthr/cdisk.6.3.3 activation-key
32c261f3 062afe24 c94ef2ea 0e299a3f
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!

Buffering startup config

All items have been buffered successfully.
If the flash reformat is interrupted or fails, data in flash will be lost
and the system might drop to monitor mode.
Do you wish to continue? [confirm]
Installing the correct file system for the image and saving the buffered data
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!
Flash downgrade succeeded








Rebooting....

Enter zero actkey:
```

次の例は、無効なアクティベーション キーを入力した場合の結果を示しています。

```
hostname# downgrade tftp://17.13.2.25//tftpboot/mananthr/cdisk.6.3.3 activation-key
0 0 0 0
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!
Error: activation key entered is invalid.

Enter the file option when there is no actkey in the source image (happens if the
source is in tftp server).
```

次の例は、ソース イメージのアクティベーション キーを指定したときに、それが存在しなかった場合の結果を示しています。

```
hostname# downgrade tftp://17.13.2.25//tftpboot/mananthr/cdisk.6.3.3 activation-key
file
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!
Activation key does not exist in the source image.
Please use the activation-key option to specify an activation key.
```

次の例は、最後のプロンプトでダウングレード手順を中止する方法を示しています。

```
hostname# downgrade tftp://17.13.2.25//tftpboot/mananthr/cdisk.6.3.3
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!

Buffering startup config

All items have been buffered successfully.
If the flash reformat is interrupted or fails, data in flash will be lost
and the system might drop to monitor mode.
Do you wish to continue? [confirm] ===<typed n here>
Downgrade process terminated.
```

ダウングレードするには、ソフトウェア バージョンが 7.0 未満である必要があります。次の例は、ソフトウェアのダウングレードに失敗した試行を示しています。

```
hostname# downgrade tftp://17.13.2.25//scratch/views/test/target/sw/cdisk
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Error: Need to use an image with version less than 7-0-0-0.
```

次の例は、イメージを指定したときにアクティベーション キーを確認しなかった場合の結果を示しています。

```
hostname# downgrade tftp://17.13.2.25//tftpboot/mananthr/cdisk.4.4.1-rel
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Image checksum has not been verified
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Warning: Activation key not verified.
Key 32c261f3 633fe24 c94ef2ea e299a3f might be incompatible with the image version
4-4-1-0.
Do you wish to continue? [confirm]
Downgrade process terminated.
Please enter an activation-key in the command line.
```

次の例は、4 分割アクティベーション キーに、現在の 5 分割アクティベーション キーのすべての機能が含まれていない場合の結果を示しています。

```
hostname# downgrade tftp://17.13.2.25//tftpboot/mananthr/cdisk.6.3.3
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!
The following features available in current activation key in flash
are NOT available in 4 tuple activation key in flash:
VPN-3DES-AES
GTP/GPRS
5 Security Contexts
Failover is different:
current activation key in flash: UR(estricted)
4 tuple activation key in flash: R(estricted)
Some features might not work in the downgraded image if this key is used.
Do you wish to continue? [confirm]
Downgrade process terminated.
Please enter an activation-key in the command line.
```

関連コマンド

コマンド	説明
copy running-config startup-config	現在実行中のコンフィギュレーションをフラッシュ メモリに保存します。

drop

指定された GTP メッセージをドロップするには、**gtp-map** コマンドを使用してアクセスされる GTP マップ コンフィギュレーション モードで **drop** コマンドを使用します。コマンドを削除するには、**no** 形式を使用します。

drop {apn *access_point_name* **| message** *message_id* **| version** *version*}

no drop {apn *access_point_name* **| message** *message_*id **| version** *version*}

シンタックスの説明

apn	指定されたアクセス ポイント ネームの GTP メッセージをドロップします。
access_point_name	ドロップされる APN のテキスト文字列です。
message	特定の GTP メッセージをドロップします。
message_id	ドロップするメッセージの英数字の識別子です。有効な範囲は 1 ～ 255 です。
version	指定されたバージョンの GTP メッセージをドロップします。
version	バージョン 0 を識別するには 0 を、バージョン 1 を識別するには 1 を使用します。GTP のバージョン 0 は ポート 2123 を使用し、バージョン 1 はポート 3386 を使用します。

デフォルト

有効なメッセージ ID、APN、およびバージョンを持つすべてのメッセージが検査されます。

任意の APN が許可されています。

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
GTP 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	このコマンドが導入されました。

使用上のガイドライン

ネットワークで許可しない特定の GTP メッセージをドロップするには、**drop message** コマンドを使用します。

指定されたアクセス ポイントの GTP メッセージをドロップするには、**drop apn** コマンドを使用します。指定されたバージョンの GTP メッセージをドロップするには、**drop version** コマンドを使用します。

例

次の例では、トラフィックをメッセージ ID 20 にドロップします。

```
hostname(config)# gtp-map qtp-policy
hostname(config-gtpmap)# drop message 20
```

関連コマンド

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

duplex

銅（RJ-45）のイーサネット インターフェイスのデュプレックス方式を設定するには、インターフェイス コンフィギュレーション モードで **duplex** コマンドを使用します。デュプレックス設定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。

duplex {***auto*** | ***full*** | ***half***}

no duplex

シンタックスの説明

auto	デュプレックス モードを自動検出します。
full	デュプレックス モードを全二重に設定します。
half	デュプレックス モードを半二重に設定します。

デフォルト

デフォルトは auto 検出です。

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	このコマンドが、**interface** コマンドのキーワー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

デュプレックス モードは、物理インターフェイス上にだけ設定します。

duplex コマンドは、ファイバ メディアでは使用できません。

ネットワークが自動検出をサポートしていない場合は、デュプレックス モードを特定の値に設定します。

ASA 5500 シリーズ適応型セキュリティ アプライアンスの RJ-45 インターフェイスでは、デフォルトのオートネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレート ケーブルが検出されると、内部クロスオーバーを実行して、クロス ケーブルによる接続を不要にします。インターフェイスで Auto-MDI/MDIX をイネーブルにするには、速度またはデュプレックス方式のいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックス方式の両方に明示的に固定値を設定して、両方の設定に関するオートネゴシエーションをディセーブルにすると、Auto-MDI/MDIX もディセーブルになります。

例

次の例では、デュプレックス モードを全二重に設定します。

```
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
```

関連コマンド

コマンド	説明
clear configure interface	インターフェイスのコンフィギュレーションをすべて消去します。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
show interface	インターフェイスのランタイム ステータスと統計情報を表示します。
show running-config interface	インターフェイスのコンフィギュレーションを表示します。
speed	インターフェイスの速度を設定します。

email

登録中に、指定された電子メール アドレスを証明書のサブジェクト代替名の拡張に含めるには、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 **email** 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。

email *address*

no email

シンタックスの説明

address	電子メール アドレスを指定します。*address* の最大長は 64 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
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	このコマンドが導入されました。

例

次の例では、トラストポイント central の暗号 CA トラストポイント コンフィギュレーション モードに入り、トラストポイント central の登録要求に電子メールアドレスの jjh@nhf.net を含めます。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# email jjh@nhf.net
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 コンフィギュレーション モードに入ります。

enable

特権 EXEC モードに入るには、ユーザ EXEC モードで **enable** コマンドを使用します。

enable [*level*]

シンタックスの説明

level	（オプション）特権レベルは 0 ～ 15 の間です。

デフォルト

特権レベル 15 を入力します。ただし、コマンドの認可を使用している場合は、デフォルトのレベルはユーザ名に設定されたレベル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
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

デフォルトのイネーブル パスワードはブランクです。パスワードを設定するには、**enable password** コマンドを参照してください。

デフォルトである 15 以外の特権レベルを使用するには、ローカル コマンド認可を設定し（**aaa authorization** コマンドを参照。***LOCAL*** キーワードを指定する）、**privilege** コマンドを使用して、コマンドを別の特権レベルに設定します。ローカル コマンド認可を設定しない場合は、イネーブル レベルが無視され、設定したレベルにかかわらずレベル 15 にアクセスできます。現在の特権レベルを表示するには、**show curpriv** コマンドを使用します。

レベル 2 以上は特権 EXEC モードに入ります。レベル 0 およびレベル 1 は、ユーザ EXEC モードに入ります。

disable コマンドを入力して、特権 EXEC モードを終了します。

例

次の例では、特権 EXEC モードに入ります。

```
hostname> enable
Password: Pa$$w0rd
hostname#
```

次の例では、レベル 10 の特権 EXEC モードに入ります。

```
hostname> enable 10
Password: Pa$$w0rd10
hostname#
```

関連コマンド

コマンド	説明
enable password	イネーブル パスワードを設定します。
disable	特権 EXEC モードを終了します。
aaa authorization command	コマンド認可を設定します。
privilege	ローカル コマンド認可のためのコマンド特権レベルを設定します。
show curpriv	現在ログインしているユーザの名前および特権レベルを表示します。

enable (webvpn)

WebVPN または電子メール プロキシのアクセスを設定済みのインターフェイス上でイネーブルにするには、enable コマンドを使用します。WebVPN の場合、このコマンドは webvpn モードで使用します。電子メール プロキシ（IMAP4S、POP3S、SMTPS）の場合、このコマンドは適切な電子メール プロキシ モードで使用します。インターフェイスの WebVPN をディセーブルにするには、このコマンドの **no** バージョンを使用します。

enable *ifname*

no enable

シンタックスの説明

ifname	設定済みのインターフェイスを指定します。インターフェイスを設定するには **nameif** コマンドを使用します。

デフォルト

WebVPN 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
Webvpn	•	—	•	—	—
Imap4s	•	—	•	—	—
Pop3s	•	—	•	—	—
SMTPS	•	—	•	—	—

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

例

次の例は、Outside という名前のインターフェイス上で WebVPN をイネーブルにする方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# enable Outside
```

次の例は、Outside という名前のインターフェイス上で POP3S 電子メール プロキシを設定する方法を示しています。

```
hostname(config)# pop3s
hostname(config-pop3s)# enable Outside
```

enable password

特権 EXEC モードのイネーブル パスワードを設定するには、グローバル コンフィギュレーション モードで **enable password** コマンドを使用します。15 以外のレベルのパスワードを削除するには、このコマンドの **no** 形式を使用します。レベル 15 のパスワードは削除できません。

enable password *password* **[level** *level*] [***encrypted***]

no enable password level *level*

シンタックスの説明

encrypted	（オプション）パスワードが暗号化された形式であることを指定します。パスワードは暗号化された形式でコンフィギュレーションに保存されるため、パスワードの入力後に元のパスワードを表示することはできません。何らかの理由でパスワードを別のセキュリティ アプライアンスにコピーする必要があるが、元のパスワードを知らない場合、暗号化されたパスワードとこのキーワードを使用して、**enable password** コマンドを入力します。通常、このキーワードは、**show running-config enable** コマンドを入力したときにだけ表示されます。
level *level*	（オプション）特権レベル 0 ～ 15 のパスワードを設定します。
password	パスワードに、大文字と小文字が区別される最大 16 文字の英数字および特殊文字の文字列を設定します。パスワードには疑問符（?）とスペースを除く任意の文字を使用できます。

デフォルト

デフォルトのパスワードはブランクです。デフォルトのレベルは、15 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

イネーブル レベル 15（デフォルトのレベル）のデフォルトのパスワードは、ブランクです。パスワードをブランクにリセットする場合は、*password* にテキストを入力しないでください。

マルチ コンテキスト モードでは、各コンテキストだけでなく、システム コンフィギュレーションにもイネーブル パスワードを作成できます。

デフォルトである 15 以外の特権レベルを使用するには、ローカル コマンド認可を設定し（**aaa authorization** コマンドを参照。***LOCAL*** キーワードを指定する）、**privilege** コマンドを使用して、コマンドを別の特権レベルに設定します。ローカル コマンド認可を設定しない場合は、イネーブル レベルが無視され、設定したレベルにかかわらずレベル 15 にアクセスできます。現在の特権レベルを表示するには、**show curpriv** コマンドを使用します。

レベル 2 以上は特権 EXEC モードに入ります。レベル 0 およびレベル 1 は、ユーザ EXEC モードに入ります。

例

次の例では、イネーブル パスワードを Pa$$w0rd に設定します。

```
hostname(config)# enable password Pa$$w0rd
```

次の例では、レベル 10 のイネーブル パスワードを Pa$$w0rd10 に設定します。

```
hostname(config)# enable password Pa$$w0rd10 level 10
```

次の例では、イネーブル パスワードを別のセキュリティ アプライアンスからコピーした暗号化されたパスワードに設定します。

```
hostname(config)# enable password jMorNbK0514fadBh encrypted
```

関連コマンド

コマンド	説明
aaa authorization command	コマンド認可を設定します。
enable	特権 EXEC モードに入ります。
privilege	ローカル コマンド認可のためのコマンド特権レベルを設定します。
show curpriv	現在ログインしているユーザの名前および特権レベルを表示します。
show running-config enable	イネーブル パスワードを暗号化された形式で表示します。

enforcenextupdate

NextUpdate CRL フィールドの処理方法を指定するには、ca-crl コンフィギュレーション モードで **enforcenextupdate** コマンドを使用します。これが設定された場合、このコマンドは CRL の NextUpdate フィールドを無効にしないことを要求します。使用されない場合、セキュリティ アプライアンスは、不明または無効な CRL の NextUpdate フィールドを許可します。

無効または不明な NextUpdate フィールドを許可するには、このコマンドの **no** 形式を使用します。

enforcenextupdate

no enforcenextupdate

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

デフォルト設定は実行（オン）です。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

例

次の例では、ca-crl コンフィギュレーション モードに入り、CRL の NextUpdate フィールドをトラストポイント central に対して期限切れにしないことを要求します

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# enforcenextupdate
hostname(ca-crl)#
```

関連コマンド

コマンド	説明
cache-time	キャッシュのリフレッシュ時間を分単位で指定します。
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。

enrollment retry count

リトライ回数を指定するには、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 **enrollment retry count** コマンドを使用します。セキュリティ アプライアンスは、証明書を要求した後、CA から証明書を受信するまで待機します。設定されたリトライ期間内にセキュリティ アプライアンスが証明書を受信しない場合、別の証明書要求が送信されます。セキュリティ アプライアンスが応答を受信するか、リトライ回数が設定回数に達するまで、要求は繰り返されます。

リトライ回数の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。

enrollment retry count *number*

no enrollment retry count

シンタックスの説明

number	登録要求の送信を再試行する最大回数です。有効な範囲は 0、1 ～ 100 リトライです。

デフォルト

number のデフォルト設定は、0（無制限）です。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドはオプションであり、自動登録を設定している場合のみ適用されます。

例

次の例では、トラストポイント central の暗号 CA トラストポイント コンフィギュレーション モードに入り、トラストポイント central 内で登録のリトライ回数を 20 リトライに設定します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment retry count 20
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 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。
enrollment retry period	登録要求を再送信するまでの待機時間を、分単位で指定します。

enrollment retry period

リトライ期間を指定するには、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 **enrollment retry period** コマンドを使用します。セキュリティ アプライアンスは、証明書を要求した後、CA から証明書を受信するまで待機します。指定されたリトライ期間内にセキュリティ アプライアンスが証明書を受信しない場合、別の証明書要求が送信されます。

リトライ期間の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。

enrollment retry period *minutes*

no enrollment retry period

シンタックスの説明

minutes	登録要求の送信を試行する分単位の間隔です。有効な範囲は 1 ～ 60 分です。

デフォルト

デフォルト設定は 1 分です。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
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	このコマンドが導入されました。

使用上のガイドライン

このコマンドはオプションであり、自動登録を設定している場合のみ適用されます。

例

次の例では、トラストポイント central の暗号 CA トラストポイント コンフィギュレーション モードに入り、トラストポイント central 内で登録のリトライ期間を 10 分に設定します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment retry period 10
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 コンフィギュレーション モードに入ります。
default enrollment	すべての登録パラメータをシステムのデフォルト値に戻します。
enrollment retry count	登録を要求するリトライの回数を定義します。

enrollment terminal

このトラストポイントでのカット アンド ペースト登録を指定するには（手動登録とも呼ばれる）、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 **enrollment terminal** コマンドを使用します。このコマンドの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。

enrollment terminal

no enrollment terminal

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルト設定はオフです。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
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	このコマンドが導入されました。

例

次の例では、トラストポイント central の暗号 CA トラストポイント コンフィギュレーション モードに入り、トラストポイント central の CA 登録のカット アンド ペースト方式を指定します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment terminal
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 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。
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	登録要求を再送信するまでの待機時間を、分単位で指定します。
enrollment url	このトラストポイントでの自動登録（SCEP）を指定し、URL を設定します。

enrollment url

このトラストポイントで登録し、登録 URL を設定するために自動登録（SCEP）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 **enrollment url** コマンドを使用します。このコマンドの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。

enrollment url *url*

no enrollment url

シンタックスの説明

url	自動登録で使用する URL の名前を指定します。最大長は 1,000 文字（実質上の無制限）です。

デフォルト

デフォルト設定はオフです。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
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	このコマンドが導入されました。

例

次の例では、トラストポイント central の暗号 CA トラストポイント コンフィギュレーション モードに入り、トラストポイント central の SCEP 登録を URL https://enrollsite で指定します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment url https://enrollsite
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 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。
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	登録要求を再送信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。

erase

ファイル システムを消去して再フォーマットするには、特権 EXEC モードで ***erase*** コマンドを使用します。このコマンドは、非表示のシステム ファイルを含むすべてのファイルを上書きし、ファイル システムを消去してからファイル システムを再インストールします。

erase [**disk0: | disk1: | flash:**]

シンタックスの説明

disk0:	（オプション）内部フラッシュ メモリを指定し、続けてコロン（:）を入力します。
disk1:	（オプション）外部のコンパクト フラッシュ メモリ カードを指定し、続けてコロン（:）を入力します。
flash:	（オプション）内部フラッシュ メモリを指定し、続けてコロン（:）を入力します。

注意　フラッシュ メモリを消去すると、フラッシュ メモリに保存されているライセンス情報も削除されます。フラッシュ メモリを消去する前に、ライセンス情報を保存してください。

ASA 5500 シリーズでは、***flash*** キーワードは ***disk0*** のエイリアスです。

デフォルト

このコマンドにデフォルト設定はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

使用上のガイドライン

erase コマンドは、OxFF パターンを使用してフラッシュ メモリ上のすべてのデータを消去し、空のファイル システム割り当てテーブルをデバイスに書き換えます。

すべての可視ファイル（非表示のシステム ファイルを除く）を削除するには、***erase*** コマンドではなく、***delete /recursive*** コマンドを使用します。

（注）　Cisco PIX セキュリティ アプライアンスでは、***erase*** コマンドと ***format*** コマンドは同じ処理を実行します。ユーザ データを 0xFF パターンを使用して破棄します。

（注）　Cisco ASA 5500 シリーズのセキュリティ アプライアンスでは、***erase*** コマンドを実行すると、ディスク上のすべてのユーザ データが 0xFF パターンを使用して破棄されます。一方、***format*** コマンドはファイル システムの制御構造をリセットするだけです。生ディスク読み取りツールを使用すると、この情報はまだ参照できる可能性があります。

例

次の例では、ファイル システムを消去して再フォーマットします。

```
hostname# erase flash:
```

関連コマンド

コマンド	説明
delete	非表示のシステム ファイルを除く、すべての可視ファイルを削除します。
format	すべてのファイル（非表示のシステム ファイルを含む）を消去して、ファイル システムをフォーマットします。

established

確立されている接続に基づくポート上のリターン接続を許可するには、グローバル コンフィギュレーション モードで **established** コマンドを使用します。**established** 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。

established *est_protocol dport* [*sport*] [**permitto** *protocol port* [*-port*]] [**permitfrom** *protocol port*[*-port*]]

no established *est_protocol dport* [*sport*] [**permitto** *protocol port* [*-port*]] [**permitfrom** *protocol port*[*-port*]]

シンタックスの説明

est_protocol	確立されている接続のルックアップに使用する IP プロトコル（UDP または TCP）を指定します。
dport	確立されている接続のルックアップに使用する宛先ポートを指定します。
permitfrom	（オプション）指定されたポートから発信されるリターン プロトコル接続を許可します。
permitto	（オプション）指定されたポート宛のリターン プロトコル接続を許可します。
port [*-port*]	（オプション）リターン接続の（UDP または TCP）宛先ポートを指定します。
protocol	（オプション）リターン接続により使用される IP プロトコル（UDP または TCP）です。
sport	（オプション）確立されている接続のルックアップに使用する送信元ポートを指定します。

デフォルト

デフォルトは次のとおりです。

- *dport*：0（ワイルドカード）
- *sport*：0（ワイルドカード）

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド 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	***to*** および ***from*** キーワードが、CLI から削除されました。代わりに ***permitto*** および ***permitfrom*** キーワードを使用してください。

使用上のガイドライン

established コマンドは、発信接続がセキュリティ アプライアンスを通してリターン アクセスするのを許可します。このコマンドは、セキュリティ アプライアンスによって保護されているネットワークからの元の接続の発信、および外部ホスト上の同じ 2 つのデバイス間のリターン接続着信と共に動作します。**established** コマンドを使用すると、接続のルックアップに使用する宛先ポートを指定できます。この追加によって、コマンドをさらに制御できるようになり、宛先ポートは既知であるが、送信元ポートは未知のプロトコルをサポートできます。**permitto** と **permitfrom** キーワードは、リターン着信接続を定義します。

注意　常に **permitto** キーワードおよび **permitfrom** キーワードと共に **established** コマンドを指定するよう推奨します。これらのキーワードを指定せずに **established** コマンドを使用すると、外部システムに接続するときに、それらのシステムが接続に関係する内部ホストに無制限に接続できるため、セキュリティ リスクになる恐れがあります。この状況は、内部システムへの攻撃に利用される可能性があります。

次の例は、**established** コマンドを正しく使用しなかった場合に発生する可能性のあるセキュリティ違反を示しています。

この例は、内部システムがポート 4000 上の外部ホストに TCP 接続を作成した場合、外部ホストは、任意のプロトコルを使用して任意のポート上に戻れることを示しています。

```
hostname(config)# established tcp 0 4000
```

使用するポートをプロトコルが指定しない場合、送信元ポートおよび宛先ポートを **0** に指定できます。必要な場合に限り、ワイルドカード ポート（0）を使用します。

```
hostname(config)# established tcp 0 0
```

（注）　**established** コマンドが正しく動作するには、クライアントが **permitto** キーワードで指定したポート上でリスンしている必要があります。

established コマンドは、**nat 0** コマンド（**global** コマンドがない）を付けて使用できます。

（注）　**established** コマンドを、PAT と共に使用することはできません。

セキュリティ アプライアンスは、**established** コマンドと連携して XDMCP をサポートしています。

注意　セキュリティ アプライアンスを介して XWindows システム アプリケーションを使用すると、セキュリティ リスクになる恐れがあります。

XDMCP は、デフォルトでオンになっていますが、**established** コマンドを次のように入力するまでセッションは作成されません。

```
hostname(config)# established tcp 0 6000 to tcp 6000 from tcp 1024-65535
```

established コマンドを入力すると、内部の XDMCP（UNIX または ReflectionX）搭載ホストが、外部の XDMCP 搭載 XWindows サーバにアクセスできます。UDP/177 ベースの XDMCP が TCP ベースの XWindows セッションをネゴシエートし、それに続く TCP リターン接続が許可されます。リターン トラフィックの送信元ポートが不明であるため、*sport* フィールドは 0（ワイルドカード）と指定する必要があります。*dport* は、6000 + *n* である必要があります。ここで、*n* は、ローカル ディスプレイ番号です。UNIX コマンドを使用して、この値を変更します。

```
hostname(config)# setenv DISPLAY hostname:displaynumber.screennumber
```

established コマンドが必要な理由は、多くの TCP 接続が生成され（ユーザとの対話に基づき）、これらの接続に使用される送信元ポートが不明であるためです。宛先ポートだけがスタティックです。セキュリティ アプライアンスは、XDMCP フィックスアップを透過的に行います。設定は不要ですが、TCP セッションに対応するには **established** コマンドの入力が必要です。

例

この例では、2 つのホスト間の、プロトコル A を使用した SRC ポート B からポート C を宛先とする接続を示しています。セキュリティ アプライアンスおよびプロトコル D（プロトコル A はプロトコル D と異なる可能性がある）を通過するリターン接続を許可するには、送信元ポートはポート F に対応し、宛先ポートはポート E に対応している必要があります。

```
hostname(config)# established A B C permitto D E permitfrom D F
```

この例は、内部ホストから外部ホストに対し、TCP 送信元ポート 6060 と任意の宛先ポートを使用して接続を開始する方法を示しています。セキュリティ アプライアンスは、このホスト間に TCP 宛先ポート 6061 と TCP 送信元ポート 6059 を経由するリターン トラフィックを許可します。

```
hostname(config)# established tcp 6060 0 permitto tcp 6061 permitfrom tcp 6059
```

この例は、内部ホストから外部ホストに対し、UPD 宛先ポート 6060 と任意の送信元ポートを使用して接続を開始する方法を示しています。セキュリティ アプライアンスは、このホスト間に TCP 宛先ポート 6061 と TCP 送信元ポート 1024-65535 を経由するリターン トラフィックを許可します。

```
hostname(config)# established udp 0 6060 permitto tcp 6061 permitfrom tcp 1024-65535
```

次の例は、ローカル ホスト 10.1.1.1 が外部のホスト 209.165.201.1 に対してポート 9999 上で TCP 接続を開始する方法を示しています。この例では、外部ホスト 209.165.201.1 のポート 4242 からのパケットがローカル ホスト 10.1.1.1 のポート 5454 に戻ることが許可されます。

```
hostname(config)# established tcp 9999 permitto tcp 5454 permitfrom tcp 4242
```

次の例は、外部ホスト 209.165.201.1 の任意のポートからローカル ホスト 10.1.1.1 のポート 5454 に戻るパケットを許可する方法を示しています。

```
hostname(config)# established tcp 9999 permitto tcp 5454
```

関連コマンド

コマンド	説明
clear configure established	確立されたコマンドをすべて削除します。
show running-config established	確立されている接続に基づく、許可済みの着信接続を表示します。

exceed-mss

スリーウェイ ハンドシェイクの間にピアによって設定された TCP の最大セグメント サイズを超えるデータ長のパケットを許可またはドロップするには、tcp マップ コンフィギュレーション モードで **exceed-mss** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

exceed-mss {**allow** | **drop**}

no exceed-mss {**allow** | **drop**}

シンタックスの説明

allow	MSS を超えるパケットを許可します。
drop	MSS を超えるパケットをドロップします。

デフォルト

デフォルトでは、パケットはドロップされます。

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
tcp マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

使用上のガイドライン

tcp-map コマンドをモジュラ ポリシー フレームワーク インフラストラクチャとともに使用します。トラフィックのクラスを **class-map** コマンドを使用して定義し、TCP 検査を **tcp-map** コマンドを使用してカスタマイズします。その新しい TCP マップを **policy-map** コマンドを使用して適用します。TCP 検査を **service-policy** コマンドを使用して有効にします。

tcp-map コマンドを使用して、tcp マップ コンフィギュレーション モードに入ります。スリーウェイ ハンドシェイクの間にピアによって設定された TCP の最大セグメント サイズを超えるデータ長の TCP パケットをドロップするには、tcp マップ コンフィギュレーション モードの **exceed-mss** コマンドを使用します。

例

次の例では、ポート 21 で MSS を超過するパケットを送信するフローを許可します。

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# exceed-mss allow
hostname(config)# class-map cmap
hostname(config-cmap)# match port tcp eq ftp
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラスマップを指定します。
help	**policy-map**、**class**、および **description** コマンドのシンタックス ヘルプを表示します。
policy-map	ポリシー（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
set connection	接続値を設定します。
tcp-map	TCP マップを作成し、tcp マップ コンフィギュレーション モードにアクセスできるようにします。

exit

現在のコンフィギュレーション モードを終了するか、特権 EXEC モードまたはユーザ EXEC モードからログアウトするには、**exit** コマンドを使用します。

exit

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

キー シーケンス ***Ctrl+Z*** を使用しても、グローバル コンフィギュレーション モード（およびそれ以上のモード）を終了できます。このキー シーケンスは、特権 EXEC モードおよびユーザ EXEC モードでは機能しません。

特権 EXEC モードまたはユーザ EXEC モードで **exit** コマンドを入力すると、セキュリティ アプライアンスからログアウトします。特権 EXEC モードからユーザ EXEC モードに戻るには、**disable** コマンドを使用します。

例

次の例は、**exit** コマンドを使用して、グローバル コンフィギュレーション モードを終了してセッションからログアウトする方法を示しています。

```
hostname(config)# exit
hostname# exit

Logoff
```

次の例は、**exit** コマンドを使用してグローバル コンフィギュレーション モードを終了する方法と、**disable** コマンドを使用して特権 EXEC モードを終了する方法を示しています。

```
hostname(config)# exit
hostname# disable
hostname>
```

関連コマンド

コマンド	説明
quit	コンフィギュレーション モードを終了します。または、特権 EXEC モードまたはユーザ EXEC モードからログアウトします。

failover

フェールオーバー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 **failover** コマンドを使用します。フェールオーバー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。

failover

no failover

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

フェールオーバー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	このコマンドは、コンフィギュレーションでフェールオーバーをイネーブルまたはディセーブルにすることに制限されています（**failover active** コマンドを参照してください）。

使用上のガイドライン

フェールオーバーをディセーブルにするには、このコマンドの **no** 形式を使用します。

注意

フェールオーバー リンクおよびステートフル フェールオーバー リンク経由で送信される情報は、フェールオーバー キーを使用して通信をセキュリティで保護しない限り、すべてクリア テキストで送信されます。VPN トンネルの終端にセキュリティ アプライアンスを使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザ名、パスワード、および事前共有キーが含まれています。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになる恐れがあります。セキュリティ アプライアンスを使用して VPN トンネルを終端する場合は、フェールオーバー通信をフェールオーバー キーによってセキュリティで保護することをお勧めします。

例

次の例では、フェールオーバーをディセーブルにします。

```
hostname(config)# no failover
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure failover	**failover** コマンドを実行コンフィギュレーションから消去し、フェールオーバーのデフォルト値に戻します。
failover active	アクティブにするスタンバイ装置を切り替えます。
show failover	装置のフェールオーバー ステータスに関する情報を表示します。
show running-config failover	実行コンフィギュレーション内の **failover** コマンドを表示します。

failover active

スタンバイ セキュリティ アプライアンスまたはフェールオーバー グループをアクティブ状態にするには、特権 EXEC モードで **failover active** コマンドを使用します。スタンバイするアクティブなセキュリティ アプライアンスまたはフェールオーバー グループを切り替えるには、このコマンドの **no** 形式を使用します。

failover active [***group*** *group_id*]

no failover active [***group*** *group_id*]

シンタックスの説明

group *group_id*	（オプション）アクティブにするフェールオーバー グループを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0	このコマンドは、新しいフェールオーバー グループを含めるように修正されました。

使用上のガイドライン

failover active コマンドを使用して、スタンバイ装置からフェールオーバー スイッチを起動します。または、アクティブな装置から **no failover active** コマンドを起動して、フェールオーバー スイッチを起動します。この機能を使用して、障害が発生した装置をサービスに戻し、メンテナンスのため、アクティブ装置を強制的にオフラインにします。ステートフル フェールオーバーを使用していない場合、すべてのアクティブな接続はドロップされます。フェールオーバーが発生した後、クライアントはそれらの接続を再度確立する必要があります。

フェールオーバー グループの切り替えは、Active/Active フェールオーバーでのみ利用可能です。フェールオーバー グループを指定せずに Active/Active フェールオーバー装置に **failover active** コマンドを入力した場合、装置上のすべてのグループがアクティブになります。

例

次の例では、スタンバイ グループ 1 をアクティブにしています。

```
hostname# failover active group 1
```

関連コマンド

コマンド	説明
failover reset	セキュリティ アプライアンスを、障害が発生した状態からスタンバイに変更します。

failover group

Active/Active フェールオーバー グループを設定するには、グローバル コンフィギュレーション モードで **failover group** コマンドを使用します。フェールオーバー 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。

failover group *num*

no failover group *num*

シンタックスの説明

num	フェールオーバー グループの番号。有効値は、1 または 2 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	このコマンドが導入されました。

使用上のガイドライン

最大 2 つのフェールオーバー グループを定義できます。**failover group** コマンドは、マルチ コンテキスト モード用に設定されたデバイスのシステム コンテキストにだけ追加できます。フェールオーバー グループの作成と登録は、フェールオーバーがディセーブルにされている場合のみ可能です。

このコマンドを入力すると、フェールオーバー グループ コマンド モードに入ります。**primary**、**secondary**、**preempt**、**replication http**、**interface-policy**、**mac address**、および **polltime interface** コマンドは、フェールオーバー グループ コンフィギュレーション モードで使用できます。グローバル コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。

（注）　**failover polltime interface**、**failover interface-policy**、**failover replication http**、および **failover mac address** コマンドは、Active/Active フェールオーバー コンフィギュレーションに影響を与えません。それらのコマンドは、フェールオーバー コンフィギュレーション モードの **polltime interface**、**interface-policy**、**replication http**、および **mac address** コマンドによって上書きされます。

フェールオーバー グループを削除するときは、フェールオーバー グループ 1 を最後に削除する必要があります。フェールオーバー グループ 1 には、常に管理コンテキストが含まれています。フェールオーバー グループに割り当てられていないコンテキストは、デフォルトによりフェールオーバー グループ 1 に割り当てられます。コンテキストが明示的に割り当てられているフェールオーバー グループは削除できません。

（注）　同じネットワーク上に Active/Active フェールオーバー ペアが複数ある場合は、あるペアのインターフェイスに割り当てられているものと同じデフォルト仮想 MAC アドレスが、他のペアのインターフェイスに割り当てられることがあります。これは、デフォルト仮想 MAC アドレスの決定方法に基づいた動作です。ネットワーク上の MAC アドレスを重複させないためには、**mac address** コマンドを使用して、各物理インターフェイスに必ずアクティブとスタンバイの仮想 MAC アドレスを割り当てるようにしてください。

例

次の例（抜粋）は、2 つのフェールオーバー 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)# exit
hostname(config)# failover group 2
hostname(config-fover-group)# secondary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
asr-group	非対称のルーティング インターフェイス グループ ID を指定します。
interface-policy	モニタリングがインターフェイス障害を検出したときのフェールオーバー ポリシーを指定します。
join-failover-group	フェールオーバー グループにコンテキストを割り当てます。
mac address	フェールオーバー グループ内のコンテキストの仮想 MAC アドレスを定義します。
polltime interface	監視されているインターフェイスに送信される hello メッセージの間隔を指定します。
preempt	リブート後、優先順位がより高い装置がアクティブな装置になるように指定します。
primary	プライマリ装置に、フェールオーバー グループに対するより高い優先順位を指定します。
replication http	選択されたフェールオーバー グループに対して HTTP セッションの複製を指定します。
secondary	セカンダリ装置に、フェールオーバー グループに対するより高い優先順位を指定します。

failover interface ip

フェールオーバー インターフェイスとステートフル フェールオーバー インターフェイスに対して IP アドレスとマスクを指定するには、グローバル コンフィギュレーション モードで **failover interface ip** コマンドを使用します。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。

failover interface ip *if_name ip_address mask* ***standby*** *ip_address*

no failover interface ip *if_name ip_address mask* ***standby*** *ip_address*

シンタックスの説明

if_name	フェールオーバーまたはステートフル フェールオーバー インターフェイスのインターフェイス名です。
ip_address mask	プライマリ モジュール上のフェールオーバーまたはステートフル フェールオーバー インターフェイスに対して、IP アドレスとマスクを指定します。
standby *ip_address*	セカンダリ モジュールがプライマリ モジュールとの通信に使用する IP アドレスを指定します。

デフォルト

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	このコマンドが導入されました。

使用上のガイドライン

フェールオーバーおよびステートフル フェールオーバー インターフェイスは、レイヤ 3 の機能です。そのことは、セキュリティ アプライアンスが透過的なファイアウォール モードで動作していたり、システムにグローバルであったりしても変わりません。

マルチ コンテキスト モードでは、システム コンテキストでフェールオーバーを設定します（**monitor-interface** コマンドを除く）。

このコマンドは、セキュリティ アプライアンスを LAN フェールオーバー用にブートストラップするときにコンフィギュレーションに含める必要があります。

例

次の例は、フェールオーバー インターフェイスに対して IP アドレスとマスクを指定する方法を示しています。

```
hostname(config)# failover interface ip lanlink 172.27.48.1 255.255.255.0 standby
172.27.48.2
```

関連コマンド

コマンド	説明
clear configure failover	**failover** コマンドを実行コンフィギュレーションから消去し、フェールオーバーのデフォルト値に戻します。
failover lan interface	フェールオーバー通信に使用するインターフェイスを指定します。
failover link	ステートフル フェールオーバーに使用するインターフェイスを指定します。
monitor-interface	指定されたインターフェイスのヘルスを監視します。
show running-config failover	実行コンフィギュレーション内の **failover** コマンドを表示します。

failover interface-policy

モニタリングがインターフェイス障害を検出したときのフェールオーバーのポリシーを指定するには、グローバル コンフィギュレーション モードで **failover interface-policy** コマンドを使用します。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。

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

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

シンタックスの説明

num	パーセンテージとして使用されるときは 1 ～ 100 の数字を指定し、番号として使用されるときは 1 からインターフェイスの最大数の数字を指定します。
%	（オプション）数字 *num* が、監視されている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

デフォルトは次のとおりです。

- *port* は 1 です。
- 物理インターフェイスのモニタリングは、デフォルトでイネーブルになっています。論理インターフェイスのモニタリングは、デフォルトで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	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、スペースはありません。

障害が発生したインターフェイスの数が、設定されたポリシーの条件を満たしており、その他のセキュリティ アプライアンスが正常に機能している場合、セキュリティ アプライアンスは、自らに障害が発生したとマーク付けしてフェールオーバーが発生する可能性があります（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。

（注） このコマンドが適用されるのは、Active/Standby フェールオーバーのみです。Active/Active フェールオーバーでは、フェールオーバー グループ コンフィギュレーション モードの **interface-policy** コマンドを使用して、各フェールオーバー グループのインターフェイス ポリシーを設定します。

例

次の例では、フェールオーバー ポリシーを指定する 2 つの方法を示しています。

```
hostname(config)# failover interface-policy 20%

hostname(config)# failover interface-policy 5
```

関連コマンド

コマンド	説明
failover polltime	装置とインターフェイスのポーリング回数を指定します。
failover reset	障害が発生した装置を、障害が発生する前の状態に戻します。
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。
show failover	装置のフェールオーバー状態に関する情報を表示します。

failover key

フェールオーバー ペアの装置間で暗号化および認証された通信のキーを指定するには、グローバル コンフィギュレーション モードで **failover key** コマンドを使用します。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。

failover key {*secret* | ***hex*** *key*}

no failover key

シンタックスの説明

hex *key*	暗号キー用の 16 進値を指定します。キーは、32 個の 16 進文字（0-9、a-f）にする必要があります。
secret	英数字の共有秘密を指定します。秘密には 1 ～ 63 文字を設定できます。有効な文字は、番号、文字、または句読点の任意の組み合せです。共有秘密は、暗号キーを生成するために使用します。

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)	このコマンドは、**failover lan key** から **failover key** に修正されました。
7.0(4)	このコマンドは、***hex*** *key* キーワードおよび引数を含めるように変更されました。

使用上のガイドライン

装置間のフェールオーバー通信を暗号化して認証するには、共有秘密または 16 進キーを使用して両方の装置を設定する必要があります。フェールオーバー キーを指定しない場合、フェールオーバー通信はクリアで送信されます。

（注） PIX セキュリティ アプライアンス プラットフォームでは、装置を接続するために専用のシリアル フェールオーバー ケーブルを使用している場合、フェールオーバーが設定されていても、フェールオーバー リンク経由の通信は暗号化されません。フェールオーバー キーは LAN ベースのフェールオーバー通信だけを暗号化します。

注意　フェールオーバー リンクおよびステートフル フェールオーバー リンク経由で送信される情報は、フェールオーバー キーを使用して通信をセキュリティで保護しない限り、すべてクリア テキストで送信されます。VPN トンネルの終端にセキュリティ アプライアンスを使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザ名、パスワード、および事前共有キーが含まれています。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになる恐れがあります。セキュリティ アプライアンスを使用して VPN トンネルを終端する場合は、フェールオーバー通信をフェールオーバー キーによってセキュリティで保護することをお勧めします。

例

次の例は、フェールオーバー ペアの装置間のフェールオーバー通信を保護するために共有秘密を指定する方法を示しています。

```
hostname(config)# failover key abcdefg
```

次の例は、フェールオーバー ペアの装置間のフェールオーバー通信を保護するために 16 進キーを指定する方法を示しています。

```
hostname(config)# failover key hex 6a1ed228381cf5c68557cb0c32e614dc
```

関連コマンド

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

failover lan enable

LAN ベースのフェールオーバーを PIX セキュリティ アプライアンス上で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 **failover lan enable** コマンドを使用します。LAN ベースのフェールオーバー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。

failover lan enable

no failover lan 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

イネーブルになっていません。

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

このコマンドの **no** 形式を使用して LAN ベースのフェールオーバーをディセーブルにした場合、フェールオーバー ケーブルがインストールされている場合はケーブル ベースのフェールオーバーが使用されます。このコマンドは、PIX セキュリティ アプライアンスでのみ使用できます。

注意

フェールオーバー リンクおよびステートフル フェールオーバー リンク経由で送信される情報は、フェールオーバー キーを使用して通信をセキュリティで保護しない限り、すべてクリア テキストで送信されます。VPN トンネルの終端にセキュリティ アプライアンスを使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザ名、パスワード、および事前共有キーが含まれています。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになる恐れがあります。セキュリティ アプライアンスを使用して VPN トンネルを終端する場合は、フェールオーバー通信をフェールオーバー キーによってセキュリティで保護することをお勧めします。

例

次の例では、LAN ベースのフェールオーバーをイネーブルにします。

```
hostname(config)# failover lan enable
```

関連コマンド

コマンド	説明
failover lan interface	フェールオーバー通信に使用するインターフェイスを指定します。
failover lan unit	LAN ベースのフェールオーバーでの、プライマリ装置またはセカンダリ装置を指定します。
show failover	装置のフェールオーバー ステータスに関する情報を表示します。
show running-config failover	実行コンフィギュレーション内の **failover** コマンドを表示します。

failover lan interface

フェールオーバー通信に使用されるインターフェイスを指定するには、グローバル コンフィギュレーション モードで **failover lan interface** コマンドを使用します。フェールオーバー 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。

failover lan interface *if_name phy_if*

no failover lan interface *if_name phy_if*

シンタックスの説明

if_name	フェールオーバー専用のセキュリティ アプライアンス インターフェイスの名前を指定します。
phy_if	物理インターフェイスまたは論理インターフェイスのポートを指定します。

デフォルト

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
既存	このコマンドが、*phy_if* 引数を含めるように修正されました。

使用上のガイドライン

LAN フェールオーバーでは、フェールオーバー トラフィックを送信するための専用のインターフェイスが必要です。ただし、ステートフル フェールオーバー リンクに対しては、LAN フェールオーバー インターフェイスを使用することもできます。

（注） LAN フェールオーバーとステートフル フェールオーバーの両方に対して同じインターフェイスを使用する場合、インターフェイスには LAN ベースのフェールオーバーとステートフル フェールオーバーの両方のトラフィックを処理するための十分な容量が必要です。

デバイス上の使用されていない任意のイーサネット インターフェイスを、フェールオーバー インターフェイスとして使用できます。現在名前で設定されているインターフェイスは指定できません。フェールオーバー インターフェイスは、通常のネットワーク インターフェイスとしては設定されません。フェールオーバー通信専用です。このインターフェイスは、フェールオーバー リンクのために（およびオプションで状態リンクのために）だけ使用する必要があります。LAN ベースのフェールオーバー リンクは、リンクにホストまたはルータのない専用スイッチを使用するか、装置を直接リンクするためのクロスオーバー イーサネット ケーブルを使用して接続できます。

（注）　VLAN を使用する場合は、フェールオーバー リンクのための専用 VLAN を使用します。フェールオーバー リンク VLAN を他の VLAN と共有すると、断続的なトラフィック障害や PING および ARP 障害が発生する場合があります。スイッチを使用してフェールオーバー リンクに接続する場合、スイッチ上の専用インターフェイスと、フェールオーバー リンク用のセキュリティ アプライアンスを使用してください。通常のネットワーク トラフィックを伝送するサブインターフェイスを持つインターフェイスを共有しないでください。

マルチ コンテキスト モードを実行しているシステム上では、フェールオーバー リンクはシステム コンテキスト内にあります。このインターフェイスと状態リンク（使用されている場合）が、システム コンテキスト内にある設定可能な唯一のインターフェイスです。他のインターフェイスは、すべてセキュリティ コンテキストに割り当てられ、セキュリティ コンテキスト内から設定されます。

（注）　フェールオーバー リンクの IP アドレスおよび MAC アドレスは、フェールオーバー時に変更されません。

このコマンドの **no** 形式も、フェールオーバー インターフェイスの IP アドレス設定をクリアします。

このコマンドは、セキュリティ アプライアンスを LAN フェールオーバー用にブートストラップするときにコンフィギュレーションに含める必要があります。

例

次の例では、フェールオーバー LAN インターフェイスを設定します。

```
hostname(config)# failover lan interface folink e4
```

関連コマンド

コマンド	説明
failover lan enable	PIX セキュリティ アプライアンス上で、LAN ベースのフェールオーバーをイネーブルにします。
failover lan unit	LAN ベースのフェールオーバーでの、プライマリ装置またはセカンダリ装置を指定します。
failover link	ステートフル フェールオーバー インターフェイスを指定します。

failover lan unit

LAN フェールオーバー設定でセキュリティ アプライアンスをプライマリ装置またはセカンダリ装置のいずれかに設定するには、グローバル コンフィギュレーション モードで **failover lan unit** 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。

failover lan unit {***primary*** | ***secondary***}

no failover lan unit {***primary*** | ***secondary***}

シンタックスの説明

primary	セキュリティ アプライアンスをプライマリ装置として指定します。
secondary	セキュリティ アプライアンスをセカンダリ装置として指定します。

デフォルト

セカンダリです。

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

Active/Standby フェールオーバーの場合、フェールオーバー装置のプライマリ宛先およびセカンダリ宛先は、ブート時にどちらの装置がアクティブになるかを指定します。次の状態が発生すると、プライマリ装置がブート時にアクティブ装置になります。

- プライマリ装置およびセカンダリ装置の両方が、最初のフェールオーバー ポーリング チェック内にブート シーケンスを完了した。
- プライマリ装置がセカンダリ装置の前にブートした。

プライマリ装置がブートするときにセカンダリ装置がすでにアクティブであった場合、プライマリ装置はアクティブではなくスタンバイ装置になります。この場合、強制的にプライマリ装置をアクティブ ステータスに戻すために、**no failover active** コマンドをセカンダリ（アクティブ）装置に発行する必要があります。

Active/Active フェールオーバーに対して、各フェールオーバー グループにはプライマリ装置またはセカンダリ装置のプリファレンスが割り当てられます。このプリファレンスは、両方の装置が同時に起動する場合（フェールオーバー ポーリング期間内で）、フェールオーバー グループのコンテキストのフェールオーバー ペアのどの装置をアクティブにするかを決定します。

このコマンドは、セキュリティ アプライアンスを LAN フェールオーバー用にブートストラップするときにコンフィギュレーションに含める必要があります。

例

次の例では、LAN ベースのフェールオーバーでセキュリティ アプライアンスをプライマリ装置として設定します。

```
hostname(config)# failover lan unit primary
```

関連コマンド

コマンド	説明
failover lan enable	PIX セキュリティ アプライアンス上で、LAN ベースのフェールオーバーをイネーブルにします。
failover lan interface	フェールオーバー通信に使用するインターフェイスを指定します。

failover link

ステートフル フェールオーバー インターフェイスを指定するには、グローバル コンフィギュレーション モードで **failover link** コマンドを使用します。ステートフル フェールオーバー 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。

failover link *if_name* [*phy_if*]

no failover link

シンタックスの説明

if_name	ステートフル フェールオーバー専用のセキュリティ アプライアンス インターフェイスの名前を指定します。
phy_if	（オプション）物理インターフェイスまたは論理インターフェイスのポートを指定します。ステートフル フェールオーバー インターフェイスが、フェールオーバー通信に割り当てられたインターフェイスまたは標準ファイアウォール インターフェイスを共有している場合、この引数は必要ありません。

デフォルト

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
既存	このコマンドが、*phy_if* 引数を含めるように修正されました。
7.0(4)	このコマンドは、標準ファイアウォール インターフェイスを受け入れるように修正されました。

使用上のガイドライン　物理インターフェイスまたは論理インターフェイスの引数は、フェールオーバー通信または標準ファイアウォール インターフェイスを共有していない場合に必要です。

failover link コマンドは、ステートフル フェールオーバーをイネーブルにします。**no failover link** コマンドを入力して、ステートフル フェールオーバー機能をディセーブルにします。専用のステートフル フェールオーバー インターフェイスを使用している場合、**no failover link** コマンドもステートフル フェールオーバー インターフェイス IP アドレス設定をクリアします。

ステートフル フェールオーバーを使用するには、すべての状態情報を渡すようにステートフル フェールオーバー リンクを設定する必要があります。ステートフル フェールオーバー リンクの設定には、3 つのオプションがあります。

- ステートフル フェールオーバー リンク専用のイーサネット インターフェイスを使用できます。
- LAN ベースのフェールオーバーを使用している場合、フェールオーバー リンクを共有できます。
- 内部インターフェイスなどの通常のデータ インターフェイスを共有できます。ただし、このオプションは推奨されていません。

ステートフル フェールオーバー リンク専用のイーサネット インターフェイスを使用している場合、スイッチまたは装置を直接接続するクロスケーブルを使用できます。スイッチを使用する場合、このリンク上に他のホストまたはルータは設定できません。

（注）　セキュリティ アプライアンスに直接接続するシスコ スイッチ ポート上で PortFast オプションをイネーブルにします。

フェールオーバー リンクをステートフル フェールオーバー リンクとして使用している場合、利用可能な最速のイーサネット インターフェイスを使用する必要があります。インターフェイス上でパフォーマンスの低下が見られる場合は、別のインターフェイスをステートフル フェールオーバー インターフェイス専用にすることを検討してください。

ステートフル フェールオーバー リンクとしてデータ インターフェイスを使用する場合は、そのインターフェイスをステートフル フェールオーバー リンクとして指定しようとすると次の警告が表示されます。

```
******* WARNING ***** WARNING ******* WARNING ****** WARNING  *********
  Sharing Stateful failover interface with regular data interface is not
  a recommended configuration due to performance and security concerns.
******* WARNING ***** WARNING ******* WARNING ****** WARNING  *********
```

データ インターフェイスをステートフル フェールオーバー インターフェイスと共有すると、リプレイ アタックを受けやすくなります。さらに、大容量のステートフル フェールオーバー トラフィックがインターフェイスに送信される可能性があり、そのネットワーク セグメントでパフォーマンスが低下する恐れがあります。

（注）　ステートフル フェールオーバー インターフェイスとしてデータ インターフェイスを使用することは、シングル コンテキスのルーテッド モードのみでサポートされています。

マルチ コンテキスト モードでは、ステートフル フェールオーバー リンクはシステム コンテキスト内にあります。このインターフェイスとフェールオーバー インターフェイスが、システム コンテキスト内にある唯一のインターフェイスです。他のインターフェイスは、すべてセキュリティ コンテキストに割り当てられ、セキュリティ コンテキスト内から設定されます。

マルチ コンテキスト モードでは、ステートフル フェールオーバー インターフェイスはシステム コンテキスト内にあります。このインターフェイスとフェールオーバー インターフェイスが、システム コンテキスト内にある唯一のインターフェイスです。他のインターフェイスは、すべてセキュリティ コンテキストに割り当てられ、セキュリティ コンテキスト内から設定されます。

（注） ステートフル フェールオーバー リンクが通常のデータ インターフェイスで設定されている場合を除き、ステートフル フェールオーバー リンクの IP アドレスおよび MAC アドレスは、フェールオーバーで変更されません。

注意 フェールオーバー リンクおよびステートフル フェールオーバー リンク経由で送信される情報は、フェールオーバー キーを使用して通信をセキュリティで保護しない限り、すべてクリア テキストで送信されます。VPN トンネルの終端にセキュリティ アプライアンスを使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザ名、パスワード、および事前共有キーが含まれています。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになる恐れがあります。セキュリティ アプライアンスを使用して VPN トンネルを終端する場合は、フェールオーバー通信をフェールオーバー キーによってセキュリティで保護することをお勧めします。

例

次の例は、ステートフル フェールオーバー インターフェイスとして専用インターフェイスを指定する方法を示しています。次の例のインターフェイスには、既存のコンフィギュレーションはありません。

```
hostname(config)# failover link stateful_if e4
INFO: Non-failover interface config is cleared on Ethernet4 and its sub-interfaces
```

関連コマンド

コマンド	説明
failover interface ip	**failover** コマンドおよびステートフル フェールオーバー インターフェイスの IP アドレスを設定します。
failover lan interface	フェールオーバー通信に使用するインターフェイスを指定します。
mtu	インターフェイスの最大伝送ユニットを指定します。

failover mac address

物理インターフェイスのためのフェールオーバー仮想 MAC 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 **failover mac address** コマンドを使用します。仮想 MAC 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。

failover mac address *phy_if active_mac standby_mac*

no failover mac address *phy_if active_mac standby_mac*

シンタックスの説明

phy_if	MAC アドレスを設定するインターフェイスの物理名。
active_mac	アクティブなセキュリティ アプライアンスの、指定されたインターフェイスに割り当てられた MAC アドレス。MAC アドレスは、h.h.h 形式で入力する必要があります。h は、16 ビットの 16 進数値です。
standby_mac	スタンバイ セキュリティ アプライアンスの指定されたインターフェイスに割り当てられた MAC アドレス。MAC アドレスは、h.h.h 形式で入力する必要があります。h は、16 ビットの 16 進数値です。

デフォルト

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
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

failover mac address コマンドは、Active/Standby フェールオーバー ペア用の仮想 MAC アドレスを設定します。仮想 MAC アドレスが定義されていない場合、各フェールオーバー装置はブート時にインターフェイスとしてバーンドイン MAC アドレスを使用し、それらのアドレスをフェールオーバー ピアと交換します。プライマリ装置上のインターフェイスの MAC アドレスは、アクティブな装置のインターフェイスに使用されます。

ただし、両方の装置が同時にオンラインにならず、セカンダリ装置が最初にブートしてアクティブになった場合は、独自のインターフェイスとしてバーンドイン MAC アドレスを使用します。プライマリ装置がオンラインになると、セカンダリ装置はプライマリ装置から MAC アドレスを取得します。この変更はネットワーク トラフィックを妨げる可能性があります。インターフェイスに仮想 MAC アドレスを設定すると、セカンダリ装置がプライマリ装置の前にオンラインになる場合でも、セカンダリ装置がアクティブな装置であるときに正しい MAC アドレスが使用されます。

LAN ベースのフェールオーバー用に設定されているインターフェイスには、**failover mac address** コマンドは、必要ありません（したがって、このコマンドは使用できません）。**failover lan interface** コマンドは、フェールオーバーが発生したときに IP アドレスおよび MAC アドレスのどちらも変更しないためです。セキュリティ アプライアンスが Active/Active フェールオーバーに対して設定され

ている場合、このコマンドは無効です。

failover mac address コマンドをコンフィギュレーションに追加する場合は、仮想 MAC アドレスを設定し、そのコンフィギュレーションをフラッシュ メモリに保存し、次にフェールオーバー ペアをリロードすることが最も良い方法です。アクティブ接続があるときに仮想 MAC アドレスが追加されると、そのアクティブ接続は停止します。また、**failover mac address** コマンドを含む完全なコンフィギュレーションをセカンダリ セキュリティ アプライアンスのフラッシュ メモリに書き込んで、仮想 MAC アドレッシングを有効にする必要があります。

failover mac address がプライマリ装置のコンフィギュレーションで指定された場合、それをセカンダリ装置のブートストラップ コンフィギュレーションでも指定する必要があります。

（注） このコマンドが適用されるのは、Active/Standby フェールオーバーのみです。Active/Active フェールオーバーでは、フェールオーバー グループ コンフィギュレーション モードの **mac address** コマンドを使用して、フェールオーバー グループのインターフェイスごとに仮想 MAC アドレスを設定します。

例

次の例では、intf2 という名前のインターフェイスに対してアクティブおよびスタンバイ MAC アドレスを設定します。

```
hostname(config)# failover mac address Ethernet0/2 00a0.c969.87c8 00a0.c918.95d8
```

関連コマンド

コマンド	説明
show interface	インターフェイス ステータス、設定、および統計情報を表示します。

failover polltime

フェールオーバー装置とインターフェイス ポーリング回数および装置の保持時間を指定するには、グローバル コンフィギュレーション モードで **failover polltime** コマンドを使用します。デフォルトのポーリング回数に戻すには、このコマンドの **no** 形式を使用します。

failover polltime [***unit***] [***msec***] *time* [***holdtime*** *time*]

failover polltime ***interface*** *time*

no failover polltime [***unit***] [***msec***] *time* [***holdtime*** *time*]

no failover polltime interface *time*

シンタックスの説明

holdtime *time*	（オプション）ピア装置の障害発生が宣言された後に、フェールオーバー リンクで装置が HELLO メッセージを受信する必要のある期間を設定します。有効となる値の範囲は、3 ～ 45 秒です。
interface *time*	インターフェイス モニタリングのポーリング時間を指定します。有効となる値の範囲は、3 ～ 15 秒です。
msec	（オプション）メッセージ間の間隔をミリ秒単位で指定します。最小値は 500 ミリ秒です。
time	hello メッセージの間隔。最大値は 15 秒です。
unit	（オプション）フェールオーバー リンクで HELLO メッセージを送信する回数を設定します。

デフォルト

デフォルトは次のとおりです。

- **unit** hold *time* は 15 秒です。
- セキュリティ アプライアンスでの ***unit*** poll *time* は 1 秒です。
- **interface** poll *time* は、15 秒です。
- **holdtime** *time* は 45 秒（ポーリング時間の 3 倍）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	このコマンドは、**failover poll** から **failover polltime** コマンドに変更され、***unit***、***interface***、および ***holdtime*** のキーワードを含むようになりました。

使用上のガイドライン

装置のポーリング時間の 3 倍未満の ***holdtime*** 値は入力できません。ポーリング時間が短いほど、セキュリティ アプライアンスは、それだけ速く障害を検出して、フェールオーバーを起動できます。ただし、検出が速すぎると、ネットワークが一時的に輻輳したときに不要な切り替えが発生する可能性があります。

unit または ***interface*** キーワードが指定されていない場合は、装置のポーリング時間が設定されます。

failover polltime unit および **failover polltime interface** コマンドの両方をコンフィギュレーションに含めることができます。

（注） **failover polltime interface** コマンドが適用されるのは、Active/Standby フェールオーバーのみです。Active/Active フェールオーバーの場合、フェールオーバー グループ コンフィギュレーション モードの **polltime interface** コマンドを、**failover polltime interface** コマンドの代わりに使用します。

保持時間内に hello パケットがフェールオーバー通信インターフェイスまたはケーブルで受信されない場合、スタンバイ装置がアクティブに切り替わり、ピアに障害が発生したとみなされます。インターフェイスの hello パケットが 5 回連続で検出されなかった場合は、インターフェイスのテストが発生します。

（注） CTIQBE トラフィックがフェールオーバー コンフィギュレーションのセキュリティ アプライアンスを通過するときは、セキュリティ アプライアンスのフェールオーバー保持時間を 30 秒より低く設定する必要があります。CTIQBE キープアライブ タイムアウトは 30 秒で、フェールオーバーの状況ではフェールオーバーが発生する前にタイムアウトする可能性があります。CTIQBE がタイムアウトした場合、Cisco Call Manager への Cisco IP SoftPhone の接続はドロップされ、IP SoftPhone クライアントは Call Manager を使用して再登録する必要があります。

例

次の例では、装置のポーリング間隔を 3 秒に設定します。

```
hostname(config)# failover polltime 3
```

関連コマンド

コマンド	説明
polltime interface	Active/Active フェールオーバー コンフィギュレーションのインターフェイス ポーリング時間を指定します。
show failover	フェールオーバー コンフィギュレーションの情報を表示します。

failover reload-standby

スタンバイ装置を強制的にリブートするには、特権 EXEC モードで **failover reload-standby** コマンドを使用します。

failover reload-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

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	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、フェールオーバー装置が同期しない場合に使用します。スタンバイ装置は、ブーティングが終了した後で、再起動してアクティブ装置に再度同期します。

例

次の例は、スタンバイ装置を強制的にリブートするために、アクティブ装置で **failover reload-standby** コマンドを使用する方法を示しています。

```
hostname# failover reload-standby
```

関連コマンド

コマンド	説明
write standby	実行コンフィギュレーションを、スタンバイ装置のメモリに書き込みます。

failover replication http

HTTP（ポート 80）接続の複製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 **failover replication http** コマンドを使用します。HTTP 接続の複製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。

failover replication http

no failover replication http

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

ディセーブル

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド 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	このコマンドが、**failover replicate http** から **failover replication http** 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、ステートフル フェールオーバーがイネーブルにされた場合、セキュリティ アプライアンスは HTTP セッション情報を複製しません。HTTP セッションは通常は存続期間が短く、HTTP クライアントは接続試行が失敗すると通常は再試行するため、HTTP セッションの複製をしないことでシステムのパフォーマンスが向上します。複製をしなくても重要なデータや接続は失われません。**failover replication http** コマンドは、ステートフル フェールオーバーの環境で HTTP セッションのステートフル複製をイネーブルにしますが、システムのパフォーマンスに悪影響を及ぼす可能性があります。

Active/Active フェールオーバー コンフィギュレーションでは、フェールオーバー グループ コンフィギュレーション モードの **replication http** コマンドを使用して、各フェールオーバー グループの HTTP セッションの複製を設定します。

例

次の例は、HTTP 接続の複製をイネーブルにする方法を示しています。

```
hostname(config)# failover replication http
```

関連コマンド

コマンド	説明
replication http	特定のフェールオーバー グループでの HTTP セッションの複製をイネーブルにします。
show running-config failover	実行コンフィギュレーション内の **failover** コマンドを表示します。

failover reset

障害が発生したセキュリティ アプライアンスを障害が発生する前の状態に戻すには、特権 EXEC モードで **failover reset** コマンドを使用します。

failover reset [***group*** *group_id*]

シンタックスの説明

group	（オプション）フェールオーバー グループを指定します。
group_id	フェールオーバー グループの番号。

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	このコマンドは、オプションのフェールオーバー グループ ID を許可するように修正されました。

使用上のガイドライン

failover reset コマンドにより、障害が発生した装置またはグループを障害が発生する前の状態に変更できます。**failover reset** コマンドは、どちらの装置からでも入力できますが、常にアクティブな装置でコマンドを入力することをお勧めします。アクティブな装置で **failover reset** コマンドを入力すると、スタンバイ装置を「unfail」にします。

装置のフェールオーバー ステータスは、**show failover** または **show failover state** コマンドで表示できます。

このコマンドの **no** バージョンはありません。

Active/Active フェールオーバーで **failover reset** を入力すると、装置全体がリセットされます。コマンドでフェールオーバー グループを指定すると、指定されたグループだけがリセットされます。

例

次の例は、障害が発生した装置を、障害が発生する前の状態に変更する方法を示しています。

```
hostname# failover reset
```

関連コマンド

コマンド	説明
failover interface-policy	モニタリングがインターフェイス障害を検出するときのフェールオーバー ポリシーを指定します。
show failover	装置のフェールオーバー ステータスに関する情報を表示します。

failover timeout

非対称ルーテッド セッションのフェールオーバーの再接続タイムアウト値を指定するには、グローバル コンフィギュレーション モードで **failover timeout** コマンドを使用します。デフォルトのタイムアウト値に戻すには、このコマンドの **no** 形式を使用します。

failover timeout *hh*[**:***mm*:[**:***ss*]

no failover timeout [*hh*[**:***mm*:[**:***ss*]]

シンタックスの説明

hh	タイムアウト値を時間単位で指定します。有効となる値の範囲は、-1 ～ 1,193 です。デフォルトでは、この値は 0 に設定されています。 この値を -1 に設定すると、タイムアウトがディセーブルにされ、任意の時間が経過した後でも接続を再開できます。 他のタイムアウト値を指定しないでこの値を 0 に設定すると、コマンドはデフォルト値に戻り、接続の再開はできません。**no failover timeout** コマンドも、この値をデフォルト（0）に設定します。 **（注）** デフォルト値に設定されている場合、このコマンドは実行コンフィギュレーション内に表示されません。
mm	（オプション）タイムアウト値を分単位で指定します。有効となる値の範囲は、0 ～ 59 です。デフォルトでは、この値は 0 に設定されています。
ss	（オプション）タイムアウト値を秒単位で指定します。有効となる値の範囲は、0 ～ 59 です。デフォルトでは、この値は 0 に設定されています。

デフォルト

デフォルトでは、*hh*、*mm*、および *ss* は 0 です。この設定では、接続が再接続されることはありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0	このコマンドは、コマンド リストに表示されるように修正されました。

使用上のガイドライン

このコマンドは、***nailed*** オプションを使用した **static** コマンドと友に使用します。***nailed*** オプションを使用すると、ブートアップ後またはシステムがアクティブになった後に、指定された時間内で接続を再確立できます。**failover timeout** コマンドは、その時間を指定します。設定しない場合は、接続を再確立できません。**failover timeout** コマンドは、**asr-group** コマンドに影響しません。

（注）　***nailed*** オプションを **static** コマンドに追加すると、その接続について、TCP のステート トラッキングおよびシーケンス チェッキングがスキップされます。

このコマンドの ***no*** 形式を入力すると、デフォルト値に戻ります。**failover timeout 0** を入力しても、デフォルト値に戻ります。デフォルト値に設定されている場合、このコマンドは実行コンフィギュレーション内に表示されません。

例

次の例では、スタンバイ グループ 1 をアクティブにしています。

```
hostname(config)# failover timeout 12:30
hostname(config)# show running-config failover
no failover
failover timeout 12:30:00
```

関連コマンド

コマンド	説明
static	ローカル IP アドレスをグローバル IP アドレスにマッピングすることによって、固定の 1 対 1 のアドレス変換規則を設定します。

filter

このグループポリシーまたはユーザ名の WebVPN 接続に使用するアクセスリストの名前を指定するには、webvpn モードで **filter** コマンドを使用します。**filter none** コマンドを発行して作成されたヌル値を含むアクセスリストを削除するには、このコマンドの **no** 形式を使用します。**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。フィルタ値を継承しないようにするには、**filter value none** コマンドを使用します。

ACL を設定して、このユーザまたはグループポリシーについて、さまざまなタイプのトラフィックを許可または拒否します。次に、**filter** コマンドを使用して、これらの ACL を WebVPN トラフィックに適用します。

filter {**value** *ACLname* | **none**}

no filter

シンタックスの説明

none	**webvpntype** アクセスリストがないことを示します。ヌル値を設定して、アクセスリストを拒否します。アクセスリストを他のグループポリシーから継承しないようにします。
value *ACLname*	設定済みアクセスリストの名前を指定します。

デフォルト

WebVPN アクセスリストは、**filter** コマンドを使用して指定するまで適用されません。

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
WebVPN モード	•	•	—	—	•

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

使用上のガイドライン

WebVPN は、**vpn-filter** コマンドで定義された ACL を使用しません。

例

次の例は、FirstGroup という名前のグループポリシーの *acl_in* という名前のアクセスリストを呼び出すフィルタ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)# filter acl_in
```

関連コマンド

コマンド	説明
access-list	アクセスリストを作成します。または、ダウンロード可能なアクセスリストを使用します。
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。
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。

filter activex

セキュリティ アプライアンスを通過する HTTP トラフィック の ActiveX オブジェクトを削除するには、グローバル コンフィギュレーション モードで **filter activex** 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。

filter activex {[*port*[**-***port*] | **except** } *local_ip local_mask foreign_ip foreign_mask*]

no filter activex {[*port*[**-***port*] | **except** } *local_ip local_mask foreign_ip foreign_mask*]

シンタックスの説明

port	フィルタリングの適用対象となる TCP ポート。一般的に、これはポート 21 ですが、他の値でも受け入れられます。**http** または **url** リテラルをポート 21 に使用できます。許可される値の範囲は 0 ～ 65535 です。
*port***-***port*	（オプション）ポートの範囲を指定します。
except	先行の **filter** 条件に対する例外を作成します。
local_ip	セキュリティ レベルが最も高い、アクセスが要求されているインターフェイスの IP アドレス。このアドレスに **0.0.0.0**（短縮形は **0**）を設定して、すべてのホストを指定できます。
local_mask	*local_ip* のネットワーク マスク。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
foreign_ip	セキュリティ レベルが最も低い、アクセスが要求されているインターフェイスの IP アドレス。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
foreign_mask	*foreign_ip* のネットワーク マスク。常に特定のマスク値を指定します。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。

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
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

ActiveX オブジェクトは、保護されたネットワーク上のホストやサーバを攻撃することを目的としたコードを含んでいる場合があるため、セキュリティ リスクになる恐れがあります。**filter activex** コマンドを使用して、ActiveX オブジェクトをディセーブルにできます。

ActiveX コントロールは、以前は OLE コントロールまたは OCX コントロールと呼ばれており、web ページまたは他のアプリケーションに挿入できるコンポーネントです。これらのコントロールには、情報の収集や表示に使用するためのカスタム フォームや、カレンダ、多数のサードパーティ フォームがあります。技術としては、ActiveX には、ネットワーク クライアントに対して起こる可能性のある問題、たとえば、ワークステーション障害の発生、ネットワーク セキュリティ問題の導入、またはサーバへの攻撃というような問題が数多く生じています。

filter activex コマンドは、HTML Web ページ内でコメント アウトすることにより HTML <object> コマンドをブロックします。HTML ファイルの ActiveX フィルタリングは、<APPLET> と </APPLET> および <OBJECT CLASSID> と </OBJECT> タグをコメントで選択的に置き換えることにより実行されます。入れ子タグのフィルタリングは、トップ レベルのタグをコメントに変換することでサポートされています。

注意　<object> タグは、Java アプレット、イメージ ファイル、およびマルチメディア オブジェクトでも使用されますが、これらは、このコマンドによってもブロックされます。

<object> タグまたは </object> HTML タグがネットワーク パケット間で分割されている場合、またはタグ内のコードが MTU 内のバイト数よりも長い場合、セキュリティ アプライアンスはタグをブロックできません。

ActiveX blocking does not occur when users access an IP address referenced by the ***alias*** command.

例

次の例では、すべての発信接続で Activex オブジェクトがブロックされるように指定します。

```
hostname(config)# filter activex 80 0 0 0 0
```

このコマンドは、ポート 80 上において、あらゆるローカル ホストから来て、あらゆる外部ホスト接続へ向かう Web トラフィックに ActiveX オブジェクトのブロッキングが適用されることを指定します。

関連コマンド

コマンド	説明
filter url	トラフィックを URL フィルタリング サーバに誘導します。
filter java	セキュリティ アプライアンスを通過する HTTP トラフィックから Java アプレットを削除します。
show running-config filter	フィルタリング コンフィギュレーションを表示します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

filter ftp

Websense サーバによりフィルタされる FTP トラフィックを指定するには、グローバル コンフィギュレーション モードで **filter ftp** 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。

filter ftp {[*port*[**-***port*] | **except** } *local_ip local_mask foreign_ip foreign_mask*] [**allow**] [**interact-block**]

no filter ftp {[*port*[**-***port*] | **except** } *local_ip local_mask foreign_ip foreign_mask*] [**allow**] [**interact-block**]

シンタックスの説明

port	フィルタリングの適用対象となる TCP ポート。一般的に、これはポート 21 ですが、他の値でも受け入れられます。ポート 80 の代わりに、**ftp** リテラルを使用できます。
*port***-***port*	（オプション）ポートの範囲を指定します。
except	先行の **filter** 条件に対する例外を作成します。
local_ip	セキュリティ レベルが最も高い、アクセスが要求されているインターフェイスの IP アドレス。このアドレスに **0.0.0.0**（短縮形は **0**）を設定して、すべてのホストを指定できます。
local_mask	*local_ip* のネットワーク マスク。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
foreign_ip	セキュリティ レベルが最も低い、アクセスが要求されているインターフェイスの IP アドレス。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
foreign_mask	*foreign_ip* のネットワーク マスク。常に特定のマスク値を指定します。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
allow	（オプション）サーバが利用できなければ、発信接続はフィルタリングなしでセキュリティ アプライアンスを通過します。このオプションを省略した場合、および N2H2 または Websense サーバがオフラインの場合、セキュリティ アプライアンスは発信ポート 80（Web）トラフィックを、N2H2 または Websense サーバがオンラインに戻るまで、停止します。
interact-block	（オプション）ユーザが対話型の FTP プログラムを使用して FTP サーバに接続しないようにします。

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
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

filter ftp コマンドは、Websense サーバによってフィルタされる FTP トラフィックを指定します。FTP フィルタリングは、N2H2 サーバではサポートされていません。

この機能をイネーブルにした後で、ユーザが FTP GET 要求をサーバに発行すると、セキュリティ アプライアンスは FTP サーバと Websense サーバに同時に要求を送信します。Websense サーバが接続を許可する場合、セキュリティ アプライアンスは正常な FTP の戻りコードが変更されずにユーザに到達することを許可します。たとえば、正常な戻りコードは「250: CWD command successful」です。

Websense サーバが接続を拒否する場合、セキュリティ アプライアンスは、FTP の戻りコードを接続が拒否されたことを表示するように変更します。たとえば、セキュリティ アプライアンスはコード 250 を「550 Requested file is prohibited by URL filtering policy」に変更します（Websense は FTP GET コマンドだけをフィルタし、PUT コマンドはフィルタしません）。

interactive-block オプションを使用して、ディレクトリ パス全体を提供しない対話型 FTP セッションを防ぎます。対話型 FTP クライアントでは、ユーザはパス全体を入力せずにディレクトリを変更できます。たとえば、ユーザは **cd /public/files** の代わりに **cd ./files** を入力する可能性があります。これらのコマンドを使用する前に、URL フィルタリング サーバを指定してイネーブルにする必要があります。

例

次の例は、FTP フィルタリングをイネーブルにする方法を示しています。

```
hostname(config)# url-server (perimeter) host 10.0.1.1
hostname(config)# filter ftp 21 0 0 0 0
hostname(config)# filter ftp except 10.0.2.54 255.255.255.255 0 0
```

関連コマンド

コマンド	説明
filter https	Websense サーバによってフィルタリングされる HTTPS トラフィックを指定します。
filter java	セキュリティ アプライアンスを通過する HTTP トラフィックから Java アプレットを削除します。
filter url	トラフィックを URL フィルタリング サーバに誘導します。
show running-config filter	フィルタリング コンフィギュレーションを表示します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

filter https

Websense サーバによりフィルタされる HTTPS トラフィックを指定するには、グローバル コンフィギュレーション モードで **filter https** 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。

filter https {[*port*[**-***port*] | **except** } *local_ip local_mask foreign_ip foreign_mask*] [**allow**]

no filter https {[*port*[**-***port*] | **except** } *local_ip local_mask foreign_ip foreign_mask*] [**allow**]

シンタックスの説明

port	フィルタリングの適用対象となる TCP ポート。一般的に、これはポート 443 ですが、他の値でも受け入れられます。ポート 443 の代わりに、**https** リテラルを使用できます。
port-port	（オプション）ポートの範囲を指定します。
except	（オプション）先行の **filter** 条件に対する例外を作成します。
dest-port	宛先ポート番号。
local_ip	セキュリティ レベルが最も高い、アクセスが要求されているインターフェイスの IP アドレス。このアドレスに **0.0.0.0**（短縮形は **0**）を設定して、すべてのホストを指定できます。
local_mask	*local_ip* のネットワーク マスク。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
foreign_ip	セキュリティ レベルが最も低い、アクセスが要求されているインターフェイスの IP アドレス。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
foreign_mask	*foreign_ip* のネットワーク マスク。常に特定のマスク値を指定します。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
allow	（オプション）サーバが利用できなければ、発信接続はフィルタリングなしでセキュリティ アプライアンスを通過します。このオプションを省略した場合、および N2H2 または Websense サーバがオフラインの場合、セキュリティ アプライアンスは発信ポート 443 トラフィックを、N2H2 または Websense サーバがオンラインに戻るまで、停止します。

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
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　セキュリティ アプライアンスは、外部 Websense フィルタリング サーバを使用して、HTTPS および FTP サイトのフィルタリングをサポートします。

（注）　HTTPS は、N2H2 フィルタリング サーバではサポートされていません。

HTTPS フィルタリングは、サイトが許可されない場合に SSL 接続ネゴシエーションの完了を防ぐことにより動作します。ブラウザには、「The Page or the content cannot be displayed」などのエラーメッセージが表示されます。

HTTPS のコンテンツは暗号化されているため、セキュリティ アプライアンスはディレクトリおよびファイル名の情報なしで URL ルックアップを送信します。

例　次の例では、10.0.2.54 ホストからの接続を除く、すべての発信 HTTPS 接続をフィルタリングします。

```
hostname(config)# url-server (perimeter) host 10.0.1.1
hostname(config)# filter https 443 0 0 0 0
hostname(config)# filter https except 10.0.2.54 255.255.255.255 0 0
```

関連コマンド

コマンド	説明
filter activex	セキュリティ アプライアンスを通過する HTTP トラフィックから ActiveX オブジェクトを削除します。
filter java	セキュリティ アプライアンスを通過する HTTP トラフィックから Java アプレットを削除します。
filter url	トラフィックを URL フィルタリング サーバに誘導します。
show running-config filter	フィルタリング コンフィギュレーションを表示します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

filter java

セキュリティ アプライアンスを通過する HTTP トラフィックから Java アプレットを削除するには、グローバル コンフィギュレーション モードで **filter java** 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。

filter java {[*port*[**-***port*] | **except** } *local_ip local_mask foreign_ip foreign_mask*]

no filter java {[*port*[**-***port*] | **except** } *local_ip local_mask foreign_ip foreign_mask*]

シンタックスの説明

port	フィルタリングの適用対象となる TCP ポート。一般的に、これはポート 80 ですが、他の値でも受け入れられます。ポート 80 の代わりに、**http** または **url** リテラルを使用できます。
*port***-***port*	（オプション）ポートの範囲を指定します。
except	（オプション）先行の **filter** 条件に対する例外を作成します。
local_ip	セキュリティ レベルが最も高い、アクセスが要求されているインターフェイスの IP アドレス。このアドレスに **0.0.0.0**（短縮形は **0**）を設定して、すべてのホストを指定できます。
local_mask	*local_ip* のネットワーク マスク。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
foreign_ip	セキュリティ レベルが最も低い、アクセスが要求されているインターフェイスの IP アドレス。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
foreign_mask	*foreign_ip* のネットワーク マスク。常に特定のマスク値を指定します。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。

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
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

Java アプレットは、保護されたネットワーク上のホストやサーバを攻撃することを目的としたコードを含んでいる場合があるため、セキュリティ リスクになる恐れがあります。**filter java** コマンドを使用して、Java アプレットを削除できます。

filter java コマンドは、発信接続からセキュリティ アプライアンスに返る Java アプレットをフィルタリングします。ユーザは、引き続き HTML ページを受信できますが、アプレットに対する Web ページのソースがコメント アウトされるため、アプレットは実行できません。

applet または /applet HTML タグがネットワーク パケット間で分割されている場合、またはタグ内のコードが MTU 内のバイト数よりも長い場合、セキュリティ アプライアンスはタグをブロックできません。Java アプレットは、<object> タグに含まれていることが分かっていれば、**filter activex** コマンドを使用して削除します。

例

次の例では、すべての発信接続で Java アプレットがブロックされるように指定します。

```
hostname(config)# filter java 80 0 0 0 0
```

このコマンドは、ポート 80 上において、あらゆるローカル ホストから来て、あらゆる外部ホスト接続へ向かう Web トラフィックに Java ブロッキングが適用されることを指定します。

次の例では、保護されたネットワーク上のホストに Java アプレットをダウンロードすることをブロックします。

```
hostname(config)# filter java http 192.168.3.3 255.255.255.255 0 0
```

このコマンドは、ホスト 192.168.3.3 が Java アプレットをダウンロードしないようにします。

関連コマンド

コマンド	説明
filter activex	セキュリティ アプライアンスを通過する HTTP トラフィックから ActiveX オブジェクトを削除します。
filter url	トラフィックを URL フィルタリング サーバに誘導します。
show running-config filter	フィルタリング コンフィギュレーションを表示します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

filter url

URL フィルタリング サーバにトラフィックを転送するには、グローバル コンフィギュレーション モードで **filter url** 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。

filter url {[*port*[*-port*] | **except** } *local_ip local_mask foreign_ip foreign_mask*] [**allow**] [**cgi-truncate**] [**longurl-truncate** | **longurl-deny**] [**proxy-block**]

no filter url {[*port*[*-port*] | **except** } *local_ip local_mask foreign_ip foreign_mask*] [**allow**] [**cgi-truncate**] [**longurl-truncate** | **longurl-deny**] [**proxy-block**]

シンタックスの説明

allow	サーバが利用できなければ、発信接続はフィルタリングなしでセキュリティ アプライアンスを通過します。このオプションを省略した場合、および N2H2 または Websense サーバがオフラインの場合、セキュリティ アプライアンスは発信ポート 80（Web）トラフィックを、N2H2 または Websense サーバがオンラインに戻るまで、停止します。
cgi_truncate	URL のパラメータ リストに CGI スクリプトなどの疑問符（?）から始まるリストがある場合は、疑問符を含む疑問符以降のすべての文字を削除することにより、フィルタリング サーバに送信された URL を切り捨てます。
except	先行の **filter** 条件に対する例外を作成します。
foreign_ip	セキュリティ レベルが最も低い、アクセスが要求されているインターフェイスの IP アドレス。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
foreign_mask	*foreign_ip* のネットワーク マスク。常に特定のマスク値を指定します。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
http	ポート 80 を指定します（ポート 80 を示す 80 の代わりに **http** または **www** を入力できます）。
local_ip	セキュリティ レベルが最も高い、アクセスが要求されているインターフェイスの IP アドレス。このアドレスに **0.0.0.0**（短縮形は **0**）を設定して、すべてのホストを指定できます。
local_mask	*local_ip* のネットワーク マスク。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
longurl-deny	URL が URL バッファ サイズの制限を超えている場合、または URL バッファが利用できない場合に、URL 要求を拒否します。
longurl-truncate	URL が URL バッファの制限を超えている場合、発信ホスト名または発信 IP アドレスだけを Websense サーバに送信します。
mask	任意のマスク。
[*port*[*-port*]	（オプション）フィルタリングの適用対象となる TCP ポート。一般的に、これはポート 80 ですが、他の値でも受け入れられます。ポート 80 の代わりに、**http** または **url** リテラルを使用できます。ハイフンの後に 2 番目のポートを追加すると、オプションでポートの範囲を指定します。
proxy-block	ユーザが HTTP プロキシ サーバに接続できないようにします。
url	セキュリティ アプライアンスを通過するデータから URL をフィルタします。

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。

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　**filter url** コマンドによって、発信ユーザが N2H2 または Websense フィルタリング アプリケーションを使用して、指示した World Wide Web URL にアクセスしないようにします。

（注）　**filter url** コマンドを実行するには、事前に **url-server** コマンドを設定する必要があります。

filter url コマンドの **allow** オプションは、N2H2 または Websense サーバがオフラインになった場合のセキュリティ アプライアンスの動作を決定します。**filter url** コマンドで **allow** オプションを使用している場合、N2H2 または Websense サーバがオフラインになると、ポート 80 トラフィックはフィルタリングなしでセキュリティ アプライアンスを通過します。**allow** オプションなしの場合、サーバがオフラインになると、セキュリティ アプライアンスはサーバがオンラインに戻るまで発信ポート 80（Web）のトラフィックを停止するか、または他の URL サーバが利用できる場合は、次の URL サーバに制御を渡します。

（注）　**allow** オプションが設定されている場合、N2H2 または Websense サーバがオフラインになると、セキュリティ アプライアンスは制御を代替サーバに渡します。

N2H2 サーバまたは Websense サーバは、セキュリティ アプライアンスと共に動作して、企業のセキュリティ ポリシーに基づいて、ユーザが Web サイトにアクセスすることを拒否します。

Websense フィルタリング サーバの使用

Websense プロトコル Version 4 は、グループとユーザ名の認証を、ホストとセキュリティ アプライアンスの間でイネーブルにします。セキュリティ アプライアンスがユーザ名のルックアップを実行し、次に、Websense サーバが URL フィルタリングとユーザ名ロギングを処理します。

N2H2 サーバは、IFP Server を実行している Windows ワークステーション（2000、NT、または XP）であり、推奨する最小メモリとして 512 MB RAM を搭載している必要があります。また、N2H2 サービス用の長い URL のサポートは、Websense の上限よりも少ない 3 KB に制限されます。

Websense プロトコルの Version 4 には、次の機能拡張があります。

- URL フィルタリングを使用すると、セキュリティ アプライアンスは、発信 URL 要求を Websense サーバ上に定義されているポリシーと照合してチェックします。
- ユーザ名ロギングは、Websense サーバ上のユーザ名、グループ、およびドメイン名を追跡します。

- ユーザ名ルックアップを使用すると、セキュリティ アプライアンスがユーザ認証テーブルを使用して、ホストの IP アドレスをユーザ名にマッピングできます。

Websense に関する情報は、次の Web サイトで利用できます。

http://www.websense.com/

設定手順

次の手順を実行して、URL フィルタリングを行います。

ステップ 1　N2H2 サーバまたは Websense サーバに **url-server** コマンドの適切なベンダー固有のフォームを指示します。

ステップ 2　**filter** コマンドでフィルタリングをイネーブルにします。

ステップ 3　必要であれば、**url-cache** コマンドを使用して、スループットを改善します。ただし、このコマンドは Websense ログをアップデートしないため、Websense アカウンティング レポートに影響を与える可能性があります。**url-cache** コマンドを使用する前に Websense 実行ログを累積します。

ステップ 4　**show url-cache statistics** コマンドおよび **show perfmon** コマンドを使用して、実行情報を表示します。

長い URL の扱い

Websense フィルタリング サーバでは最大 4 KB の URL、N2H2 フィルタリング サーバでは最大 1159 バイトの URL がサポートされています。

最大の許可サイズよりも長い URL 要求を処理できるようにするには、***longurl-truncate*** および ***cgi-truncate*** オプションを使用します。

最大サイズよりも URL が長い場合、**longurl-truncate** または **longurl-deny** オプションがイネーブルになっていないと、パケットはセキュリティ アプライアンスによりドロップされます。

longurl-truncate オプションを使用すると、許可された最大長よりも URL が長い場合、セキュリティ アプライアンスは URL のホスト名または IP アドレスの部分だけを評価のために送信します。許可された最大長よりも URL が長い場合に発信 URL トラフィックを拒否するには、**longurl-deny** オプションを使用します。

パラメータなしで CGI スクリプトの場所とスクリプト名だけが含まれるように CGI URL を切り捨てるには、**cgi-truncate** オプションを使用します。長い HTTP 要求の多くは CGI 要求です。パラメータ リストが非常に長い場合、パラメータ リストを含む完全な CGI 要求を待機および送信すると、メモリ リソースが浪費されてセキュリティ アプライアンスのパフォーマンスに影響します。

HTTP 応答のバッファリング

デフォルトでは、ユーザが特定の Web サイトに接続する要求を発行すると、セキュリティ アプライアンスは Web サーバとフィルタリング サーバに同時に要求を送信します。フィルタリング サーバが Web コンテンツ サーバの前に応答しない場合、Web サーバからの応答はドロップされます。これが原因で、Web クライアントからは Web サーバの応答が遅れているように見えます。

HTTP 応答バッファをイネーブルにすることにより、Web コンテンツ サーバからの応答はバッファされ、フィルタリング サーバが接続を許可すると、応答は要求したユーザに転送されます。これにより、発生する可能性のある遅延を防ぎます。

HTTP の応答バッファをイネーブルにするには、次のコマンドを入力します。

```
url-block block block-buffer-limit
```

block-buffer-limit をバッファされるブロックの最大数で置き換えます。許可される値は、0 ～ 128 で、一度にバッファされることが可能な 1,550 バイトのブロック数を指定します。

例

次の例では、10.0.2.54 ホストからの接続を除く、すべての発信 HTTP 接続をフィルタリングします。

```
hostname(config)# url-server (perimeter) host 10.0.1.1
hostname(config)# filter url 80 0 0 0 0
hostname(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

次の例では、ポート 8080 上でリスンするプロキシ サーバに向かう発信 HTTP 接続をすべてブロックします。

```
hostname(config)# filter url 8080 0 0 0 0 proxy-block
```

関連コマンド

コマンド	説明
filter activex	セキュリティ アプライアンスを通過する HTTP トラフィックから ActiveX オブジェクトを削除します。
filter java	セキュリティ アプライアンスを通過する HTTP トラフィックから Java アプレットを削除します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間に Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

fips enable

システムまたはモジュールに対して FIPS 準拠を強制するためのポリシーチェックをイネーブルまたはディセーブルにするには、**fips enable** コマンドまたは **[no] fips enable** コマンドを使用します。

fips enable

[no] fips enable

シンタックスの説明

enable	FIPS 準拠を強制するためのポリシーチェックをイネーブルまたはディセーブルします。

デフォルト

このコマンドにデフォルト設定はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0(4)	このコマンドが導入されました。

使用上のガイドライン

FIPS 準拠の動作モードで実行するには、**fips enable** コマンドと、セキュリティ ポリシーで指定された正しい設定の両方を適用する必要があります。内部 API は、実行時に正しい設定を強制するためにデバイスが移行することを許可します。

「fips enable」がスタートアップ コンフィギュレーションにある場合、FIPS POST が実行されて、次のコンソール メッセージが表示されます。

```
Copyright (c) 1996-2005 by Cisco Systems, Inc.
Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set
forth in subparagraph (c) of the Commercial Computer Software - Restricted Rights
clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical
Data and Computer Software clause at DFARS sec. 252.227-7013.

               Cisco Systems, Inc.
               170 West Tasman Drive
               San Jose, California 95134-1706

....
Cryptochecksum (unchanged): 6c6d2f77 ef13898e 682c9f94 9c2d5ba9

INFO: FIPS Power-On Self-Test in process.  Estimated completion in 90 seconds.
.................................................
INFO: FIPS Power-On Self-Test complete.
Type help or '?' for a list of available commands.
sw8-5520>
```

例

```
sw8-ASA(config)# fips enable
```

関連コマンド

コマンド	説明
clear configure fips	NVRAM に格納されている、システムまたはモジュールの FIPS コンフィギュレーション情報を消去します。
crashinfo console disable	フラッシュに対するクラッシュ書き込み情報の読み取り、書き込み、および設定をディセーブルにします。
fips self-test poweron	パワーオン セルフテストを実行します。
show crashinfo console	フラッシュに対するクラッシュ書き込みの読み取り、書き込み、および設定を行います。
show running-config fips	セキュリティ アプライアンス上で実行されている FIPS コンフィギュレーションを表示します。

fips self-test poweron

パワーオン セルフテストを実行するには、**fips self-test powereon** コマンドを使用します。

fips self-test poweron

シンタックスの説明

poweron	パワーオン セルフテストを実行します。

デフォルト

このコマンドにデフォルト設定はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

このコマンドを実行すると、デバイスは FIPS 140-2 準拠に要求されるすべてのセルフテストを実行します。テストは、暗号アルゴリズム テスト、ソフトウェア整合性テスト、および主要な機能テストで構成されています。

例

```
sw8-5520(config)# fips self-test poweron
```

関連コマンド

コマンド	説明
clear configure fips	NVRAM に格納されている、システムまたはモジュールの FIPS コンフィギュレーション情報を消去します。
crashinfo console disable	フラッシュに対するクラッシュ書き込み情報の読み取り、書き込み、および設定をディセーブルにします。
fips enable	システムまたはモジュールに対して FIPS 準拠を強制するためのポリシーチェックをイネーブルまたはディセーブルにします。
show crashinfo console	フラッシュに対するクラッシュ書き込みの読み取り、書き込み、および設定を行います。
show running-config fips	FWSM 上で実行されている FIPS コンフィギュレーションを表示します。

firewall transparent

ファイアウォール モードを透過モードに設定するには、グローバル コンフィギュレーション モードで **firewall transparent** コマンドを使用します。ルーテッド モードに戻すには、このコマンドの **no** 形式を使用します。透過的なファイアウォールは、「回線上の隆起物」または「秘密の防火壁」の機能を果たすレイヤ 2 のファイアウォールで、接続装置に対するルータ ホップとしては見られません。

firewall ***transparent***

no firewall ***transparent***

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	このコマンドが導入されました。

使用上のガイドライン

マルチ コンテキスト モードでは、すべてのコンテキストに対して 1 つのファイアウォール モードだけを使用できます。システム コンフィギュレーションでモードを設定する必要があります。このコマンドは、情報提供だけを目的として各コンテキスト コンフィギュレーションでも表示されますが、コンテキストにこのコマンドを入力することはできません。

コマンドの多くは両方のモードでサポートされていないため、モードを変更すると、セキュリティ アプライアンスによりコンフィギュレーションがクリアされます。データが入力されたコンフィギュレーションがある場合、モードを変更する前にコンフィギュレーションをバックアップしてください。新しいコンフィギュレーションを作成するときに、このバックアップを参照として使用できます。

firewall transparent コマンドを使用してモードを変更するように設定されているセキュリティ アプライアンスに、テキスト コンフィギュレーションをダウンロードする場合は、コンフィギュレーションの先頭にコマンドを置くようにしてください。セキュリティ アプライアンスはコマンドを読み込むとすぐにモードを変更し、ダウンロードしたコンフィギュレーションの読み込みを継続します。コマンドがコンフィギュレーションの後ろの方に置かれていると、コンフィギュレーションでコマンドより前に置かれているラインはセキュリティ アプライアンスによりすべてクリアされます。

例

次の例では、ファイアウォール モードを透過的なモードに変更します。

```
hostname(config)# firewall transparent
```

関連コマンド

コマンド	説明
arp-inspection	ARP 検査をイネーブルにして、ARP パケットをスタティック ARP エントリと比較します。
mac-address-table static	MAC アドレス テーブルにスタティック MAC アドレス エントリを追加します。
mac-learn	MAC アドレス ラーニングをディセーブルにします。
show firewall	ファイアウォール モードを示します。
show mac-address-table	ダイナミック エントリとスタティック エントリを含め、MAC アドレス テーブルを表示します。

format

すべてのファイルを消去してファイル システムをフォーマットするには、特権 EXEC モードで **format** コマンドを使用します。このコマンドは、非表示のシステム ファイルを含むファイル システム上のすべてのファイルを消去し、ファイル システムを再インストールします。

format {**disk0: | disk1: | flash:**}

シンタックスの説明

disk0:	内部フラッシュ メモリを指定し、続けてコロン（:）を入力します。
disk1:	外部フラッシュ メモリ カードを指定し、続けてコロン（:）を入力します。
flash:	内部フラッシュ メモリを指定し、続けてコロン（:）を入力します。ASA 5500 シリーズでは、***flash*** キーワードは ***disk0*** のエイリアスです。

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	このコマンドが導入されました。

使用上のガイドライン

format コマンドは、指定されたファイル システム上のすべてのデータを消去し、デバイスに FAT 情報を再度書き込みます。

注意

format コマンドは、破損したフラッシュ メモリをクリーン アップするのに必要な場合のみ、細心の注意を払って使用してください。

すべての可視ファイル（非表示のシステム ファイルを除く）を削除するには、***format*** コマンドではなく、***delete /recursive*** コマンドを使用します。

（注）　Cisco PIX セキュリティ アプライアンスでは、***erase*** コマンドと ***format*** コマンドは同じ処理を実行します。ユーザ データを 0xFF パターンを使用して破棄します。

破損したファイル システムを修復するには、**format** コマンドを入力する前に **fsck** コマンドを入力してみます。

（注）　Cisco ASA 5500 シリーズのセキュリティ アプライアンスでは、***erase*** コマンドを実行すると、ディスク上のすべてのユーザ データが 0xFF パターンを使用して破棄されます。一方、***format*** コマンドはファイル システムの制御構造をリセットするだけです。生ディスク読み取りツールを使用すると、この情報はまだ参照できる可能性があります。

破損したファイル システムを修復するには、**format** コマンドを入力する前に **fsck** コマンドを入力してみます。

例

この例は、フラッシュ メモリをフォーマットする方法を示しています。

```
hostname# format flash:
```

関連コマンド

コマンド	説明
delete	ユーザから見えるすべてのファイルを削除します。
erase	すべてのファイルを削除し、フラッシュ メモリをフォーマットします。
fsck	破損したファイル システムを修復します。

fqdn

登録中に、指定された FQDN を証明書のサブジェクト代替名の拡張に含めるには、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 **fqdn** コマンドを使用します。fqdn の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。

fqdn *fqdn*

no fqdn

シンタックスの説明

fqdn	完全修飾ドメイン名を指定します。*fqdn* の最大長は 64 文字です。

デフォルト

デフォルト設定では、FQDN 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	このコマンドが導入されました。

例

次の例では、トラストポイント central の暗号 CA トラストポイント コンフィギュレーション モードに入り、トラストポイント central の登録要求に FQDN エンジニアリングを含めます。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# fqdn engineering
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 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。
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。

fragment

特別なパケット フラグメント化の管理を提供して NFS との互換性を向上させるには、グローバル コンフィギュレーション モードで **fragment** コマンドを使用します。

fragment {**size** | **chain** | **timeout** *limit*} [*interface*]

no fragment {**size** | **chain** | **timeout** *limit*} *interface*

シンタックスの説明

chain *limit*	完全な IP パケットがフラグメント化されるパケット数の最大値を示す。
interface	（オプション）セキュリティ アプライアンスのインターフェイスを指定します。インターフェイスが指定されていなければ、このコマンドはすべてのインターフェイスに適用されます。
size *limit*	再構成のために待機している IP 再構成データベースに含めることができる、パケットの最大数を設定します。
timeout *limit*	フラグメント化されたパケット全体の到着を待つ最大秒数を指定します。タイマーは、パケットの最初のフラグメントが到着すると始動します。指定した秒数以内にパケットのすべてのフラグメントが到着しない場合、それまでに受信したパケット フラグメントはすべて廃棄されます。

デフォルト

デフォルトは次のとおりです。

- ***chain*** は 24 パケットです。
- *interface* はすべてのインターフェイスです。
- ***size*** は 200 です。
- ***timeout*** は 5 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	このコマンドは、***chain***、***size***、または ***timeout*** のいずれかの引数を必ず選択するように変更されました。ソフトウェアの以前のリリースでサポートされていた、これらの引数を入力しない ***fragment*** コマンドは、入力できなくなりました。

使用上のガイドライン

デフォルトでは、セキュリティ アプライアンスは、完全な IP パケットの再構築をするために、最大 24 個のフラグメントを受け入れます。ネットワーク セキュリティ ポリシーに基づいて、各インターフェイスについて **fragment chain 1** *interface* コマンドを入力することで、フラグメント化されたパケットがセキュリティ アプライアンスを通過できなくするようにセキュリティ アプライアンスの設定を検討する必要があります。制限に 1 を設定すると、すべてのパケットが元のまま、つまり、フラグメント化されていない状態である必要があります。

セキュリティ アプライアンスを通過するネットワーク トラフィックのほとんどが NFS である場合、データベースのオーバーフローを防ぐため、さらに調整が必要になる可能性があります。

WAN インターフェイスなどのように NFS サーバとクライアントの間の MTU サイズが小さな環境では、**chain** キーワードをさらに調整する必要があります。この場合、効率を改善するには NFS over TCP の使用を推奨します。

size *limit* に大きな値を設定すると、セキュリティ アプライアンスは、さらにフラグメント フラッディングによる DoS 攻撃を受けやすくなります。***size limit*** に 1550 プールまたは 16384 プール内のブロックの総数以上の値を設定しないでください。

デフォルト値では、フラグメント フラッディングによって発生する DoS 攻撃が制限されます。

例

次の例は、フラグメント化したパケットを外部および内部のインターフェイスで防ぐ方法を示しています。

```
hostname(config)# fragment chain 1 outside
hostname(config)# fragment chain 1 inside
```

パケットのフラグメント化をさせない追加インターフェイスそれぞれに対して、続けて **fragment chain 1** *interface* コマンドを入力します。

次の例では、外部インターフェイスのフラグメント データベースを、最大サイズ 2000、最大チェイン長 45、待ち時間 10 秒に設定する方法を示しています。

```
hostname(config)# fragment size 2000 outside
hostname(config)# fragment chain 45 outside
hostname(config)# fragment timeout 10 outside
```

関連コマンド

コマンド	説明
clear configure fragment	すべての IP フラグメント再構成コンフィギュレーションを、デフォルトにリセットします。
clear fragment	IP フラグメント再構成モジュールの運用データを消去します。
show fragment	IP フラグメント再構成モジュールの運用データを表示します。
show running-config fragment	IP フラグメント再構成コンフィギュレーションを表示します。

ftp-map

厳密な FTP 検査のパラメータを定義するとき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 **ftp-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。

ftp-map *map_name*

no ftp-map *map_name*

シンタックスの説明

map_name	FTP 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	このコマンドが導入されました。

使用上のガイドライン

厳密な FTP 検査のパラメータを定義するときに使用する特定のマップを指定するには、**ftp-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 FTP マップ 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。FTP クライアントが特定のコマンドを FTP サーバに送信するのを防ぐには、**request-command deny** コマンドを使用します。

FTP マップを定義したら、**inspect ftp strict** 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。

例

次の例は、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 ftp-port
hostname(config-cmap)# match port tcp eq 21
hostname(config-cmap)# exit
hostname(config)# ftp-map inbound_ftp
hostname(config-ftp-map)# 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
```

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。
inspect ftp	アプリケーション検査用に特定の FTP マップを適用します。
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。

ftp mode passive

FTP モードをパッシブに設定するには、グローバル コンフィギュレーション モードで **ftp mode passive** コマンドを使用します。FTP クライアントをアクティブ モード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。

ftp mode passive

no ftp mode passive

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	このコマンドが導入されました。

使用上のガイドライン

ftp mode passive コマンドは、FTP モードをパッシブに設定します。セキュリティ アプライアンスは、イメージ ファイルまたはコンフィギュレーション ファイルの FTP サーバへのアップロードや FTP サーバからのダウンロードに FTP を使用できます。**ftp mode passive** コマンドは、セキュリティ アプライアンス上の FTP クライアントが FTP サーバと対話する方法を設定します。

パッシブ FTP では、クライアントが制御接続とデータ接続の両方を開始します。パッシブ モードはサーバ状態を参照します。つまり、サーバは、クライアントによって開始された制御接続とデータ接続の両方を受動的に受け入れます。

パッシブ モードでは、宛先ポートと送信元ポートの両方が一時ポートです（1023 より大きい）。クライアントが **passive** コマンドを発行してパッシブなデータ接続の設定を開始するため、このモードはクライアントにより設定されます。パッシブ モードでのデータ接続の受信者であるサーバは、特定の接続をリスンしているポート番号で応答します。

例

次の例では、FTP モードをパッシブに設定します。

```
hostname(config)# ftp mode passive
```

関連コマンド

copy	イメージ ファイルまたはコンフィギュレーション ファイルを FTP サーバとの間でアップロードまたはダウンロードします。
debug ftp client	FTP クライアントのアクティビティに関する詳細な情報を表示します。
show running-config ftp mode	FTP クライアントのコンフィギュレーションを表示します。

functions

このユーザまたはグループポリシーに対して、WebVPN 経由でファイル アクセスとファイル ブラウジング、MAPI プロキシ、HTTP プロキシ、および URL エントリを設定するには、グループポリシーまたはユーザ名モードから入力する webvpn モードで **functions** コマンドを使用します。設定済み機能を削除するには、このコマンドの **no** 形式を使用します。

functions none コマンドを発行して作成されたヌル値を含むすべての設定済み機能を削除するには、このコマンドの **no** 形式を引数なしで使用します。**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。機能の値を継承しないようにするには、**functions none** コマンドを使用します。

functions {**file-access | file-browsing | file-entry | filter | http-proxy | url-entry | mapi | port-forward | none**}

no functions [**file-access | file-browsing | file-entry | filter | url-entry | mapi | port-forward**]

シンタックスの説明

file-access	ファイル アクセスをイネーブルまたはディセーブルにします。イネーブルの場合、WebVPN のホームページにはサーバ リスト内のファイル サーバが一覧表示されます。ファイル ブラウジングまたはファイル エントリをイネーブルにするには、ファイル アクセスをイネーブルにする必要があります。
file-browsing	ファイル サーバおよび共有のブラウジングをイネーブルまたはディセーブルにします。ファイル サーバのユーザ エントリを許可するには、ファイル ブラウジングをイネーブルにする必要があります。
file-entry	ファイル サーバの名前を入力するユーザ機能をイネーブルまたはディセーブルにします。
filter	webtype ACL を適用します。イネーブルにすると、セキュリティ アプライアンスは webvpn の **filter** コマンドで定義された webtype ACL を適用します。
http-proxy	クライアントへの HTTP アプレット プロキシの転送をイネーブルまたはディセーブルにします。プロキシは、Java、ActiveX、および Flash などの独特のマングリングに干渉するテクノロジーに効果的です。プロキシを使用するとマングリングはバイパスされますが、セキュリティ アプライアンスの使用は確実に継続されます。転送されたプロキシはブラウザの古いプロキシ設定を自動的に変更し、すべての HTTP および HTTPS 要求を新しいプロキシ設定にリダイレクトします。HTML、CSS、JavaScript、VBScript、ActiveX、および Java を含む、すべてのクライアント側のテクノロジーを実質的にサポートします。サポートしているブラウザは、Microsoft Internet Explorer だけです。
mapi	Microsoft Outlook/Exchange のポート転送をイネーブルまたはディセーブルにします。
none	すべての WebVPN **functions** にヌル値を設定します。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機能を継承しないようにします。
port-forward	ポート転送をイネーブルにします。イネーブルにすると、セキュリティ アプライアンスは webvpn の **port-forward** コマンドで定義されたポート フォワーディング リストを使用します。
url-entry	URL のユーザ エントリをイネーブルまたはディセーブルにします。イネーブルになっても、セキュリティ アプライアンスは依然として URL を任意の設定された URL またはネットワーク ACL に制限します。URL エントリをディセーブルにすると、セキュリティ アプライアンスは WebVPN ユーザをホームページ上の URL に制限します。

デフォルト

デフォルトでは、この機能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
WebVPN モード	•	—	•	—	—

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

例

次の例は、FirstGroup という名前のグループポリシーに対してファイル アクセス、ファイル ブラウジング、および MAPI プロキシ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)# functions file-access file-browsing MAPI
```

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。
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。