CHAPTER 10

database path コマンド～ debug xml コマンド

database path

ローカル CA サーバ データベースのパスまたは位置を指定するには、CA サーバ コンフィギュレーション モードで **database** コマンドを使用します。フラッシュ メモリへのパスをデフォルト設定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。

[no] database path *mount-name directory-path*

構文の説明

directory-path	CA ファイルが保存される、マウント ポイント上のディレクトリへのパスを指定します。
mount-name	マウント名を指定します。

デフォルト

デフォルトでは、CA サーバ データベースはフラッシュ メモリに保存されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

データベースに保存されるローカル CA ファイルには、証明書データベース ファイル、ユーザ データベース ファイル、一時 PKCS12 ファイル、および現在の CRL ファイルが含まれます。*mount-name* は、セキュリティ アプライアンスのファイル システムを指定するために使用する **mount** コマンドの *name* 引数と同じです。

（注） これらの CA ファイルは内部保存ファイルです。変更しないでください。

例

次に、CA データベースのマウント ポイントを cifs_share と定義する例を示します。また、マウント ポイント上のデータベース ファイル ディレクトリを ca_dir/files_dir と定義しています。

```
hostname(config)# crypto ca server
hostname(config-ca-server)# database path cifs_share ca_dir/files_dir/
hostname(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	ローカル CA の設定および管理が可能な CA サーバ コンフィギュレーション モードの CLI コマンド セットへのアクセスを提供します。
crypto ca server user-db write	ローカル CA データベースに設定されているユーザ情報をディスクに書き込みます。
debug crypto ca server	ユーザがローカル CA サーバを設定する場合にデバッグ メッセージを表示します。
mount	Common Internet File System（CIFS; 共通インターネット ファイル システム）および File Transfer Protocol File Systems（FTPFS; ファイル転送プロトコル ファイル システム）の一方または両方を、セキュリティ アプライアンスがアクセスできるようにします。
show crypto ca server	セキュリティ アプライアンスの CA コンフィギュレーションの特性を表示します。
show crypto ca server cert-db	CA サーバが発行する証明書を表示します。

ddns (DDNS-update-method)

DDNS 更新方式のタイプを指定するには、DDNS 更新方式モードで **ddns** コマンドを使用します。実行コンフィギュレーションから更新方式タイプを削除するには、このコマンドの **no** 形式を使用します。

ddns [**both**]

no ddns [**both**]

構文の説明

both	（任意）DNS A と PTR の両方の Resource Record（RR; リソース レコード）の更新を指定します。

デフォルト

A RR のみ更新します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

Dynamic DNS（DDNS; ダイナミック DNS）は、DNS で管理されている名前からアドレスへのマッピング、およびアドレスから名前へのマッピングを更新します。DDNS 更新を実行するための 2 つの方式（RFC 2136 で規定されている IETF 標準、および一般的な HTTP 方式）のうち、セキュリティ アプライアンスのこのリリースでは、IETF 方式をサポートしています。

次の 2 つのタイプの Resource Record（RR; リソース レコード）に、名前マッピングおよびアドレス マッピングが含まれます。

- A リソース レコードには、ドメイン名から IP アドレスへのマッピングが含まれます。
- PTR リソース レコードには、IP アドレスからドメイン名へのマッピングが含まれます。

DDNS アップデートを使用して、A RR タイプと PTR RR タイプとの間で一貫した情報を保持できます。

DDNS 更新方式コンフィギュレーション モードで **ddns** コマンドを発行するとき、更新を A RR に対してのみ行うか、A RR と PTR RR の両方に対して行うかを定義します。

例

次に、ddns-2 という名前の DDNS 更新方式に対し A と PTR の両方の RR の更新を設定する例を示します。

```
hostname(config)# ddns update method ddns-2
hostname(DDNS-update-method)# ddns both
```

関連コマンド

コマンド	説明
ddns update（インターフェイス コンフィギュレーション モード）	Dynamic DNS（DDNS; ダイナミック DNS）アップデート方式を、セキュリティ アプライアンスのインターフェイスまたは DDNS アップデート ホスト名に関連付けます。
ddns update method（グローバル コンフィギュレーション モード）	DNS のリソース レコードをダイナミックにアップデートするための方式を作成します。
dhcp-client update dns	DHCP クライアントが DHCP サーバに渡すアップデート パラメータを設定します。
dhcpd update dns	DHCP サーバによる DDNS アップデートの実行をイネーブルにします。
interval maximum	DDNS アップデート方式によるアップデート試行の最大間隔を設定します。

ddns update（インターフェイス コンフィギュレーション）

Dynamic DNS（DDNS; ダイナミック DNS）更新方式を、セキュリティ アプライアンス インターフェイスまたは更新ホスト名に関連付けるには、インターフェイス コンフィギュレーション モードで **ddns update** コマンドを使用します。DDNS 更新方式とインターフェイスまたはホスト名とのアソシエーションを、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。

ddns update [*method-name* | **hostname** *hostname*]

no ddns update [*method-name* | **hostname** *hostname*]

構文の説明

hostname	コマンド文字列内の後続の語をホスト名として指定します。
hostname	更新で使用するホスト名を指定します。
method-name	設定するインターフェイスとのアソシエーションの方式名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

DDNS 更新方式を定義した後、DDNS 更新をトリガーするために、その DDNS 更新方式をセキュリティ アプライアンス インターフェイスに関連付ける必要があります。

ホスト名は、Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）またはホスト名のみを指定できます。ホスト名のみ指定した場合、セキュリティ アプライアンスは、ドメイン名をホスト名に追加して FQDN を作成します。

例

次に、インターフェイス GigabitEthernet0/2 に ddns-2 という名前の DDNS 更新方式およびホスト名 hostname1.example.com を関連付ける例を示します。

```
hostname(config)# interface GigabitEthernet0/2
hostname(config-if)# ddns update ddns-2
hostname(config-if)# ddns update hostname hostname1.example.com
```

関連コマンド

コマンド	説明
ddns（DDNS 更新方式モード）	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
ddns update method（グローバル コンフィギュレーション モード）	DNS のリソース レコードをダイナミックにアップデートするための方式を作成します。
dhcp-client update dns	DHCP クライアントが DHCP サーバに渡すアップデート パラメータを設定します。
dhcpd update dns	DHCP サーバによる DDNS アップデートの実行をイネーブルにします。
interval maximum	DDNS アップデート方式によるアップデート試行の最大間隔を設定します。

ddns update method（グローバル コンフィギュレーション モード）

DNS Resource Record（RR; リソース レコード）をダイナミックに更新するための方式を作成するには、グローバル コンフィギュレーション モードで **ddns update method** コマンドを使用します。実行コンフィギュレーションから Dynamic DNS（DDNS; ダイナミック DNS）更新方式を削除するには、このコマンドの **no** 形式を使用します。

ddns update method *name*

no ddns update method *name*

構文の説明

name	ダイナミックに DNS レコードを更新するための方式の名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

DDNS は、DNS で保持されている名前/アドレスおよびアドレス/名前のマッピングを更新します。**ddns update method** コマンドで設定する更新方式により、ダイナミック DNS 更新の実行方法および実行頻度が決まります。DDNS 更新を実行するための 2 つの方式（RFC 2136 で規定されている IETF 標準、および一般的な HTTP 方式）のうち、セキュリティ アプライアンスのこのリリースでは、IETF 方式をサポートしています。

次の 2 つのタイプの Resource Record（RR; リソース レコード）に、名前マッピングおよびアドレス マッピングが含まれます。

- A リソース レコードには、ドメイン名から IP アドレスへのマッピングが含まれます。
- PTR リソース レコードには、IP アドレスからドメイン名へのマッピングが含まれます。

DDNS アップデートを使用して、A RR タイプと PTR RR タイプとの間で一貫した情報を保持できます。

（注） **ddns update method** を実行する前に、インターフェイスでドメイン ルックアップをイネーブルにした状態で、**dns** コマンドを使用して到達可能なデフォルト DNS サーバを設定する必要があります。

例

次に、ddns-2 という名前の DDNS 更新方式を設定する例を示します。

```
hostname(config)# ddns update method ddns-2
```

関連コマンド

コマンド	説明
ddns（DDNS 更新方式モード）	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
ddns update（インターフェイス コンフィギュレーション モード）	Dynamic DNS（DDNS; ダイナミック DNS）アップデート方式を、セキュリティ アプライアンスのインターフェイスまたは DDNS アップデート ホスト名に関連付けます。
dhcp-client update dns	DHCP クライアントが DHCP サーバに渡すアップデート パラメータを設定します。
dhcpd update dns	DHCP サーバによるダイナミック DNS アップデートの実行をイネーブルにします。
interval maximum	DDNS アップデート方式によるアップデート試行の最大間隔を設定します。

debug aaa

AAA 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 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** | **common** | **internal** | **vpn** [*level*]]

no debug aaa

構文の説明

accounting	（任意）アカウンティングのデバッグ メッセージのみ表示します。
authentication	（任意）認証のデバッグ メッセージのみ表示します。
authorization	（任意）認可のデバッグ メッセージのみ表示します。
common	（任意）AAA 機能内の各種状態に関するデバッグ メッセージを表示します。
internal	（任意）ローカル データベースがサポートする AAA 機能に関するデバッグ メッセージのみ表示します。
level	（任意）デバッグ レベルを指定します。**vpn** キーワードを指定した場合に限り有効です。
vpn	（任意）VPN 関連の AAA 機能のデバッグ メッセージのみ表示します。

デフォルト

デフォルトの *level* は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.0(1)	このコマンドは変更され、新しいキーワードが追加されました。

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、イネーブルになっているすべてのデバッグをオフにします。

例

次に、ローカル データベースがサポートする AAA 機能のデバッグをイネーブルにする例を示します。

```
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 appfw

アプリケーション インスペクションに関する詳細情報を表示するには、特権 EXEC モードで **debug appfw** 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 appfw [**chunk** | **event** | **eventverb** | **regex**]

no debug appfw [**chunk** | **event** | **eventverb** | **regex**]

構文の説明

chunk	（任意）チャンク転送エンコード パケットの処理に関する実行時情報を表示します。
event	（任意）パケット インスペクション イベントに関するデバッグ情報を表示します。
eventverb	（任意）イベントへの応答でセキュリティ アプライアンスが実行したアクションを表示します。
regex	（任意）定義済みシグニチャを使用したマッチング パターンに関する情報を表示します。

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です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

debug appfw コマンドは、HTTP アプリケーション インスペクション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、イネーブルになっているすべてのデバッグ コマンドをオフにします。

例

次に、アプリケーション インスペクションに関する詳細情報の表示をイネーブルにする例を示します。

```
hostname# debug appfw
```

関連コマンド

コマンド	説明
http-map	拡張 HTTP インスペクションを設定するための HTTP マップを定義します。
inspect http	アプリケーション インスペクション用に特定の HTTP マップを適用します。

debug arp

ARP 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 arp** コマンドを使用します。ARP のデバッグ 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

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
既存	このコマンドは既存です。

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でトラフィックが遅くなる可能性があります。

例

次に、ARP のデバッグ メッセージをイネーブルにする例を示します。

```
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 インスペクションのデバッグ メッセージを表示するには、特権 EXEC モードで **debug arp-inspection** コマンドを使用します。ARP インスペクションのデバッグ 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

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

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

例

次に、ARP インスペクションのデバッグ メッセージをイネーブルにする例を示します。

```
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	トランスペアレント ファイアウォール モードで、ARP パケットを調査し、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*

構文の説明

level	（任意）デバッグ レベルを指定します。

デフォルト

デフォルトの *level* は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.0(1)	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 プロセスで高プライオリティ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。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、ASDM のレベル 1 デバッグをイネーブルにする例を示します。

```
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 context

セキュリティ コンテキストを追加または削除するときにデバッグ 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。コンテキストのデバッグ 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*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

デフォルトの level は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

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

例

次に、コンテキスト管理のデバッグ メッセージをイネーブルにする例を示します。

```
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 モードを開始します。
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。コントロール 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*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

デフォルトの level は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
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でトラフィックが遅くなる可能性があります。

例

次に、コントロール プレーンのデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug cplane
```

関連コマンド

コマンド	説明
hw-module module recover	リカバリ イメージを TFTP サーバからロードして、インテリジェント SSM を回復します。
hw-module module reset	SSM をシャットダウンし、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。

コマンド	説明
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準備をして、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 で使用される）PKI アクティビティのデバッグ メッセージを表示するには、特権 EXEC モードで **debug crypto ca** コマンドを使用します。PKI のデバッグ 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*]

構文の説明

messages	（任意）PKI 入力および出力メッセージのデバッグ メッセージのみ表示します。
transactions	（任意）PKI トランザクションのデバッグ メッセージのみ表示します。
level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。レベル 1（デフォルト）では、エラーが発生した場合に限り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メッセージが表示されます。

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 level は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
既存	このコマンドは既存です。

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でトラフィックが遅くなる可能性があります。

例

次に、PKI のデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug crypto ca
```

関連コマンド

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

debug crypto ca server

ローカル CA サーバのデバッグ メッセージのレベルを設定し、関連するデバッグ メッセージのリスト表示を開始するには、CA サーバ コンフィギュレーション モードで **debug crypto ca server** コマンドを使用します。すべてのデバッグ メッセージのリスト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 server [*level*]

no debug crypto ca server [*level*]

構文の説明

level	表示するデバッグ メッセージのレベルを設定します。指定できる値の範囲は 1 ～ 255 です。

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 モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	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でトラフィックが遅くなる可能性があります。レベル 5 以上は raw データ ダンプ用に予約されており、デバッグ出力が非常に多くなるため、通常のデバッグ時には使用しないでください。

例

次の例では、デバッグ レベルを 3 に設定しています。

```
hostname(config-ca-server)# debug crypto ca server 3
hostname(config-ca-server)#
```

次に、すべてのデバッグをオフにする例を示します。

```
hostname(config-ca-server)# no debug crypto ca server
hostname(config-ca-server)#
```

関連コマンド

コマンド	説明
cdp-url	CA が発行する証明書に含める Certificate Revocation List（CRL; 証明書失効リスト）Distribution Point（CDP; 証明書失効リスト分散ポイント）を指定します。
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
database path	ローカル CA サーバ データベースのパスまたは位置を指定します。
show crypto ca server	ASCII テキスト形式でセキュリティ アプライアンスの認証局のコンフィギュレーションの特性を表示します。
show crypto ca server certificate	base64 形式でローカル CA コンフィギュレーションを表示します。
show crypto ca server crl	ローカル CA の現在の CRL を表示します。

debug crypto condition

指定した条件に基づき IPSec および ISAKMP のデバッグ メッセージをフィルタリングするには、特権 EXEC モードで **debug crypto condition** コマンドを使用します。他の条件に影響を与えずに単一のフィルタリング条件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 crypto condition [[peer [address *peer_addr*] **subnet** *subnet_mask*]] | [**user** *user_name*] | [**group** *group_name*] | [spi *spi*] | [**reset**]

[no] debug crypto condition [[peer [address *peer_addr*] **subnet** *subnet_mask*]] | [**user** *user_name*] | [**group** *group_name*] | [**spi** *spi*] | [**reset**]

構文の説明

group *group_name*	使用するグループおよびクライアント グループ名を指定します。
peer *peer_addr*	IPSec ピアおよびその IP アドレスを指定します。
reset	すべてのフィルタリング条件をクリアし、フィルタリングをディセーブルにします。
spi *spi*	IPSec SPI を指定します。
subnet *subnet_mask*	指定した IP アドレスに関連するサブネットおよびサブネット マスクを指定します。
user *user_name*	使用するクライアントおよびクライアント ユーザ名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
8.0(2)	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 crypto condition コマンドは、syslog メッセージの表示やロギングには影響しません。この機能はコンフィギュレーションには保存されず、電源を再投入するたびにリセットする必要があります。

例

次に、ネットワーク 10.1.1.0 およびピア 10.2.2.2 のフィルタを設定する例を示します。

```
hostname# debug crypto condition peer address 10.1.1.0 subnet 255.255.255.0
hostname# debug crypto condition peer address 10.2.2.2
```

次に、ユーザ「example_user」のフィルタを設定する例を示します。

```
hostname# debug crypto condition user example_user
```

次に、デバッグ フィルタをクリアする例を示します。

```
hostname# debug crypto condition reset
```

関連コマンド

コマンド	説明
debug crypto condition error	フィルタリング条件が指定されているかどうかのデバッグ メッセージを表示します。
debug crypto condition unmatched	フィルタリングに十分なコンテキスト情報が含まれていない IPSec および ISAKMP のデバッグ メッセージを表示します。
show crypto debug-condition	IPSec および ISAKMP デバッグ メッセージに設定されているフィルタを表示します。

debug crypto condition error

IPSec および ISAKMP のデバッグ メッセージが設定済みのフィルタに一致するかどうかに関係なく、それらのデバッグ メッセージを表示するには、特権 EXEC モードで **debug crypto condition error** コマンドを使用します。IPSec および ISAKMP のデバッグ メッセージが設定済みのフィルタに一致するかどうかに関係なく、それらのデバッグ メッセージを表示しないようにするには、このコマンドの **no** 形式を使用します。

debug crypto condition error [[ipsec | isakmp]

[no] debug crypto condition error [ipsec | isakmp]

構文の説明

ipsec	IPSec デバッグ メッセージ システムを指定します。
isakmp	ISAKMP デバッグ メッセージ システムを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
8.0(2)	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 crypto condition error コマンドは、syslog メッセージの表示やロギングには影響しません。この機能はコンフィギュレーションには保存されず、電源を再投入するたびにリセットする必要があります。

例

次に、フィルタリング条件が指定されているかどうかに関係なく、IPSec メッセージが表示されるように設定する例を示します。

```
hostname# debug crypto condition error ipsec
```

関連コマンド

コマンド	説明
debug crypto condition	IPSec および ISAKMP デバッグ メッセージのフィルタリング条件を設定します。

コマンド	説明
debug crypto condition unmatched	フィルタリングに十分なコンテキスト情報が含まれていない IPSec および ISAKMP のデバッグ メッセージを表示します。
show crypto debug-condition	IPSec および ISAKMP デバッグ メッセージに設定されているフィルタを表示します。

debug crypto condition unmatched

フィルタリングのための十分なコンテキスト情報を含まない IPSec および ISAKMP 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 crypto condition unmatched** コマンドを使用します。十分なコンテキスト情報を含まない IPSec および ISAKMP のデバッグ メッセージをフィルタリングするには、このコマンドの **no** 形式を使用します。

debug crypto condition unmatched [[ipsec | isakmp]

[no] debug crypto condition unmatched [ipsec | isakmp]

構文の説明

ipsec	IPSec デバッグ メッセージ システムを指定します。
isakmp	ISAKMP デバッグ メッセージ システムを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
8.0(2)	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 crypto condition unmatched コマンドは、syslog メッセージの表示やロギングには影響しません。この機能はコンフィギュレーションには保存されず、電源を再投入するたびにリセットする必要があります。

例

次に、十分なコンテキストを含まない IPSec メッセージが表示されるようにフィルタを設定する例を示します。

```
hostname# debug crypto condition unmatched ipsec
```

関連コマンド

コマンド	説明
debug crypto condition	IPSec および ISAKMP デバッグ メッセージのフィルタリング条件を設定します。

コマンド	説明
debug crypto condition error	フィルタリング条件が指定されているかどうかのデバッグ メッセージを表示します。
show crypto debug-condition	IPSec および ISAKMP デバッグ メッセージに設定されているフィルタを表示します。

debug crypto engine

クリプト エンジンのデバッグ メッセージを表示するには、特権 EXEC モードで **debug crypto engine** コマンドを使用します。クリプト エンジンのデバッグ 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*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

デフォルトの level は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
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でトラフィックが遅くなる可能性があります。

例

次に、クリプト エンジンのデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug crypto engine
```

関連コマンド

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

debug crypto ipsec

IPSec 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 crypto ipsec** コマンドを使用します。IPSec のデバッグ 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*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

デフォルトの level は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
既存	このコマンドは既存です。

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でトラフィックが遅くなる可能性があります。

例

次に、IPSec のデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug crypto ipsec
```

関連コマンド

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

debug crypto isakmp

ISAKMP 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 crypto isakmp** コマンドを使用します。ISAKMP のデバッグ 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*]

構文の説明

timers	（任意）ISAKMP タイマー失効のデバッグ メッセージを表示します。
level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。レベル 1（デフォルト）では、エラーが発生した場合に限り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、ヒト可読形式で復号化 ISAKMP パケットが表示されます。レベル 255 では、復号化 ISAKMP パケットの 16 進数ダンプが表示されます。

デフォルト

デフォルトの level は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
既存	このコマンドは既存です。

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でトラフィックが遅くなる可能性があります。

例

次に、ISAKMP のデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug crypto isakmp
```

関連コマンド

コマンド	説明
debug crypto ca	CA のデバッグ メッセージを表示します。

コマンド	説明
debug crypto engine	暗号化エンジンのデバッグ メッセージを表示します。
debug crypto ipsec	IPSec のデバッグ メッセージを表示します。

debug ctiqbe

CTIQBE アプリケーション インスペクションのデバッグ メッセージを表示するには、特権 EXEC モードで **debug ctiqbe** コマンドを使用します。CTIQBE アプリケーション インスペクションのデバッグ 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*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
既存	このコマンドは既存です。

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。すべてのデバッグ メッセージの表示を停止するには、**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トラフィックが遅くなる可能性があります。

例

次に、CTIQBE アプリケーション インスペクションに対しデフォルト レベル（1）でデバッグ メッセージをイネーブルにする例を示します。

```
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 インスペクションをイネーブルにします。

コマンド	説明
show ctiqbe	セキュリティ アプライアンスを通じて確立された 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 ctl-provider

証明書信頼リスト プロバイダーのデバッグ メッセージを表示するには、特権 EXEC モードで **debug ctl-provider** 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 ctl-provider [**errors** | **events** | **parser**]

no debug ctl-provider [**errors** | **events** | **parser**]

構文の説明

errors	CTL プロバイダー エラー デバッグを指定します。
events	CTL プロバイダー イベント デバッグを指定します。
parser	CTL プロバイダー パーサー デバッグを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
8.0(2)	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でトラフィックが遅くなる可能性があります。

例

次に、CTL プロバイダーのデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug ctl-provider
```

関連コマンド

コマンド	説明
ctl	CTL クライアントの CTL ファイルを解析し、トラストポイントをインストールします。
ctl-provider	CTL プロバイダー モードで CTL プロバイダー インスタンスを設定します。
export	クライアントにエクスポートする証明書を指定します。
service	CTL プロバイダーがリッスンするポートを指定します。

debug dap

ダイナミック アクセス ポリシー イベントのロギングをイネーブルにするには、特権 EXEC モードで **debug dap** コマンドを使用します。DAP デバッグ メッセージのロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug dap {errors | trace}

no debug dap [errors | trace]

構文の説明

errors	DAP 処理エラーを指定します。
trace	DAP 機能トレースを指定します。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力には高いプライオリティが割り当てられるため、システムが使用できなくなることがあります。したがって、debug コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、debug コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、debug コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次の例は、DAP トレース デバッグをイネーブルにする方法を示しています。

```
hostname # debug dap trace
hostname #
```

関連コマンド

コマンド	説明
dynamic-access-policy-record	DAP レコードを作成します。

debug ddns

DDNS 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 ddns** コマンドを使用します。デバッグ メッセージをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug ddns

no debug ddns

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

debug ddns コマンドは、DDNS に関する詳細情報を表示します。**undebug ddns** は、**no debug ddns** コマンドと同様に、DDNS デバッグ情報をオフにします。

デバッグ出力は CPU プロセスで高プライオリティ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。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、DDNS デバッグ メッセージをイネーブルにする例を示します。

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

関連コマンド

コマンド	説明
ddns（**DDNS 更新方式モード**）	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。

コマンド	説明
ddns update（インターフェイス コンフィギュレーション モード）	DDNS アップデート方式をセキュリティ アプライアンスのインターフェイスまたは DDNS アップデート ホスト名に関連付けます。
ddns update method（グローバル コンフィギュレーション モード）	DNS のリソース レコードをダイナミックにアップデートするための方式を作成します。
show running-config ddns	実行コンフィギュレーションに設定されているすべての DDNS 方式のタイプおよび間隔を表示します。

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*]

構文の説明

detail	DHCP クライアントに関連する詳細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	（任意）デバッグ レベルを指定します。有効な値の範囲は 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 モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
既存	このコマンドは既存です。

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 プロセスで高プライオリティ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。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、DHCP クライアントのデバッグをイネーブルにするためのコマンドの使用例を示します。

```
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情報を表示します。
show running-config interface	指定し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*]

構文の説明

event	DHCP サーバに関連するイベント情報を表示します。
level	（任意）デバッグ レベルを指定します。有効な値の範囲は 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 モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
既存	このコマンドは既存です。

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。

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

デバッグ出力は CPU プロセスで高プライオリティ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。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、DHCP イベントのデバッグをイネーブルにする例を示します。

```
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 dhcpd ddns

DHCP DDNS 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 ddns** 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 ddns [*level*]

no debug dhcpd ddns [*level*]

構文の説明

level	（任意）デバッグ レベルを指定します。有効値の範囲は、1 ～ 255 です。

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 モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

debug dhcpd ddns コマンドは、DHCP および DDNS に関する詳細情報を表示します。**undebug dhcpd ddns** コマンドは、**no debug dhcpd ddns** コマンドと同様に、DHCP と DDNS のデバッグ情報をオフにします。

デバッグ出力は CPU プロセスで高プライオリティ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。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、DHCP DDNS のデバッグをイネーブルにする例を示します。

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

関連コマンド

コマンド	説明
dhcpd update dns	DHCP サーバによるダイナミック DNS アップデートの実行をイネーブルにします。
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。
show running-config ddns	実行コンフィギュレーションの DDNS 更新方式を表示します。

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*]

構文の説明

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	（任意）デバッグ レベルを指定します。有効な値の範囲は 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 モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティ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。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、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の例を示します。

```
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 エージェントの統計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	DHCP リレー エージェントの現在の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**}

構文の説明

file	ファイルレベルのディスク 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	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
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 プロセスで高プライオリティ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。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、ファイルレベルのディスク デバッグ メッセージをイネーブルにする例を示します。**show debug** コマンドで、ファイルレベルのディスク デバッグ メッセージがイネーブルになっていることを確認できます。**dir** コマンドにより、いくつかのデバッグ メッセージが発生します。

```
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 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 dns** コマンドを使用します。DNS のデバッグ 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*]

構文の説明

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。
level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。
resolver	（任意）DNS リゾルバ メッセージのみ表示します。

デフォルト

デフォルトの level は 1 です。キーワードを指定しない場合、セキュリティ アプライアンスによりすべてのメッセージが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

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

例

次に、DNS のデバッグ メッセージをイネーブルにする例を示します。

```
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 インスペクションをイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

debug eap

EAP イベントのロギングをイネーブルにして NAC メッセージをデバッグするには、特権 EXEC モードで **debug eap** コマンドを使用します。EAP デバッグ メッセージのロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug eap {**all** | **errors** | **events** | **packets** | **sm**}

no debug eap [**all** | **errors** | **events** | **packets** | **sm**]

構文の説明

all	すべての EAP 情報に関するデバッグ メッセージのロギングをイネーブルにします。
errors	EAP パケット エラーのロギングをイネーブルにします。
events	EAP セッション イベントのロギングをイネーブルにします。
packets	EAP パケット情報に関するデバッグ メッセージのロギングをイネーブルにします。
sm	EAP ステート マシン情報に関するデバッグ メッセージのロギン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 モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、セキュリティ アプライアンスは、EAP セッション状態の変化および EAP ステータス クエリー イベントを記録し、16 進数形式で EAP およびパケット コンテンツの完全レコードを生成します。

デバッグ出力には高いプライオリティが割り当てられるため、システムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、すべての EAP セッション イベントのロギングをイネーブルにする例を示します。

```
hostname# debug eap events
hostname#
```

次に、すべての EAP デバッグ メッセージのロギングをイネーブルにする例を示します。

```
hostname# debug eap all
hostname#
```

次に、すべての EAP デバッグ メッセージのロギングをディセーブルにする例を示します。

```
hostname# no debug eap
hostname#
```

関連コマンド

コマンド	説明
debug eou	NAC メッセージングをデバッグするための EAPoUDP イベントのロギングをイネーブルにします。
debug nac	NAC イベントのロギングをイネーブルにします。
eou initialize	1 つ以上の NAC セッションに割り当てられているリソースを消去し、セッションごとに、新しい無条件のポスチャ確認を開始します。
eou revalidate	1 つ以上の NAC セッションの即時ポスチャ確認を強制実行します。
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 eigrp fsm

DUAL 有限状態マシンのデバッグ情報を表示するには、特権 EXEC モードで **debug eigrp 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 eigrp fsm

no debug eigrp fsm

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、EIGRP フィジブル サクセサ アクティビティをモニタし、ルート更新がルーティング プロセスによりインストールされているかどうか、および削除されているかどうかを確認できます。

デバッグ出力は CPU プロセスで高プライオリティ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、Cisco TAC 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、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、**debug eigrp fsm** コマンドの出力例を示します。

```
hostname# debug eigrp fsm

DUAL: dual_rcvupdate(): 172.25.166.0 255.255.255.0 via 0.0.0.0 metric 750080/0
DUAL: Find FS for dest 172.25.166.0 255.255.255.0. FD is 4294967295, RD is 4294967295
found
DUAL: RT installed 172.25.166.0 255.255.255.0 via 0.0.0.0
DUAL: dual_rcvupdate(): 192.168.4.0 255.255.255.0 via 0.0.0.0 metric 4294967295/4294967295
DUAL: Find FS for dest 192.168.4.0 255.255.255.0. FD is 2249216, RD is 2249216
DUAL:   0.0.0.0 metric 4294967295/4294967295not found Dmin is 4294967295
```

```
DUAL: Dest 192.168.4.0 255.255.255.0 not entering active state.
DUAL: Removing dest 192.168.4.0 255.255.255.0, nexthop 0.0.0.0
DUAL: No routes. Flushing dest 192.168.4.0 255.255.255.0
```

最初の行の DUAL は Diffusing Update Algorithm（DUAL; 拡散更新アルゴリズム）の略語です。DUAL は、ルーティングを決定する EIGRP 内の基本メカニズムです。次の 3 つのフィールドは、宛先ネットワークのインターネット アドレスとマスク、および更新を受信したときに経由したアドレスです。metric フィールドは、ルーティング データベースに保存されているメトリック、および情報を送信するネイバーがアドバイタイズしたメトリックを表します。「Metric... inaccessible」という語句が表示された場合、通常、隣接ルータが宛先へのルートを失ったこと、または宛先がホールドダウン状態であることを示します。

次の出力では、EIGRP は、宛先のフィジブル サクセサを検出しようとしています。フィジブル サクセサは、DUAL ループ回避方式の一部です。FD フィールドには、追加のループ回避状態情報が含まれます。RD フィールドはレポートされるディスタンスで、これは更新パケット、クエリー パケット、または応答パケットで使用されるメトリックです。

「not found」メッセージを含むインデントされた行は、192.168.4.0 についてフィジブル サクセサが検出されなかったことを示し、EIGRP が拡散の計算を開始する必要があることを示します。これは、EIGRP が、192.164.4.0 への代替パスを検出するために、ネットワークのアクティブ プローブを開始すること（宛先 192.168.4.0 に関するクエリー パケットを送信すること）を意味します。

```
DUAL: Find FS for dest 192.168.4.0 255.255.255.0. FD is 2249216, RD is 2249216
DUAL:   0.0.0.0 metric 4294967295/4294967295not found Dmin is 4294967295
```

次の出力は、ルート DUAL がルーティング テーブルに正常にインストールされたことを示します。

```
DUAL: RT installed 172.25.166.0 255.255.255.0 via 0.0.0.0
```

次の出力は、宛先へのルートが検出されなかったこと、およびルート情報がトポロジ テーブルから削除されることを示します。

```
DUAL: Dest 192.168.4.0 255.255.255.0 not entering active state.
DUAL: Removing dest 192.168.4.0 255.255.255.0, nexthop 0.0.0.0
DUAL: No routes. Flushing dest 192.168.4.0 255.255.255.0
```

関連コマンド

コマンド	説明
show eigrp topology	EIGRP トポロジ テーブルを表示します。

debug eigrp neighbors

EIGRP により検出されたネイバーのデバッグ情報を表示するには、特権 EXEC モードで **debug eigrp neighbors** 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 eigrp neighbors [**siatimer** | **static**]

no debug eigrp neighbors [**siatimer** | **static**]

構文の説明

siatimer	（任意）アクティブ メッセージの EIGRP スタックを表示します。
static	（任意）EIGRP スタティック ネイバー 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 モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
8.0(2)	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 プロセスで高プライオリティ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、Cisco TAC 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、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、**debug eigrp neighbors static** コマンドの出力例を示します。この例では、スタティック ネイバーの追加と削除、および対応するデバッグ メッセージが示されています。

```
hostname# debug eigrp neighbors static

EIGRP Static Neighbors debugging is on

hostname# configure terminal
hostname(config) router eigrp 100
hostname(config-router)# neighbor 10.86.194.3 interface outside
hostname(config-router)#

EIGRP: Multicast Hello is disabled on Ethernet0/0!
```

```
EIGRP: Add new static nbr 10.86.194.3 to AS 100 Ethernet0/0

hostname(config-router)# no neighbor 10.86.194.3 interface outside
hostname(config-router)#

EIGRP: Static nbr 10.86.194.3 not in AS 100 Ethernet0/0 dynamic list
EIGRP: Delete static nbr 10.86.194.3 from AS 100 Ethernet0/0
EIGRP: Multicast Hello is enabled on Ethernet0/0!

hostname(config-router)# no debug eigrp neighbors static

EIGRP Static Neighbors debugging is off
```

関連コマンド

コマンド	説明
neighbor	EIGRP ネイバーを定義します。
show eigrp neighbors	EIGRP ネイバー テーブルを表示します。

debug eigrp packets

EIGRP パケットのデバッグ情報を表示するには、特権 EXEC モードで **debug eigrp packets** 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 eigrp packets [**SIAquery** | **SIAreply** | **ack** | **hello** | **probe** | **query** | **reply** | **request** | **retry** | **stub** | **terse** | **update** | **verbose**]

no debug eigrp packets [**SIAquery** | **SIAreply** | **ack** | **hello** | **probe** | **query** | **reply** | **request** | **retry** | **stub** | **terse** | **update** | **verbose**]

構文の説明

ack	（任意）デバッグ出力を EIGRP ACK パケットに制限します。
hello	（任意）デバッグ出力を EIGRP hello パケットに制限します。
probe	（任意）デバッグ出力を EIGRP プローブ パケットに制限します。
query	（任意）デバッグ出力を EIGRP クエリー パケットに制限します。
reply	（任意）デバッグ出力を EIGRP 応答パケットに制限します。
request	（任意）デバッグ出力を EIGRP 要求パケットに制限します。
retry	（任意）デバッグ出力を EIGRP 再試行パケットに制限します。
SIAquery	（任意）デバッグ出力をアクティブ クエリー パケットの EIGRP スタックに制限します。
SIAreply	（任意）デバッグ出力をアクティブ応答パケットの EIGRP スタックに制限します。
stub	（任意）デバッグ出力を EIGRP スタブ ルーティング パケットに制限します。
terse	（任意）hello パケット以外のすべての EIGRP パケットを表示します。
update	（任意）デバッグ出力を EIGRP 更新パケットに制限します。
verbose	（任意）すべてのパケット デバッグ メッセージを出力します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

単一のコマンドで複数のパケット タイプを指定できます。以下に例を示します。

```
debug eigrp packets query reply
```

デバッグ出力は CPU プロセスで高プライオリティ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、Cisco TAC 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、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

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

```
hostname# debug eigrp packets

EIGRP: Sending HELLO on Ethernet0/1
       AS 109, Flags 0x0, Seq 0, Ack 0
EIGRP: Sending HELLO on Ethernet0/1
       AS 109, Flags 0x0, Seq 0, Ack 0
EIGRP: Sending HELLO on Ethernet0/1
       AS 109, Flags 0x0, Seq 0, Ack 0
EIGRP: Received UPDATE on Ethernet0/1 from 192.195.78.24,
       AS 109, Flags 0x1, Seq 1, Ack 0
EIGRP: Sending HELLO/ACK on Ethernet0/1 to 192.195.78.24,
       AS 109, Flags 0x0, Seq 0, Ack 1
EIGRP: Sending HELLO/ACK on Ethernet0/1 to 192.195.78.24,
       AS 109, Flags 0x0, Seq 0, Ack 1
EIGRP: Received UPDATE on Ethernet0/1 from 192.195.78.24,
       AS 109, Flags 0x0, Seq 2, Ack 0
```

この出力は、EIGRP パケットの送信と受信を示しています。EIGRP の信頼できるトランスポート アルゴリズムで使用されるシーケンス番号および確認応答番号が出力に表示されています。該当する場合、隣接ルータのネットワーク層アドレスも含まれます。

関連コマンド

コマンド	説明
show eigrp traffic	送受信された EIGRP パケットの数を表示します。

debug eigrp transmit

EIGRP により送信された送信メッセージを表示するには、特権 EXEC モードで **debug eigrp transmit** 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 eigrp transmit [**ack**] [**build**] [**detail**] [**link**] [**packetize**] [**peerdown**] [**sia**] [**startup**] [**strange**]

no debug eigrp transmit [**ack**] [**build**] [**detail**] [**link**] [**packetize**] [**peerdown**] [**sia**] [**startup**] [**strange**]

構文の説明

ack	（任意）システムが送信した Acknowledgment（ACK; 確認応答）メッセージの情報。
build	（任意）構築情報メッセージ（トポロジ テーブルが正常に構築されたこと、または構築できなかったことを示すメッセージ）。
detail	（任意）デバッグ出力の追加詳細。
link	（任意）トポロジ テーブル リンクリストの管理に関する情報。
packetize	（任意）パケット化イベントに関する情報。
peerdown	（任意）ピアがダウンした場合のパケット生成への影響に関する情報。
sia	（任意）Stuck-in-active メッセージ。
startup	（任意）送信されたピア起動パケットおよび初期化パケットに関する情報。
strange	（任意）パケット処理に関連する通常外イベント。

デフォルト

送信イベントを少なくとも 1 つ指定していない場合、すべての送信イベントがデバッグ出力に表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

単一のコマンドで複数の送信イベントを指定できます。以下に例を示します。

```
hostname# debug eigrp ack build link
```

デバッグ出力は CPU プロセスで高プライオリティ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、Cisco TAC 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、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、**debug eigrp transmit** コマンドの出力例を示します。この例では、**network** コマンドの入力、および生成された送信イベント デバッグ メッセージが示されています。

```
hostname# debug eigrp transmit

EIGRP Transmission Events debugging is on

    (ACK, PACKETIZE, STARTUP, PEERDOWN, LINK, BUILD, STRANGE, SIA, DETAIL)

hostname# configure terminal
hostname(config)# router eigrp 100
hostname(config-router)# network 10.86.194.0 255.255.255.0

DNDB UPDATE 10.86.194.0 255.255.255.0, serno 0 to 1, refcount 0

hostname(config-router)# no debug eigrp transmit

EIGRP Transmission Events debugging is off
```

関連コマンド

コマンド	説明
show eigrp traffic	送受信された EIGRP パケットの数を表示します。

debug eigrp user-interface

EIGRP ユーザ イベントのデバッグ情報を表示するには、特権 EXEC モードで **debug eigrp user-interface** 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 eigrp user-interface

no debug eigrp user-interface

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
8.0(2)	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 プロセスで高プライオリティ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、Cisco TAC 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、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、**debug eigrp user-interface** コマンドの出力例を示します。管理者が EIGRP コンフィギュレーションから **passive-interface** コマンドを削除することで出力が生成されています。

```
hostname# debug eigrp user-interface

EIGRP UI Events debugging is on

hostname# configure terminal
hostname(config) router eigrp 100
hostname(config-router)# no passive-interface inside

CSB2AF: FOUND (AS=100, Name=, VRF=0, AFI=ipv4)

hostname(config-router)# no debug eigrp user-interface
```

```
EIGRP UI Events debugging is off
```

関連コマンド

コマンド	説明
router eigrp	EIGRP ルーティング プロセスをイネーブルにし、ルータ コンフィギュレーション モードを開始します。
show running-config eigrp	実行コンフィギュレーションの EIGRP コマンドを表示します。

debug entity

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

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
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 プロセスで高プライオリティ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。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、MIB のデバッグ メッセージをイネーブルにする例を示します。**show debug** コマンドにより、MIB のデバッグ メッセージがイネーブルになっていることが示されています。

```
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 eou

EAPoUDP イベントのロギングをイネーブルにして、NAC メッセージをデバッグするには、特権 EXEC モードで **debug eou** コマンドを使用します。EAPoUDP デバッグ メッセージのロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug eou {**all** | **eap** | **errors** | **events** | **packets** | **sm**}

no debug eou [**all** | **eap** | **errors** | **events** | **packets** | **sm**]

構文の説明

all	すべての EAPoUDP 情報に関するデバッグ メッセージのロギングをイネーブルします。
eap	EAPoUDP パケットに関するデバッグ メッセージのロギングをイネーブルにします。
errors	EAPoUDP パケット エラーのロギングをイネーブルにします。
events	EAPoUDP セッション イベントのロギングをイネーブルにします。
packets	EAPoUDP パケット情報に関するデバッグ メッセージのロギングをイネーブルにします。
sm	EAPoUDP ステート マシン情報に関するデバッグ メッセージのロギン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 モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、セキュリティ アプライアンスは、EAPoUDP セッション状態の変化およびタイマー イベントを記録し、16 進数形式で EAPoUDP ヘッダーとパケット コンテンツの完全レコードを生成します。

デバッグ出力には高いプライオリティが割り当てられるため、システムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、すべての EAPoUDP セッション イベントのロギングをイネーブルにする例を示します。

```
hostname# debug eou events
hostname#
```

次に、すべての EAPoUDP デバッグ メッセージのロギングをイネーブルにする例を示します。

```
hostname# debug eou all
hostname#
```

次に、すべての EAPoUDP デバッグ メッセージのロギングをディセーブルにする例を示します。

```
hostname# no debug eou
hostname#
```

関連コマンド

コマンド	説明
debug eap	EAP イベントのロギングをイネーブルにして、NAC メッセージをデバッグします。
debug nac	NAC イベントのロギングをイネーブルにします。
eou initialize	1 つ以上の NAC セッションに割り当てられているリソースを消去し、セッションごとに、新しい無条件のポスチャ確認を開始します。
eou revalidate	1 つ以上の NAC セッションの即時ポスチャ確認を強制実行します。
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 esmtp

SMTP/ESMTP アプリケーション インスペクションのデバッグ メッセージを表示するには、特権 EXEC モードで **debug esmtp** コマンドを使用します。SMTP/ESMTP アプリケーション インスペクションのデバッグ 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 esmtp [*level*]

no debug esmtp [*level*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
既存	このコマンドは既存です。

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。すべてのデバッグ メッセージの表示を停止するには、**no debug all** コマンドを入力します。

（注）　**debug esmtp** 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トラフィックが遅くなる可能性があります。

例

次に、SMTP/ESMTP アプリケーション インスペクションに対しデフォルト レベル（1）でデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug esmtp
```

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トラフィック クラスを定義します。

コマンド	説明
inspect esmtp	ESMTP アプリケーション インスペクションをイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上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 を含む各種接続タイプの接続状態を表示します。

debug fixup

アプリケーション インスペクション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です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
既存	このコマンドは既存です。

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 インスペクション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、イネーブルになっているすべてのデバッグ コマンドをオフにします。

例

次に、アプリケーション インスペクションに関する詳細情報の表示をイネーブルにする例を示します。

```
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トラフィック クラスを定義します。
inspect *protocol*	特定プロトコルについてアプリケーション インスペクションをイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。

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** | **cmd-exec** | **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**}

構文の説明

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。
cmd-exec	**failover exec** コマンドの実行トレース。
fail	フェールオーバーの内部例外。
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 ステータスのトレース。
open	フェールオーバー デバイスのオープン。
rx	フェールオーバー メッセージの受信。
rxdmp	フェールオーバー受信メッセージのダンプ（シリアル コンソールのみ）。
rxip	IP ネットワークのフェールオーバー パケットの受信。
switch	フェールオーバー スイッチング ステータス。
sync	フェールオーバーのコンフィギュレーションまたはコマンドのレプリケーション。
tx	フェールオーバー メッセージの送信。
txdmp	フェールオーバー送信メッセージのダンプ（シリアル コンソールのみ）。
txip	IP ネットワークのフェールオーバー パケットの送信。
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 モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.0(1)	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 プロセスで高プライオリティ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、Cisco TAC 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、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、**debug fover cmd-exec** コマンドの出力例を示します。デバッグをイネーブルにした後、**failover exec** コマンドを入力しています。デバッグ出力の後に、**failover exec** コマンドの結果が表示されています。

```
hostname(config)# debug fover cmd-exec

fover event trace on

hostname(config)# failover exec mate show running-config failover

ci/console: Sending cmd: show runn failovero to peer for execution, seq = 4
ci/console: frep_execv_cmd: replicating exec cmd: show runn failover...
fover_parse: Fover rexec response: seq=4, size=228, data="fail..."
ci/console: Fover rexec waiting at clock tick 2670960
fover_parse: Fover rexec ack: seq = 4, ret_val = 0
ci/console: Fover rexec conteinuer at clock tick: 2671040
ci/console: Fover exec succeeded, seq = 5

failover
failover lan interface failover GigabitEthernet0/3
failover polltime unit 1 holdtime 3
failover key *****
failover link failover GigabitEthernet0/3
failover interface ip failover 10.0.5.1 255.255.255.0 standby 10.0.5.2
ciscoasa(config)#
```

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および動作統計に関する情報を表示します。

debug fsm

FSM 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

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
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 プロセスで高プライオリティ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。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、FSM デバッグ メッセージをイネーブルにする例を示します。**show debug** コマンドにより、FSM デバッグ メッセージがイネーブルになっていることが示されています。

```
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 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 ftp client** コマンドを使用します。FTP のデバッグ 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*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
既存	このコマンドは既存です。

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。すべてのデバッグ メッセージの表示を停止するには、**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トラフィックが遅くなる可能性があります。

例

次に、FTP に対しデフォルト レベル（1）でデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug ftp client
```

関連コマンド

コマンド	説明
copy	イメージ ファイルや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。

コマンド	説明
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

各種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。各種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

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティ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。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、各種のデバッグ メッセージをイネーブルにする例を示します。**show debug** コマンドにより、各種のデバッグ メッセージがイネーブルになっていることが示されています。

```
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 インスペクション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**}

構文の説明

error	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	GTP イベントのデバッグ情報を表示します。
ha option	GTP HA イベントのデバッグ情報。
parser	GTP メッセージの解析に関するデバッグ情報を表示します。

デフォルト

デフォルトでは、すべてのオプションがイネーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

debug gtp コマンドは、GTP インスペクション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、イネーブルになっているすべてのデバッグ コマンドをオフにします。

（注） GTP インスペクションには、特別なライセンスが必要です。

例

次に、GTP インスペクションに関する詳細情報の表示をイネーブルにする例を示します。

```
hostname# debug gtp
```

関連コマンド

コマンド	説明
clear service-policy inspect gtp	グローバルな GTP 統計情報をクリアします。

コマンド	説明
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 インスペクションで使用する 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 GTP マップを表示します。

debug h323

H.323 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 h323** コマンドを使用します。H.323 のデバッグ 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]

構文の説明

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、アドミッション、およびステータス プロトコルを指定します。
asn	（任意）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	（任意）シグナリング イベントを表示します。または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 モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
既存	このコマンドは既存です。

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。すべてのデバッグ メッセージの表示を停止するには、**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トラフィックが遅くなる可能性があります。

例

次に、H.225 シグナリングに対しデフォルト レベル（1）でデバッグ メッセージをイネーブルにする例を示します。

```
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 インスペクションをイネーブルにします。
show h225	セキュリティ アプライアンスで確立されている 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によってセキュリティ アプライアンス間で確立された 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 アプライアンス間で確立された 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 制御接続が終了するまでのアイドル時間を設定します。

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*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルトは 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
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、イネーブルになっているすべてのデバッグ コマンドをオフにします。

例

次に、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する例を示します。

```
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 サーバにアクセスできる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 インスペクション マップのデバッグ メッセージを表示するには、特権 EXEC モードで **debug http-map** コマンドを使用します。HTTP アプリケーション インスペクションのデバッグ 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 モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

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。すべてのデバッグ メッセージの表示を停止するには、**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トラフィックが遅くなる可能性があります。

例

次に、HTTP アプリケーション インスペクションに対しデフォルト レベル（1）でデバッグ メッセージをイネーブルにする例を示します。

```
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 インスペクションに関する詳細情報を表示します。
http-map	拡張 HTTP インスペクションを設定するための HTTP マップを定義します。
inspect http	アプリケーション インスペクション用に特定の HTTP マップを適用します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。

debug icmp

ICMP インスペクション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*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。
trace	ICMP トレース アクティビティ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です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
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 インスペクション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、イネーブルになっているすべてのデバッグをオフにします。

例

次に、ICMP インスペクションに関する詳細情報の表示をイネーブルにする例を示します。

```
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クリアします。
icmp	セキュリティ アプライアンス インターフェイスで終了する ICMP トラフィックのアクセス ルールを設定します。
show conn	各種プロトコルおよびセッション タイプの、セキュリティ アプライアンスを通じた接続の状態を表示します。

コマンド	説明
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*]

構文の説明

group *group_id*	指定したグループの IGMP デバッグ情報を表示します。
interface *if_name*	指定し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 モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティ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。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

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ている受信者、および IGMP を通じて学習された受信者を含むマルチキャスト 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 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 ils** コマンドを使用します。ILS のデバッグ 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*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
既存	このコマンドは既存です。

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。すべてのデバッグ メッセージの表示を停止するには、**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トラフィックが遅くなる可能性があります。

例

次に、ILS アプリケーション インスペクションに対しデフォルト レベル（1）でデバッグ メッセージをイネーブルにする例を示します。

```
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 インスペクションをイネーブルにします。

コマンド	説明
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上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

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
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 プロセスで高プライオリティ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。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、Image Manager のデバッグ メッセージをイネーブルにする例を示します。**show debug** コマンドでは、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確認できます。

```
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 inspect tls-proxy

TLS プロキシ インスペクションのデバッグ メッセージを表示するには、特権 EXEC モードで **debug inspect tls-proxy** 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 inspect tls-proxy [**all** | **errors** | **events** | **packets**]

no debug inspect tls-proxy [**all** | **errors** | **events** | **packets**]

構文の説明

all	すべての TLS プロキシのデバッグを指定します。
errors	TLS プロキシ エラーのデバッグを指定します。
events	TLS プロキシ イベントのデバッグを指定します。
packets	TLS プロキシ パケットのデバッグを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
8.0(2)	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でトラフィックが遅くなる可能性があります。

例

次に、TLS プロキシのデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug inspect tls-proxy
```

関連コマンド

コマンド	説明
client	暗号スイートを定義し、ローカル ダイナミック証明書の発行者またはキーペアを設定します。
ctl-provider	CTL プロバイダー インスタンスを定義し、プロバイダー コンフィギュレーション モードを開始します。

コマンド	説明
show tls-proxy	TLS プロキシを表示します。
tls-proxy	TLS プロキシ インスタンスを定義し、最大セッション数を設定します。

debug ip eigrp

EIGRP プロトコル パケットのデバッグ情報を表示するには、特権 EXEC モードで **debug ip eigrp** 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 ip eigrp [*as-number*] [*ip-addr mask* | **neighbor** *nbr-addr* | **notifications** | **summary**]

no debug ip eigrp [*as-number*] [*ip-addr mask* | **neighbor** *nbr-addr* | **notifications** | **summary**]

構文の説明

as-number	（任意）イベント ログを表示している EIGRP プロセスの自律システム番号を指定します。セキュリティ アプライアンスがサポートする EIGRP ルーティング プロセスは 1 つだけであるため、自律システム番号を指定する必要はありません。
ip-addr mask	（任意）デバッグ出力を、IP アドレスおよびネットワーク マスクにより定義される範囲内のメッセージに制限します。
neighbor *nbr-addr*	（任意）デバッグ出力を、指定したネイバーに制限します。
notifications	（任意）デバッグ出力を、EIGRP プロトコル イベントおよび通知に制限します。
summary	（任意）デバッグ出力を集約ルート処理に制限します。
user-interface	（任意）デバッグ出力をユーザ イベントに制限します。

デフォルト

キーワードまたは引数を指定しない場合、IPv4 ASDM のデバッグ メッセージのみ表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
8.0(2)	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、インターフェイスで送受信されるパケットの分析に役立ちます。

デバッグ出力は CPU プロセスで高プライオリティ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、Cisco TAC 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、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、**debug ip eigrp** コマンドの出力例を示します。

```
hostname# debug ip eigrp

IP-EIGRP Route Events debugging is on

EIGRP-IPv4(Default-IP-Routing-Table:1): Processing incoming UPDATE packet
EIGRP-IPv4(Default-IP-Routing-Table:1): Ext 192.168.3.0 255.255.255.0 M 386560 - 256000
130560 SM 360960 - 256000 104960
EIGRP-IPv4(Default-IP-Routing-Table:1): Ext 192.168.0.0 255.255.255.0 M 386560 - 256000
130560 SM 360960 - 256000 104960
EIGRP-IPv4(Default-IP-Routing-Table:1): Ext 192.168.3.0 255.255.255.0 M 386560 - 256000
130560 SM 360960 - 256000 104960
EIGRP-IPv4(Default-IP-Routing-Table:1): 172.69.43.0 255.255.255.0, - do advertise out
Ethernet0/1
EIGRP-IPv4(Default-IP-Routing-Table:1): Ext 172.69.43.0 255.255.255.0 metric 371200 -
256000 115200
EIGRP-IPv4(Default-IP-Routing-Table:1): 192.135.246.0 255.255.255.0, - do advertise out
Ethernet0/1
EIGRP-IPv4(Default-IP-Routing-Table:1): Ext 192.135.246.0 255.255.255.0 metric 46310656 -
45714176 596480
EIGRP-IPv4(Default-IP-Routing-Table:1): 172.69.40.0 255.255.255.0, - do advertise out
Ethernet0/1
EIGRP-IPv4(Default-IP-Routing-Table:1): Ext 172.69.40.0 255.255.255.0 metric 2272256 -
1657856 614400
EIGRP-IPv4(Default-IP-Routing-Table:1): 192.135.245.0 255.255.255.0, - do advertise out
Ethernet0/1
EIGRP-IPv4(Default-IP-Routing-Table:1): Ext 192.135.245.0 255.255.255.0 metric 40622080 -
40000000 622080
EIGRP-IPv4(Default-IP-Routing-Table:1): 192.135.244.0 255.255.255.0, - do advertise out
Ethernet0/1
```

表 10-1 に、この出力で表示される重要なフィールドの説明を示します。

表 10-1　debug ip eigrp のフィールドの説明

フィールド	説明
IP-EIGRP:	IP EIGRP メッセージを示します。
Ext	後続のアドレスが内部ルートではなく外部ルートであることを示します。内部ルートには、Int というラベルが付加されます。
M	計算済みのメトリックを示します。計算済みのメトリックには、SM フィールドの値、および当該ルータとネイバーとの間のコストが含まれます。最初の数値は複合メトリックです。次の 2 つの数値はそれぞれ逆帯域幅および遅延です。
SM	ネイバーがレポートしたとおりのメトリックを表示します。

関連コマンド

コマンド	説明
debug eigrp packets	EIGRP パケットのデバッグ情報を表示します。

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

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
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 プロセスで高プライオリティ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。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、IPSec-over-TCP のデバッグ メッセージをイネーブルにする例を示します。**show debug** コマンドにより、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が示されています。

```
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 | mld | nd | packet | routing}

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

構文の説明

icmp	ICMPv6 ネイバー探索トランザクションを除く IPv6 ICMP トランザクションのデバッグ メッセージを表示します。
interface	IPv6 インターフェイスのデバッグ情報を表示します。
mld	Multicast Listener Discovery（MLD; マルチキャスト リスナー検出）のデバッグ メッセージを表示します。
nd	ICMPv6 ネイバー探索トランザクションのデバッグ メッセージを表示します。
packet	IPv6 パケットのデバッグ メッセージを表示します。
routing	IPv6 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 アップデートのデバッグ 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 モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティ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。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

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了する ICMP メッセージのアクセス ルールを定義します。
ipv6 address	1 つ以上の IPv6 アドレスを持つインターフェイスを設定します。
ipv6 nd dad attempts	重複アドレス検出時に実行するネイバー探索試行の回数を定義します。
ipv6 route	IPv6 ルーティング テーブル内にスタティック エントリを定義します。

debug iua-proxy

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

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
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 プロセスで高プライオリティ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。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、IUA プロキシのデバッグ メッセージをイネーブルにする例を示します。**show debug** コマンドにより、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が示されています。

```
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

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
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 プロセスで高プライオリティ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。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、Kerberos のデバッグ メッセージをイネーブルにする例を示します。**show debug** コマンドにより、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が示されています。

```
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 l2tp

L2TP のデバッグ情報を表示するには、特権 EXEC モードで **debug l2tp** 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 l2tp {**data** | **error** | **event** | **packet**} *level*

no debug l2tp {**data** | **error** | **event** | **packet**} *level*

構文の説明

data	データ パケットのトレース情報を表示します。
error	エラー イベントを表示します。
event	L2TP 接続イベントを表示します。
packet	パケット トレース情報を表示します。
level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティ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。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、接続イベントに関する L2TP デバッグ メッセージをイネーブルにする例を示します。**show debug** コマンドにより、L2TP デバッグ メッセージがイネーブルになっていることが示されています。

```
hostname# debug l2tp event 1
hostname# show debug
debug l2tp event 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

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティ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。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、LDAP のデバッグ メッセージをイネーブルにする例を示します。**show debug** コマンドにより、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が示されています。

```
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 mac-address-table** コマンドを使用します。MAC アドレス テーブルのデバッグ 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*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

デフォルトの level は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

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

例

次に、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する例を示します。

```
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。

コマンド	説明
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、Cisco TAC の指導の下でのみ使用する必要があります。

構文の説明

このコマンドは、Cisco TAC の指示の元でのみ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 モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
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 プロセスで高プライオリティ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、Cisco TAC 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、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

このコマンドは、Cisco TAC の指示の元でのみ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*]

構文の説明

db	（任意）ルート データベースの動作に関するデバッグ情報を表示します。
group	（任意）マルチキャスト グループの IP アドレスです。
init	（任意）システム初期化アクティビティを表示します。
mrib	（任意）MFIB との通信のデバッグ情報を表示します。
pak	（任意）パケット転送動作のデバッグ情報を表示します。
ps	（任意）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	（任意）ルーティング プロトコルに対する 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 モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティ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。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、MFIB データベース動作のデバッグ情報を表示する例を示します。

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

関連コマンド

コマンド	説明
show mfib	MFIB 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 インスペクション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**}

messages	MGCP メッセージに関するデバッグ情報を表示します。
parser	MGCP メッセージの解析に関する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です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

debug mgcp コマンドは、mgcp インスペクション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、イネーブルになっているすべてのデバッグをオフにします。

例

次に、MGCP アプリケーション インスペクションに関する詳細情報の表示をイネーブルにする例を示します。

```
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 インスペクション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。

コマンド	説明
show mgcp	セキュリティ アプライアンスを通じて確立された 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 mmp

MMP イベントのインスペクションを表示するには、特権 EXEC モードで **debug mmp** コマンドを使用します。MMP イベントのインスペクション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 mmp

no debug mmp

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
8.0(4)	このコマンドが追加されました。

例

次に、MMP イベントのインスペクションを表示する **debug mmp** コマンドの使用例を示します。

```
hostname# debug mmp
ciscoasa5520-tfw-cuma/admin(config-pmap)# MMP:: received 28 bytes from outside:1
72.23.62.204/2494 to inside:10.0.0.42/5443
MMP:: version OLWP-2.0
MMP status: 0
MMP:: forward 28/28 bytes from outside:172.23.62.204/2494 to inside:10.0.0.42/5443
MMP:: received 85 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2494
MMP:: version OLWP-2.0
MMP:: session-id: 41A3D410-8B10-4DEB-B15C-B2B4B0D22055
MMP status: 201
MMP:: forward 85/85 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2494
MMP:: received 265 bytes from outside:172.23.62.204/2494 to inside:10.0.0.42/5443
MMP:: content-length: 196
MMP:: content-type: text/oml21+wbxml
MMP:: processing entity body 200/196
MMP:: forward 265/265 bytes from outside:172.23.62.204/2494 to inside:10.0.0.42/5443
MMP:: received 267 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2494
MMP:: content-length: 198
MMP:: content-type: text/oml21+wbxml
MMP:: processing entity body 202/198
MMP:: forward 267/267 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2494
MMP:: received 135 bytes from outside:172.23.62.204/2494 to inside:10.0.0.42/5443
MMP:: content-length: 67
```

```
MMP:: content-type: text/oml21+wbxml
MMP:: processing entity body 71/67
MMP:: forward 135/135 bytes from outside:172.23.62.204/2494 to inside:10.0.0.42/5443
MMP:: received 100 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2442
MMP:: content-length: 32
MMP:: content-type: text/oml21+wbxml
MMP:: processing entity body 36/32
MMP:: forward 100/100 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2442
MMP:: received 130 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2494
MMP:: content-length: 62
MMP:: content-type: text/oml21+wbxml
MMP:: processing entity body 66/62
MMP:: forward 130/130 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2494
MMP:: received 220 bytes from outside:172.23.62.204/2494 to inside:10.0.0.42/5443
MMP:: content-length: 151
MMP:: content-type: text/oml21+wbxml
MMP:: processing entity body 155/151
MMP:: forward 220/220 bytes from outside:172.23.62.204/2494 to inside:10.0.0.42/5443
MMP:: received 130 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2494
MMP:: content-length: 62
MMP:: content-type: text/oml21+wbxml
MMP:: processing entity body 66/62
MMP:: forward 130/130 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2494
```

関連コマンド

コマンド	説明
inspect mmp	MMP インスペクション エンジンを設定します。
show debug mmp	MMP インスペクション モジュールの現在のデバッグ設定を表示します。
show mmp	既存の MMP セッションに関する情報を表示します。

debug module-boot

SSM ブート 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 ブート プロセスのデバッグ 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*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

デフォルトの level は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

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

例

次に、SSM ブート プロセスのデバッグ メッセージをイネーブルにする例を示します。

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

関連コマンド

コマンド	説明
hw-module module recover	リカバリ イメージを TFTP サーバからロードして、インテリジェント SSM を回復します。
hw-module module reset	SSM をシャットダウンし、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。

コマンド	説明
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準備をして、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**}

構文の説明

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	指定したグループの 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 モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティ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。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、MRIB I/O イベントのデバッグをイネーブルにする方法の例を示します。

```
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 nac

NAC フレームワーク イベントのロギングをイネーブルにするには、特権 EXEC モードで **debug nac** コマンドを使用します。NAC デバッグ メッセージのロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug nac {**all | auth | errors** | **events**}

no debug nac {**all | auth | errors** | **events**}

構文の説明

all	すべての NAC 情報に関するデバッグ メッセージのロギングをイネーブルにします。
auth	NAC 認証の要求および応答に関するデバッグ メッセージのロギングをイネーブルにします。
errors	NAC セッション エラーのロギングをイネーブルにします。
events	NAC セッション イベントのロギン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 モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、セキュリティ アプライアンスは、初期化、例外リスト一致、ACS トランザクション、クライアントレス認証、デフォルト ACL アプリケーション、および再検証の各タイプの NAC イベントをログに記録します。

デバッグ出力には高いプライオリティが割り当てられるため、システムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、すべての NAC セッション イベントのロギングをイネーブルにする例を示します。

```
hostname# debug nac events
hostname#
```

次に、すべての NAC デバッグ メッセージのロギングをイネーブルにする例を示します。

```
hostname# debug nac all
hostname#
```

次に、すべての NAC デバッグ メッセージのロギングをディセーブルにする例を示します。

```
hostname# no debug nac
hostname#
```

関連コマンド

コマンド	説明
debug eap	NAC フレームワーク メッセージのデバッグのための拡張認証プロトコル イベントのロギングをイネーブルにします。
debug eou	EAP over UDP イベントのロギングをイネーブルにして、NAC フレームワーク メッセージをデバッグします。
show vpn-session_summary.db	IPSec、WebVPN、および NAC セッションの数を表示します。
show vpn-session.db	NAC の結果を含む、VPN セッションの情報を表示します。

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

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティ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。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、NT ドメインのデバッグ メッセージをイネーブルにする例を示します。**show debug** コマンドにより、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が示されています。

```
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 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 ntp** コマンドを使用します。NTP のデバッグ 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**}

構文の説明

adjust	NTP クロックの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 クロックの選択に関するメッセージを表示します。
sync	NTP クロックの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 モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
既存	このコマンドは既存です。

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でトラフィックが遅くなる可能性があります。

例

次に、NTP のデバッグ メッセージをイネーブルにする例を示します。

```
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 プロセスに関する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。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 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**]

構文の説明

adj	（任意）OSPF 隣接イベントのデバッグをイネーブルにします。
database-timer	（任意）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	（任意）OSPF イベントのデバッグをイネーブルにします。
external	（任意）SPF デバッグを外部イベントに制限します。
flood	（任意）OSPF フラッディングのデバッグをイネーブルにします。
inter	（任意）SPF デバッグをエリア間イベントに制限します。
intra	（任意）SPF デバッグをエリア内イベントに制限します。
lsa-generation	（任意）OSPF サマリー LSA 生成のデバッグをイネーブルにします。
packet	（任意）受信済みの OSPF パケットのデバッグをイネーブルにします。
retransmission	（任意）OSPF 再送信イベントのデバッグをイネーブルにします。
spf	（任意）OSPF の最短パス優先計算のデバッグをイネーブルにします。**external**、**inter**、および **intra** キーワードを使用することで、SPF デバッグ情報を制限できます。
tree	（任意）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

キーワードを指定しないと、すべての OSPF デバッグ情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティ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。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

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

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティ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。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、CLI パーサーのデバッグ メッセージをイネーブルにする例を示します。**show debug** コマンドにより、現在のデバッグ コンフィギュレーションが示されています。**show debug** コマンドの出力の前後に、CLI パーサーのデバッグ メッセージが表示されています。

```
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 phone-proxy

電話プロキシ インスタンスのデバッグ メッセージを表示するには、特権 EXEC モードで **debug phone-proxy** コマンドを使用します。電話プロキシ 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 phone-proxy [<**media** | **signaling** | **tftp**> [**errors** | **events**]]

no debug phone-proxy [<**media** | **signaling** | **tftp**> [**errors** | **events**]]

構文の説明

errors	（任意）電話プロキシ エラーのデバッグ メッセージを表示します。
events	（任意）電話プロキシ イベントのデバッグ メッセージを表示します。
media	（任意）SIP インスペクションおよび Skinny インスペクションのメディア セッションのデバッグ メッセージを表示します。
signaling	（任意）SIP インスペクションおよび Skinny インスペクションのシグナリング セッションのデバッグ メッセージを表示します。
tftp	（任意）CTL ファイルの作成、コンフィギュレーション ファイルの解析など、TFTP インスペクションのデバッグ メッセージを表示します。

デフォルト

debug phone-proxy コマンドでオプションを指定しない場合、すべての電話プロキシ デバッグ メッセージが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
8.0(4)	このコマンドが追加されました。

使用上のガイドライン

debug phone-proxy コマンドは、電話プロキシ アクティビティに関する詳細情報を表示します。**no debug phone-proxy** コマンドは、イネーブルになっているすべてのデバッグをオフにします。

例

次に、**debug phone-proxy** コマンドを使用して、電話プロキシのコンフィギュレーション ファイル要求に関する成功 TFTP トランザクションを表示する例を示します。

```
hostname(config)# debug phone-proxy tftp
PP: 98.208.49.30/1028 requesting SEP00070E364804.cnf.xml.sgn
PP: opened 0x33952aa2
PP: Received data from 192.168.200.101 to outside:98.208.49.30/1028
        Received Block 1
PP: Acked Block #1 from 98.208.49.30/1028 to 192.168.200.101/39514
```

```
          .... [snip].....
PP: Received data from 192.168.200.101 to outside:98.208.49.30/1028
       Received Block 10
PP: Acked Block #10 from 98.208.49.30/1028 to 192.168.200.101/39514
PP: Installed application redirect rule from 98.208.49.30 to 192.168.200.101 using
redirect port 2000 and secure port 2443
PP: Modifying to TLS as the transport layer protocol.
PP: Modifying to encrypted mode.
PP: Data Block 1 forwarded from 192.168.200.101/39514 to 98.208.49.30/1028
PP: Received ACK Block 1 from outside:98.208.49.30/1028 to inside:192.168.200.101
          ..... [snip] ....
PP: Data Block 11 forwarded to 98.208.49.30/1028
PP: Received ACK Block 11 from outside:98.208.49.30/1028 to inside:192.168.200.101
PP: TFTP session complete, all data sent
```

関連コマンド

コマンド	説明
phone-proxy	Phone Proxy インスタンスを設定します。
show running-config phone-proxy	Phone Proxy 固有の情報を表示します。

debug pim

PI M 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**]

構文の説明

df-election	（任意）PIM 双方向 DF 選出メッセージ処理のデバッグ メッセージを表示します。
group *group*	（任意）指定したグループのデバッグ情報を表示します。*group* には、値として次のいずれかを指定できます。 • 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、**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 分割ドット付き 10 進表記のマルチキャスト IP アドレスです。
interface *if_name*	（任意）**df-election** キーワードを指定してこのコマンドを使用すると、DF 選出のデバッグ表示が、指定したインターフェイスの情報に制限されます。 **df-election** キーワードを指定せずにこのコマンドを使用すると、指定したインターフェイスの PIM エラー メッセージが表示されます。 **（注）** **debug pim interface** コマンドでは、PIM プロトコル アクティビティ メッセージは表示されず、エラー メッセージのみ表示されます。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** キーワードを指定せずに **debug pim** コマンドを使用します。**group** キーワードを使用することで、指定したマルチキャスト グループに表示を制限できます。
neighbor	（任意）送受信された PIM hello メッセージのみ表示します。
rp *rp*	（任意）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 分割ドット付き 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 モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

送受信された PIM パケットおよび PIM 関連のイベントをログに記録します。

デバッグ出力は CPU プロセスで高プライオリティ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。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

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	グループ対プロトコルのマッピング テーブルを表示します。
show pim interface	PIM のインターフェイス固有情報を表示します。
show pim neighbor	PIM ネイバー テーブル内のエントリを表示します。

debug pix acl

PIX ACL 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 pix acl** 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 acl

no debug pix acl

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティ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、Cisco TAC 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、debug コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、debug コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、デバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug pix acl
```

関連コマンド

コマンド	説明
debug pix process	xlate および 2 番めの接続処理のデバッグ 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 cls

PIX CLS 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 pix cls** 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 cls

no debug pix cls

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティ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、Cisco TAC 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、debug コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、debug コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、デバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug pix cls
```

関連コマンド

コマンド	説明
debug pix process	xlate および 2 番めの接続処理のデバッグ 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 pkt2pc

uauth コードに送信されるパケットをトレースするデバッグ メッセージ、および uauth プロキシ セッションがデータ パスにカットスルーされる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

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
既存	このコマンドは既存です。

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でトラフィックが遅くなる可能性があります。

例

次に、uauth コードに送信されるパケットをトレースするデバッグ メッセージ、および uauth プロキシ セッションがデータ パスにカットスルーされる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する例を示します。

```
hostname# debug pix pkt2pc
```

関連コマンド

コマンド	説明
debug pix process	xlate および 2 番めの接続処理のデバッグ 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 2 番めの接続処理のデバッグ メッセージを表示するには、特権 EXEC モードで **debug 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

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
既存	このコマンドは既存です。

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でトラフィックが遅くなる可能性があります。

例

次に、xlate および 2 番めの接続処理のデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug pix process
```

関連コマンド

コマンド	説明
debug pix pkt2pc	uauth コードに送信されるパケットをトレースするデバッグ メッセージ、および uauth プロキシ セッションがデータ パスにカットスルーされる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 pix uauth

pix uauth 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 pix uauth** 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 uauth

no debug pix uauth

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティ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、Cisco TAC 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、debug コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、debug コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、デバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug pix uauth
```

関連コマンド

コマンド	説明
debug pix process	xlate および 2 番めの接続処理のデバッグ 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 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 pptp** コマンドを使用します。PPTP のデバッグ 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*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
既存	このコマンドは既存です。

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。すべてのデバッグ メッセージの表示を停止するには、**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トラフィックが遅くなる可能性があります。

例

次に、PPTP アプリケーション インスペクションに対しデフォルト レベル（1）でデバッグ メッセージをイネーブルにする例を示します。

```
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 インスペクションをイネーブルにします。

コマンド	説明
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上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 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 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

構文の説明

all	（任意）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（デコードされた RADIUS メッセージを含む）を表示します。
decode	（任意）RADIUS メッセージのデコードされた内容を表示します。16 進数形式の値、およびこれらの値の、人が判読できるデコード済みバージョンを含む、すべての RADIUS パケットの内容が表示されます。
session	（任意）セッション関連の RADIUS メッセージを表示します。送受信された RADIUS メッセージのパケット タイプは表示されますが、パケットの内容は表示されません。
user	（任意）特定ユーザの RADIUS デバッグ メッセージを表示します。
username	表示するメッセージの所有者であるユーザを指定します。**user** キーワードを指定した場合に限り有効です。

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 モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
既存	このコマンドは既存です。

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 サーバとの間の RADIUS メッセージング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、イネーブルになっているすべてのデバッグをオフにします。

例

次に、デコードされた RADIUS メッセージの例を示します。この RADIUS メッセージ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                                   |  1.1.1.10
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コンフィギュレーションを表示します。

debug redundant-interface

冗長インターフェイ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 redundant-interface** コマンドを使用します。冗長インターフェイスのデバッグ 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 redundant-interface [*level*]

no debug redundant-interfac [*level*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

デフォルトの level は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
8.0(2)	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でトラフィックが遅くなる可能性があります。

例

次に、冗長インターフェイスのデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug redundant-interface
```

関連コマンド

コマンド	説明
interface redundant	冗長インターフェイスを作成します。
member-interface	物理インターフェイスを冗長インターフェイスに割り当てます。
redundant-interface	冗長インターフェイス ペア内のアクティブ インターフェイスを変更します。
show debug	イネーブルなデバッガをすべて表示します。

debug 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 [**database** | **events**]

no debug rip [**database** | **events**]

構文の説明

database	RIP データベース イベントを表示します。
events	RIP 処理イベントを表示します。

デフォルト

すべての RIP イベントがデバッグ出力に表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
既存	このコマンドは既存です。
7.2(1)	**database** キーワードと **events** キーワードが追加されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティ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、Cisco TAC 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、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、**debug rip** コマンドの出力例を示します。

```
hostname# debug rip

RIP: broadcasting general request on GigabitEthernet0/1
RIP: broadcasting general request on GigabitEthernet0/2
RIP: Received update from 10.89.80.28 on GigabitEthernet0/1
    10.89.95.0 in 1 hops
    10.89.81.0 in 1 hops
    10.89.66.0 in 2 hops
    172.31.0.0 in 16 hops (inaccessible)
    0.0.0.0 in 7 hops
RIP: Sending update to 255.255.255.255 via GigabitEthernet0/1 (10.89.64.31)
```

```
    subnet 10.89.94.0, metric 1
    172.31.0.0 in 16 hops (inaccessible)
RIP: Sending update to 255.255.255.255 via GigabitEthernet0/2 (10.89.94.31)
    subnet 10.89.64.0, metric 1
    subnet 10.89.66.0, metric 3
    172.31.0.0 in 16 hops (inaccessible)
    default 0.0.0.0, metric 8
RIP: bad version 128 from 192.168.80.43
```

関連コマンド

コマンド	説明
router rip	RIP プロセスを設定します。
show running-config rip	実行コンフィギュレーションの RIP コマンドを表示します。

debug rtp

H.323 および SIP インスペクションに関連する RTP パケットの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 rtp** 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 rtp [*level*]

no debug rtp [*level*]

構文の説明

level	（任意）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 *level* は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティ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。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、**debug rtp** コマンドを使用して RTP パケットのデバッグをイネーブルにする例を示します。

```
hostname# debug rtp 255
debug rtp  enabled at level 255
```

関連コマンド

コマンド	説明
policy-map	レイヤ 3/4 のポリシー マップを作成します。

コマンド	説明
rtp-conformance	H.323 および SIP のプロトコル適合のために、ピンホールをフローする RTP パケットをチェックします。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

debug rtsp

RTSP アプリケーション インスペクションのデバッグ メッセージを表示するには、特権 EXEC モードで **debug rtsp** コマンドを使用します。RTSP アプリケーション インスペクションのデバッグ 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*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
既存	このコマンドは既存です。

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。すべてのデバッグ メッセージの表示を停止するには、**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トラフィックが遅くなる可能性があります。

例

次に、RTSP アプリケーション インスペクションに対しデフォルト レベル（1）でデバッグ メッセージをイネーブルにする例を示します。

```
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 インスペクションをイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上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

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティ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。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、SDI デバッグ メッセージをイネーブルにする例を示します。**show debug** コマンドにより、SDI デバッグ メッセージがイネーブルになっていることが示されています。

```
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 メッセージの先頭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

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

デフォルトの設定は次のとおりです。

- デバッグ メッセージのシーケンス番号はディセーブルです。
- *level* のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティ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。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、デバッグ メッセージのシーケンス番号をイネーブルにする例を示します。**debug parser cache** コマンドは、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** コマンドにより、現在のデバッグ コンフィギュレーションが示されています。表示されている CLI パーサーのデバッグ メッセージでは、各メッセージの前にシーケンス番号が追加されています。

```
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 とのセッションのデバッグ メッセージを表示するには、特権 EXEC モードで **debug session-command** コマンドを使用します。セッションのデバッグ 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*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

デフォルトの level は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

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

例

次に、セッションのデバッグ メッセージをイネーブルにする例を示します。

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

関連コマンド

コマンド	説明
session	SSM とのセッション。

debug sip

SIP アプリケーション インスペクションのデバッグ メッセージを表示するには、特権 EXEC モードで **debug sip** コマンドを使用します。SIP アプリケーション インスペクションのデバッグ 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 [**ha**]

no debug sip [**ha**]

構文の説明

ha	（任意）SIP ステートフル フェールオーバー メッセージを表示します。 アクティブ ユニットに対する **debug sip** コマンドでこのキーワードを使用すると、SIP 状態情報がスタンバイ ユニットに送信されるときにデバッグ メッセージが表示されます。スタンバイ ユニットに対する **debug sip** コマンドでこのキーワードを使用すると、アクティブ ユニットから状態更新が受信されるときにデバッグ メッセージが表示されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
既存	このコマンドは既存です。
8.0(2)	**ha** キーワードが追加されました。

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。すべてのデバッグ メッセージの表示を停止するには、**no debug all** コマンドを入力します。

デバッグ出力は CPU プロセスで高プライオリティ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、Cisco TAC 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、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、アクティブ ユニットまたはフェールオーバー ペア内のフェールオーバー グループに対して実行した **debug sip** コマンドの出力例を示します。

```
hostname# debug sip ha
SIP HA:    Sending    update SESSION message from faddr 10.132.80.120/5060 laddr
10.130.80.4/50295 Call-id: 001201e8-8a36000d-196df7f1-17cfef14@10.130.80.4 From:
sip:1004@10.132.80.120:001201e88a3600124a7fad61-640406c0 To: sip:1009@10.132.80.120:
State:1

SIP HA:    msg sent to peer successful  Version: 1 Action: update Object: session

SIP HA:    Sending    update TX message from faddr 10.132.80.120/5060laddr
10.130.80.4/50295CSeq 101 INVITEState Transaction Calling
```

次に、スタンバイ ユニットまたはフェールオーバー ペア内のフェールオーバー グループに対して実行した **debug sip** コマンドの出力例を示します。

```
hostname# debug sip ha
SIP HA:    Message    received from peer, Version: 1 Action: add Object: session

SIP HA:    Created    SIP session for faddr 10.132.80.120/5060 laddr 10.130.80.4/50295
Call-id: 001201e8-8a36000d-196df7f1-17cfef14@10.130.80.4 From:
sip:1004@10.132.80.120:001201e88a3600124a7fad61-640406c0 To: sip:1009@10.132.80.120: 1
total

SIP HA:    Message    received from peer, Version: 1 Action: add Object: tx

SIP HA:    Found an existing session faddr 10.132.80.120/5060 laddr 10.130.80.4/50295
Call-id: 001201e8-8a36000d-196df7f1-17cfef14@10.130.80.4 From:
sip:1004@10.132.80.120:001201e88a3600124a7fad61-640406c0 To: sip:1009@10.132.80.120:

SIP HA:    Created    SIP Transaction    for faddr 10.132.80.120/5060 to   laddr
10.130.80.4/50295CSeq 101 INVITEState Transaction Calling
```

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 インスペクション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 アプライアンスを通じて確立された 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 インスペクションのデバッグ メッセージを表示するには、特権 EXEC モードで **debug skinny** コマンドを使用します。SCCP アプリケーション インスペクションのデバッグ 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*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
既存	このコマンドは既存です。

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。すべてのデバッグ メッセージの表示を停止するには、**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トラフィックが遅くなる可能性があります。

例

次に、SCCP アプリケーション インスペクションに対しデフォルト レベル（1）でデバッグ メッセージをイネーブルにする例を示します。

```
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 インスペクションをイネーブルにします。
show skinny	セキュリティ アプライアンスを通じて確立された 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 sla monitor

SLA モニタ動作のデバッグ メッセージを表示するには、特権 EXEC モードで **debug sla monitor** 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 sla monitor [**error** | **trace**] [*sla-id*]

no debug sla monitor [*sla-id*]

構文の説明

error	（任意）IP SLA モニタのエラー メッセージを出力します。
sla-id	（任意）デバッグする SLA の ID。
trace	（任意）IP SLA モニタのトレース メッセージを出力します。

デフォルト

デフォルトでは、エラー メッセージとトレース メッセージの両方が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

同時にデバッグできる SLA 動作は 32 個のみです。

デバッグ出力は CPU プロセスで高プライオリティ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、Cisco TAC 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、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、SLA 動作のエラー デバッグをイネーブルにする例を示します。

```
hostname(config)# debug sla monitor error
```

次に、指定した SLA 動作に関する SLA 動作トレース メッセージを表示する例を示します。

```
hostname(config)# debug sla monitor trace 123
```

関連コマンド

コマンド	説明
clear configure route	スタティックに設定された **route** コマンドを削除します。
clear route	RIP などのダイナミック ルーティング プロトコルを通じて学習されたルートを削除します。
show route	ルート情報を表示します。
show running-config route	設定されているルートを表示します。

debug sqlnet

SQL*Net アプリケーション インスペクションのデバッグ メッセージを表示するには、特権 EXEC モードで **debug sqlnet** コマンドを使用します。SQL*Net アプリケーション インスペクションのデバッグ 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*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
既存	このコマンドは既存です。

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。すべてのデバッグ メッセージの表示を停止するには、**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トラフィックが遅くなる可能性があります。

例

次に、SQL*Net アプリケーション インスペクションに対しデフォルト レベル（1）でデバッグ メッセージをイネーブルにする例を示します。

```
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 インスペクションをイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上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*]

構文の説明

level	（任意）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 *level* は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティ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。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

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 コマンドをクリアします。
show running-config ssh	実行コンフィギュレーションの現在の SSH コマンドを表示します。
show ssh sessions	セキュリティ アプライアンスとのアクティブ 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 sunrpc

RPC アプリケーション インスペクションのデバッグ メッセージを表示するには、特権 EXEC モードで **debug sunrpc** コマンドを使用します。RPC アプリケーション インスペクションのデバッグ 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*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
既存	このコマンドは既存です。

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。すべてのデバッグ メッセージの表示を停止するには、**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トラフィックが遅くなる可能性があります。

例

次に、RPC アプリケーション インスペクションに対しデフォルト レベル（1）でデバッグ メッセージをイネーブルにする例を示します。

```
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 インスペクションをイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
show conn	RPC を含む各種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 switch ilpm

組み込みスイッチ（ASA 5505 適応型セキュリティ アプライアンスなど）を使用するモデル、または PoE 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 switch ilpm** コマンドを使用します。PoE のデバッグ 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 switch ilpm [**events** | **errors**] [*level*]

no debug switch ilpm [**events** | **errors**] [*level*]

構文の説明

errors	（任意）エラーがある場合にトラブルシューティング情報を表示します。
events	（任意）PoE イベントを表示します。
level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

デフォルトでは、キーワードを指定しない場合、イベントとエラーの両方が表示されます。デフォルトの level は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

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

例

次に、PoE ポートのデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug switch ilpm
```

関連コマンド

コマンド	説明
interface vlan	VLAN インターフェイスを追加します。

コマンド	説明
debug switch manager	VLAN 割り当ておよび **switchport** コマンドが原因のイベントおよびエラーに関するデバッグ 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 switch manager

組み込みスイッチ（ASA 5505 適応型セキュリティ アプライアンスなど）を使用するスイッチ ポート モデル、VLAN 割り当て、および **switchport** コマンドが原因のイベントおよびエラーに関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug switch manager** コマンドを使用します。スイッチ ポー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 switch manager [**events** | **errors**] [*level*]

no debug switch manager [**events** | **errors**] [*level*]

構文の説明

errors	（任意）エラーがある場合にトラブルシューティング情報を表示します。
events	（任意）スイッチ マネージャ イベントを表示します。
level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

デフォルトでは、キーワードを指定しない場合、イベントとエラーの両方が表示されます。デフォルトの level は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

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

例

次に、スイッチ ポートのデバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug switch manager
```

関連コマンド

コマンド	説明
interface vlan	VLAN インターフェイスを追加します。

コマンド	説明
debug switch ilpm	PoE のデバッグ 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 tacacs

TACACS+ 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 tacacs** コマンドを使用します。TACACS+ 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 tacacs [**session** | **user** *username*]

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

構文の説明

session	セッション関連の TACACS+ のデバッグ メッセージを表示します。
user	ユーザ固有の TACACS+ のデバッグ メッセージを表示します。一度に 1 人のユーザのみの TACACS+ デバッグ メッセージを表示できます。
username	表示する TACACS+ デバッグ メッセージの所有者であ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 モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティ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。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、TACACS+ デバッグ メッセージをイネーブルにする例を示します。**show debug** コマンドにより、TACACS+ デバッグ メッセージがイネーブルになっていることが示されています。

```
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 インスペクション マップのデバッグ メッセージを表示するには、特権 EXEC モードで **debug tcp-map** コマンドを使用します。TCP アプリケーション インスペクションのデバッグ 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

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティ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、Cisco TAC 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、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、TCP アプリケーション インスペクション マップのデバッグ メッセージをイネーブルにする例を示します。**show debug** コマンドにより、TCP アプリケーション インスペクション 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が示されています。

```
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 メッセージの先頭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

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

デフォルトの設定は次のとおりです。

- 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 モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティ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、Cisco TAC 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、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、デバッグ メッセージのタイムスタンプをイネーブルにする例を示します。**debug parser cache** コマンドは、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** コマンドにより、現在のデバッグ コンフィギュレーションが示されています。表示されている CLI パーサーのデバッグ メッセージでは、各メッセージの前にタイムスタンプが追加されています。

```
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 vpn-sessiondb [*level*]

no debug vpn-sessiondb

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティ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、Cisco TAC 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、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、VPN セッション データベースのこデバッグ メッセージをイネーブルにする例を示します。**show debug** コマンドにより、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が示されています。

```
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 wccp

WCCP イベントのロギングをイネーブルにするには、特権 EXEC モードで **debug wccp** コマンドを使用します。WCCP デバッグ メッセージのロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug wccp {**events | packets | subblocks**}

no debug wccp {**events | packets | subblocks**}

構文の説明

events	WCCP セッション イベントのロギングをイネーブルにします。
packets	WCCP パケット情報に関するデバッグ メッセージのロギングをイネーブルにします。
subblocks	WCCP サブブロックに関するデバッグ メッセージのロギン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 モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力には高いプライオリティが割り当てられるため、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、Cisco TAC 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、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、すべての WCCP セッション イベントのロギングをイネーブルにする例を示します。

```
hostname# debug wccp events
hostname#
```

次に、WCCP パケットのデバッグ メッセージのロギングをイネーブルにする例を示します。

```
hostname# debug wccp packets
hostname#
```

次に、WCCP デバッグ メッセージのロギングをディセーブルにする例を示します。

```
hostname# no debug wccp
hostname#
```

関連コマンド

コマンド	説明
wccp	WCCP のサポートをイネーブルにします。
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 webvpn

WebVPN のデバッグ メッセージをログに記録するには、特権 EXEC モードで **debug webvpn** コマンドを使用します。WebVPN のデバッグ メッセージのロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug webvpn [**chunk** | **cifs** | **citrix** | **failover** | **html** | **javascript** | **request** | **response** | **svc** | **transformation** | **url** | **util** | **xml**] [*level*]

no debug webvpn [**chunk** | **cifs** | **citrix** | **failover** | **html** | **javascript** | **request** | **response** | **svc** | **transformation** | **url** | **util** | **xml**] [*level*]

構文の説明

chunk	WebVPN 接続をサポートするために使用されるメモリ ブロックに関するデバッグ メッセージを表示します。
cifs	CIFS サーバと WebVPN ユーザの間の接続に関するデバッグ メッセージを表示します。
citrix	WebVPN を介した Citrix Metaframe サーバと Citrix ICA クライアントの間の接続に関するデバッグ メッセージを表示します。
failover	WebVPN 接続に影響する装置フェールオーバーに関するデバッグ メッセージを表示します。
html	WebVPN 接続を介して送信される HTML ページに関するデバッグ メッセージを表示します。
javascript	WebVPN 接続で送信された JavaScript に関するデバッグ メッセージを表示します。
request	WebVPN 接続を介して発行された要求に関するデバッグ メッセージを表示します。
response	WebVPN 接続を介して発行された応答に関するデバッグ メッセージを表示します。
svc	WebVPN を介した SSL VPN クライアントへの接続に関するデバッグ メッセージを表示します。
transformation	WebVPN コンテンツ変換に関するデバッグ メッセージを表示します。
url	WebVPN 接続を介して発行された Web サイト要求に関するデバッグ メッセージを表示します。
util	WebVPN リモート ユーザへの接続のサポートのために占有される CPU 使用率に関するデバッグ メッセージを表示します。
xml	WebVPN 接続で送信された JavaScript に関するデバッグ メッセージを表示します。
level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力には高いプライオリティが割り当てられるため、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、Cisco TAC 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、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

次に、CIFS に関する WebVPN デバッグ メッセージをイネーブルにする例を示します。**show debug** コマンドにより、CIFS のデバッグ メッセージがイネーブルになっていることが示されています。

```
hostname# debug webvpn cifs
INFO: debug webvpn cifs enabled at level 1.
hostname# show debug
debug webvpn cifs 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 インスペクションのデバッグ メッセージを表示するには、特権 EXEC モードで **debug xdmcp** コマンドを使用します。XDMCP アプリケーション インスペクションのデバッグ 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*]

構文の説明

level	（任意）表示するデバッグ メッセージのレベルを 1 ～ 255 で設定します。デフォルトは 1 です。より高いレベルの追加メッセージを表示する場合は、このレベルにより大きな数字を設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
既存	このコマンドは既存です。

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。すべてのデバッグ メッセージの表示を停止するには、**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トラフィックが遅くなる可能性があります。

例

次に、XDMCP アプリケーション インスペクションに対しデフォルト レベル（1）でデバッグ メッセージをイネーブルにする例を示します。

```
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 インスペクションをイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

debug xml

XML 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 xml** 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 xml [**element** | **event**]

no debug xml [**element** | **event**]

構文の説明

element	（任意）個々の XML 要素の処理に関連するデバッグ イベントを表示します。
event	（任意）XML 解析またはエラー イベントを表示します。

デフォルト

キーワードを指定しないと、すべての XML パーサー デバッグ メッセージが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	変更内容
8.0(2)	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 プロセスで高プライオリティ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。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

例

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

```
hostname# debug xml element
debug xml element enabled at level 1

XML Executes cmd: hostname hostname
XML Executes cmd: domain-name example.com
XML Executes cmd: names
XML Executes cmd: dns-guard
XML Executes cmd: !
XML Executes cmd: interface Ethernet0
XML Executes cmd:  nameif outside
```

```
XML Executes cmd:  security-level 0
XML Executes cmd:  ip address 192.168.5.151 255.255.255.0 standby 192.168.5.152
XML Executes cmd: interface Ethernet1
XML Executes cmd:  nameif inside
XML Executes cmd:  security-level 100
XML Executes cmd:  ip address 192.168.0.151 255.255.255.0 standby 192.168.0.152
XML Executes cmd: !
XML Executes cmd: boot system flash:/f
XML Executes cmd: ftp mode passive
XML Executes cmd: clock timezone jst 9
XML Executes cmd: dns server-group DefaultDNS
XML Executes cmd:  domain-name cisco.com
_tcp_listen: could not query index for interface 65535 port 23
XML Executes cmd: pager lines 24
XML Executes cmd: logging console debugging
XML Executes cmd: logging buffered debugging
XML Executes cmd: mtu outside 1500
XML Executes cmd: mtu inside 1500
XML Executes cmd: failover
XML Executes cmd: no asdm history enable
XML Executes cmd: arp timeout 14000
XML Executes cmd: route outside 0.0.0.0 0.0.0.0 192.168.5.1 1
XML Executes cmd: timeout xlate 3:00:00
XML Executes cmd: timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
XML Executes cmd: timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat
0:05:00
XML Executes cmd: timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect
0:02:00
XML Executes cmd: timeout uauth 0:05:00 absolute
XML Executes cmd: username user1 password mbO2jYs13AXlIAGa encrypted
XML Executes cmd: username sugi password EB3OP7Hu2hSu6x/7 encrypted
XML Executes cmd: http server enable
XML Executes cmd: http 0.0.0.0 0.0.0.0 outside
XML Executes cmd: no snmp-server location
XML Executes cmd: no snmp-server contact
XML Executes cmd: snmp-server enable traps snmp authentication linkup linkdown coldstart
XML Executes cmd: telnet timeout 5
XML Executes cmd: ssh timeout 5
XML Executes cmd: console timeout 0
XML Executes cmd: !
XML Executes cmd: class-map inspection_default
XML Executes cmd:  match default-inspection-traffic
XML Executes cmd: !
XML Executes cmd: !
XML Executes cmd: policy-map type inspect dns migrated_dns_map_1
XML Executes cmd:  parameters
XML Executes cmd:   message-length maximum 512
XML Executes cmd: policy-map global_policy
XML Executes cmd:  class inspection_default
XML Executes cmd:   inspect ftp
XML Executes cmd:   inspect h323 h225
XML Executes cmd:   inspect h323 ras
XML Executes cmd:   inspect netbios
XML Executes cmd:   inspect rsh
XML Executes cmd:   inspect rtsp
XML Executes cmd:   inspect skinny
XML Executes cmd:   inspect esmtp
XML Executes cmd:   inspect sqlnet
XML Executes cmd:   inspect sunrpc
XML Executes cmd:   inspect tftp
XML Executes cmd:   inspect sip
XML Executes cmd:   inspect xdmcp
XML Executes cmd: !
XML Executes cmd: service-policy global_policy global
```

```
XML error info: cmd-id 87 type info
XML Executes cmd: prompt hostname context
XML Executes cmd: crashinfo save disable
```

次に、**debug xml event** コマンドの出力例を示します。

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

XML parsing: data = <con... len = 3176
Exit XML parser, ret code = 0
```

関連コマンド

コマンド	説明
show debug	各種の **debug** コマンドのデバッグ ステータスを表示します。