CHAPTER 19

logging asdm コマンド～ logout message コマンド

logging asdm

ASDM ログ バッファにシステム ログ メッセージを送信するには、グローバル コンフィギュレーション モードで **logging asdm** コマンドを使用します。ASDM ログ バッファへのロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

logging asdm [*logging_list* | *level*]

no logging asdm [*logging_list* | *level*]

シンタックスの説明

level	システム ログ メッセージの最大レベルを設定します。たとえば、レベルを 3 に設定すると、セキュリティ アプライアンスはレベル 3、2、1、および 0 のシステム ログ メッセージを生成します。次の数値または名前で指定できます。 • **0** または **emergencies**：システムが使用不能 • **1** または **alerts**：ただちに処置が必要 • **2** または **critical**：クリティカルな状態 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：正常だが、注意が必要な状態 • **6** または **informational**：情報 • **7** または **debugging**:デバッグ メッセージ、ログ FTP コマンド、WWW URL
logging_list	ASDM ログ バッファに送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

デフォルト

ASDM のロギングは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

使用上のガイドライン

ASDM ログ バッファにメッセージが送信される前に、**logging enable** コマンドを使用して、ロギングをイネーブルにしておく必要があります。

ASDM のログ バッファがいっぱいである場合、セキュリティ アプライアンスは最も古いメッセージを削除して、新しいメッセージ用の空き領域をバッファ内に確保します。ASDM のログ バッファに保持されるシステム ログ メッセージの数を制御するには、**logging asdm-buffer-size** コマンドを使用します。

ASDM のログ バッファは、**logging buffered** コマンドでイネーブルにするログ バッファとは別のバッファです。

例

次の例は、ロギングをイネーブルにして、ASDM ログ バッファに重大度 0、1、および 2 のメッセージを送信する方法を示しています。また、ASDM ログ バッファのサイズを 200 メッセージに設定する方法も示しています。

```
hostname(config)# logging enable
hostname(config)# logging asdm 2
hostname(config)# logging asdm-buffer-size 200
hostname(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: level critical, 48 messages logged
```

関連コマンド

コマンド	説明
clear logging asdm	ASDM ログ バッファが保持しているメッセージをすべて消去します。
logging asdm-buffer-size	ASDM ログ バッファに保持される ASDM メッセージの数を指定します。
logging enable	ロギングをイネーブルにします。
logging list	再使用可能なメッセージ選択基準リストを作成します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	ロギングのコンフィギュレーションを表示します。

logging asdm-buffer-size

ASDM のログ バッファに保持されるシステム ログ メッセージの数を指定するには、グローバル コンフィギュレーション モードで **logging asdm-buffer-size** コマンドを使用します。ASDM ログ バッファをデフォルト サイズの 100 メッセージにリセットするには、このコマンドの **no** 形式を使用します。

logging asdm-buffer-size *num_of_msgs*

no logging asdm-buffer-size *num_of_msgs*

シンタックスの説明

num_of_msgs	セキュリティ アプライアンスが ASDM ログ バッファに保持するシステム ログ メッセージの数を指定します。

デフォルト

デフォルトの ASDM syslog バッファ サイズは 100 メッセージです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

使用上のガイドライン

ASDM のログ バッファがいっぱいである場合、セキュリティ アプライアンスは最も古いメッセージを削除して、新しいメッセージ用の空き領域をバッファ内に確保します。ASDM ログ バッファへのロギングをイネーブルにするかどうかを制御する場合や、ASDM ログ バッファに保持されるシステム ログ メッセージの種類を制御する場合は、**logging asdm** コマンドを使用します。

ASDM のログ バッファは、**logging buffered** コマンドでイネーブルにするログ バッファとは別のバッファです。

例

次の例は、ロギングをイネーブルにして、ASDM ログ バッファに重大度 0、1、および 2 のメッセージを送信する方法を示しています。また、ASDM ログ バッファのサイズを 200 メッセージに設定する方法も示しています。

```
hostname(config)# logging enable
hostname(config)# logging asdm 2
hostname(config)# logging asdm-buffer-size 200
hostname(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: level critical, 48 messages logged
```

関連コマンド

コマンド	説明
clear logging asdm	ASDM ログ バッファが保持しているメッセージをすべて消去します。
logging asdm	ASDM ログ バッファへのロギングをイネーブルにします。
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在動作しているロギング コンフィギュレーションを表示します。

logging buffered

セキュリティ アプライアンスがシステム ログ メッセージをログ バッファに送信できるようにするには、グローバル コンフィギュレーション モードで **logging buffered** コマンドを使用します。ログ バッファへのロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

logging buffered [*logging_list* | *level*]

no logging buffered [*logging_list* | *level*]

シンタックスの説明

level	システム ログ メッセージの最大レベルを設定します。たとえば、レベルを 3 に設定すると、セキュリティ アプライアンスはレベル 3、2、1、および 0 のシステム ログ メッセージを生成します。次の数値または名前で指定できます。 • **0** または **emergencies**：システムが使用不能 • **1** または **alerts**：ただちに処置が必要 • **2** または **critical**：クリティカルな状態 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：正常だが、注意が必要な状態 • **6** または **informational**：情報 • **7** または **debugging**:デバッグ メッセージ、ログ FTP コマンド、WWW URL
logging_list	ログ バッファに送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

デフォルト

デフォルトは次のとおりです。

- バッファへのロギングはディセーブルです。
- バッファのサイズは 4 KB です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル 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
既存	このコマンドは既存のものです。

使用上のガイドライン

ログ バッファにメッセージが送信される前に、**logging enable** コマンドを使用してロギングをイネーブルにしておく必要があります。

新しいメッセージは、バッファの最後に追加されます。バッファがいっぱいになると、セキュリティ アプライアンスはバッファを消去してから、メッセージの追加を続行します。ログ バッファがいっぱいである場合、セキュリティ アプライアンスは最も古いメッセージを削除して、新しいメッセージ用の空き領域をバッファ内に確保します。バッファの内容が「ラップ」されるたびにバッファの内容を自動的に保存することができます。これは、最後に保存されてから追加されたすべてのメッセージが新しいメッセージに置き換えられることを意味します。詳細については、**logging flash-bufferwrap** コマンドと **logging ftp-bufferwrap** コマンドを参照してください。

バッファの内容は、いつでもフラッシュ メモリに保存できます。詳細については、**logging savelog** コマンドを参照してください。

バッファに送信されたシステム ログ メッセージは、**show logging** コマンドで表示できます。

例

次の例では、レベル 0 およびレベル 1 のイベントに対して、バッファへのロギングを設定します。

```
hostname(config)# logging buffered alerts
hostname(config)#
```

次の例では、最大ロギング レベル 7 の notif-list というリストを作成し、notif-list リストで識別されるシステム ログ メッセージに対して、バッファへのロギングを設定します。

```
hostname(config)# logging list notif-list level 7
hostname(config)# logging buffered notif-list
hostname(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファが保持しているシステム ログ メッセージをすべて消去します。
logging buffer-size	ログ バッファのサイズを指定します。
logging enable	ロギングをイネーブルにします。
logging flash-bufferwrap	ログ バッファがいっぱいになったときに、ログ バッファをフラッシュ メモリに書き込みます。
logging ftp-bufferwrap	ログ バッファがいっぱいになったときに、ログ バッファを FTP サーバに送信します。
logging list	再使用可能なメッセージ選択基準リストを作成します。
logging savelog	ログ バッファの内容をフラッシュ メモリに保存します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在動作しているロギング コンフィギュレーションを表示します。

logging buffer-size

ログ バッファのサイズを指定するには、グローバル コンフィギュレーション モードで **logging buffer-size** コマンドを使用します。ログ バッファをデフォルト サイズの 4 KB にリセットするには、このコマンドの **no** 形式を使用します。

logging buffer-size *bytes*

no logging buffer-size *bytes*

シンタックスの説明

bytes	ログ バッファに使用するメモリ量をバイト単位で設定します。たとえば、8,192 を指定した場合、セキュリティ アプライアンスはログ バッファに 8 KB のメモリを使用します。

デフォルト

ログ バッファのメモリ サイズは 4KB です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスが使用しているログ バッファのサイズがデフォルトのバッファ サイズと異なっているかどうかを確認するには、**show running-config logging** コマンドを使用します。**logging buffer-size** コマンドが表示されない場合、セキュリティ アプライアンスが使用するログ バッファのサイズは 4 KB です。

セキュリティ アプライアンスによるバッファの使用方法の詳細については、**logging buffered** コマンドを参照してください。

例

次の例では、ロギングとロギング バッファをイネーブルにし、セキュリティ アプライアンスがログ バッファ用に 16 KB のメモリを使用するように指定します。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging buffer-size 16384
hostname(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファが保持しているシステム ログ メッセージをすべて消去します。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging enable	ロギングをイネーブルにします。
logging flash-bufferwrap	ログ バッファがいっぱいになったときに、ログ バッファをフラッシュ メモリに書き込みます。
logging savelog	ログ バッファの内容をフラッシュ メモリに保存します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在動作しているロギング コンフィギュレーションを表示します。

logging class

メッセージ クラスに対して、ロギング先ごとの最大ロギング レベルを設定するには、グローバル コンフィギュレーション モードで **logging class** コマンドを使用します。メッセージ クラスのロギング レベル コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

logging class *class destination level* [*destination level . . .*]

no logging class ***class***

シンタックスの説明

class	設定するロギング先ごとの最大ロギング レベルの対象となるメッセージ クラスを指定します。クラスの有効値については、後述する「使用上のガイドライン」の項を参照してください。
destination	*class* に対してロギング先を指定します。このロギング先についての、*destination* に送信される最大ロギング レベルは、*level* によって決まります。*destination* の有効値については、後述する「使用上のガイドライン」の項を参照してください。
level	システム ログ メッセージの最大レベルを設定します。たとえば、レベルを 3 に設定すると、セキュリティ アプライアンスはレベル 3、2、1、および 0 のシステム ログ メッセージを生成します。次の数値または名前で指定できます。 • **0** または **emergencies**：システムが使用不能 • **1** または **alerts**：ただちに処置が必要 • **2** または **critical**：クリティカルな状態 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：正常だが、注意が必要な状態 • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、WWW URL

デフォルト

デフォルトでは、セキュリティ アプライアンスは、ロギング先およびメッセージ クラスごとにロギング レベルを適用しないようになっています。代わりに、イネーブルになっている各ロギング先は、ロギング リストで指定されたロギング レベル、またはロギング先をイネーブルにするときに指定されたレベルで、すべてのクラスに対するメッセージを受信します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル 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　*class* の有効値は、次のとおりです。

- **auth**：ユーザ認証。
- **bridge**：透過ファイアウォール。
- **ca**：PKI 認証局。
- **config**：コマンド インターフェイス。
- **eap**：Extensible Authentication Protocol（EAP）。ネットワーク アドミッション コントロールをサポートするために、EAP セッションの状態変化、EAP ステータス クエリー イベント、および EAP ヘッダーとパケット内容の 16 進ダンプをログに記録します。
- **eapoudp**：Extensible Authentication Protocol（EAP）over UDP。ネットワーク アドミッション コントロールをサポートするための EAPoUDP イベントをログに記録し、EAPoUDP ヘッダーとパケット内容の完全なレコードを生成します。
- **email**：電子メール プロキシ。
- **ha**：フェールオーバー。
- **ids**：侵入検知システム。
- **ip**：IP スタック。
- **nac**：ネットワーク アドミッション コントロール。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 の適用、および再検証の各イベントをログに記録します。
- **np**：ネットワーク プロセッサ。
- **ospf**：OSPF ルーティング。
- **rip**：RIP ルーティング。
- **session**：ユーザ セッション。
- **snmp**：SNMP。
- **sys**：システム。
- **vpn**：IKE および IPSec。
- **vpnc**：VPN クライアント。
- **vpnfo**：VPN フェールオーバー。
- **vpnlb**：VPN ロード バランシング。

有効なロギング先は、次のとおりです。

- **asdm**：このロギング先については、**logging asdm** コマンドを参照してください。
- **buffered**：このロギング先については、**logging buffered** コマンドを参照してください。
- **console**：このロギング先については、**logging console** コマンドを参照してください。
- **history**：このロギング先については、**logging history** コマンドを参照してください。
- **mail**：このロギング先については、**logging mail** コマンドを参照してください。
- **monitor**：このロギング先については、**logging monitor** コマンドを参照してください。
- **trap**：このロギング先については、**logging trap** コマンドを参照してください。

例　次の例では、フェールオーバー関連のメッセージに対して、ASDM ログ バッファの最大ロギング レベルが 2 で、システム ログ バッファの最大ロギング レベルが 7 であることを指定します。

```
hostname(config)# logging class ha asdm 2 buffered 7
hostname(config)#
```

関連コマンド

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

logging console

セキュリティ アプライアンスがシステム ログ メッセージをコンソール セッションに表示できるようにするには、グローバル コンフィギュレーション モードで **logging console** コマンドを使用します。システム ログ メッセージをコンソール セッションに表示しないようにするには、このコマンドの **no** 形式を使用します。

logging console [*logging_list* | *level*]

no logging console

（注） このコマンドを使用すると、バッファ オーバーフローによって多数のシステム ログ メッセージがドロップされる可能性があるため、このコマンドの使用はお勧めできません。詳細については、後述する「使用上のガイドライン」の項を参照してください。

シンタックスの説明

level	システム ログ メッセージの最大レベルを設定します。たとえば、レベルを 3 に設定すると、セキュリティ アプライアンスはレベル 3、2、1、および 0 のシステム ログ メッセージを生成します。次の数値または名前で指定できます。 • **0** または **emergencies**：システムが使用不能 • **1** または **alerts**：ただちに処置が必要 • **2** または **critical**：クリティカルな状態 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：正常だが、注意が必要な状態 • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、WWW URL
logging_list	コンソール セッションに送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

デフォルト

セキュリティ アプライアンスは、デフォルトでは、システム ログ メッセージをコンソール セッションに表示しません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

コンソールにメッセージが送信される前に、**logging enable** コマンドを使用してロギングをイネーブルにしておく必要があります。

注意　**logging console** コマンドを使用すると、システム パフォーマンスが大幅に低下する可能性があります。代わりに、**logging buffered** を使用してロギングを開始し、**show logging** コマンドを使用してメッセージを表示してください。最新のメッセージをより簡単に表示するには、**clear logging** ***buffer*** コマンドを使用してバッファを消去します。

例

次の例は、レベル 0、1、2、および 3 のシステム ログ メッセージをコンソール セッションに表示できるようにする方法を示しています。

```
hostname(config)# logging enable
hostname(config)# logging console errors
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging list	再使用可能なメッセージ選択基準リストを作成します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのロギング関連の部分を表示します。

logging debug-trace

デバッグ メッセージを、重大度 7 で発行された syslog メッセージ 711001 としてログにリダイレクトするには、グローバル コンフィギュレーション モードで **logging debug-trace** コマンドを使用します。ログへのデバッグ メッセージの送信を停止するには、このコマンドの **no** 形式を使用します。

logging debug-trace

no logging debug-trace

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトでは、セキュリティ アプライアンスはデバッグ出力をシステム ログ メッセージに含めません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ メッセージは、重大度 7 のメッセージとして生成されます。このメッセージは、syslog メッセージ番号 711001 と一緒にログに表示されます。

例

次の例は、ロギングをイネーブルにし、ログ メッセージをシステム ログ バッファに送信し、デバッグ出力をログにリダイレクトし、ディスク アクティビティのデバッグをオンにする方法を示しています。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging debug-trace
hostname(config)# debug disk filesystem
```

ログに表示できるデバッグ メッセージの例を次に示します。

```
%PIX-7-711001: IFS: Read: fd 3, bytes 4096
```

関連コマンド

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

logging device-id

EMBLEM 形式でないシステム ログ メッセージにデバイス ID を含めるようにセキュリティ アプライアンスを設定するには、グローバル コンフィギュレーション モードで **logging device-id** コマンドを使用します。デバイス ID の使用をディセーブルにするには、このコマンドの **no** 形式を使用します。

logging device-id {***context-name*** | ***hostname*** | ***ipaddress*** *interface_name* | ***string*** *text*}

no logging device-id {***context-name*** | ***hostname*** | ***ipaddress*** *interface_name* | ***string*** *text*}

シンタックスの説明

context-name	デバイス ID として、現在のコンテキストの名前を使用します。
hostname	デバイス ID として、セキュリティ アプライアンスのホスト名を使用します。
ipaddress *interface_name*	デバイス ID として、*interface_name* で指定されたインターフェイスの IP アドレスを使用します。**ipaddress** キーワードを使用すると、セキュリティ アプライアンスがログ データを外部サーバに送信するために使用するインターフェイスに関係なく、外部サーバに送信されるシステム ログ メッセージに、指定されたインターフェイスの IP アドレスが含まれます。
string *text*	デバイス ID として、*text* に含まれている最大 16 文字の文字を使用します。*text* にスペースや次の文字は使用できません。 • &：アンパサンド • '：一重引用符 • "：二重引用符 • <：小なり • >：大なり • ?：疑問符

デフォルト

システム ログ メッセージにデフォルトのデバイス ID は使用されません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル 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
既存	このコマンドは既存のものです。

使用上のガイドライン

ipaddress キーワードを使用すると、デバイス ID は、メッセージが送信されたインターフェイスに関係なく、指定したセキュリティ アプライアンス インターフェイスの IP アドレスとなります。このキーワードの使用により、そのデバイスから送信されるメッセージすべてに、1 つの同じデバイス ID が割り当てられます。

例

次の例は、secappl-1 というホストを設定する方法を示しています。

```
hostname(config)# logging device-id hostname
hostname(config)# show logging
Syslog logging: disabled
Facility: 20
Timestamp logging: disabled
Standby logging: disabled
Console logging: disabled
Monitor logging: disabled
Buffer logging: level informational, 991 messages logged
Trap logging: disabled
History logging: disabled
Device ID: hostname "secappl-1"
```

syslog メッセージでは、ホスト名 secappl-1 はメッセージの先頭に表示されます。メッセージの例を次に示します。

```
secappl-1 %PIX-5-111008: User 'enable_15' executed the 'logging buffer-size 4096'
command.
```

関連コマンド

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

logging emblem

syslog サーバ以外のロギング先に送信されるシステム ログ メッセージに EMBLEM 形式を使用するには、グローバル コンフィギュレーション モードで **logging emblem** コマンドを使用します。EMBLEM 形式の使用をディセーブルにするには、このコマンドの **no** 形式を使用します。

logging emblem

no logging emblem

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトでは、セキュリティ アプライアンスはシステム ログ メッセージに EMBLEM 形式を使用しません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが **logging host** コマンドと無関係になるように変更されました。

使用上のガイドライン

logging emblem コマンドを使用すると、syslog サーバを除くすべてのロギング先に対して、EMBLEM 形式のロギングをイネーブルにできます。**logging timestamp** キーワードもイネーブルにすると、タイムスタンプ付きのメッセージが送信されます。

syslog サーバに対して EMBLEM 形式のロギングをイネーブルにするには、**logging host** コマンドに ***format emblem*** オプションを使用します。

例

次の例は、ロギングをイネーブルにし、syslog サーバを除くすべてのロギング先へのロギングに対して、EMBLEM 形式の使用をイネーブルにする方法を示しています。

```
hostname(config)# logging enable
hostname(config)# logging emblem
hostname(config)#
```

関連コマンド

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

logging enable

設定済みの出力場所すべてに対してロギングをイネーブルにするには、グローバル コンフィギュレーション モードで **logging enable** コマンドを使用します。ロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

logging enable

no logging enable

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

ロギングは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが **logging on** コマンドから変更されました。

使用上のガイドライン

logging enable コマンドを使用すると、サポートされている任意のロギング先に対するシステム ログ メッセージの送信をイネーブルまたはディセーブルにできます。すべてのロギングを停止するには、**no logging enable** コマンドを使用します。

個別のロギング先へのロギングをイネーブルにするには、次のコマンドを使用します。

- **logging asdm**
- **logging buffered**
- **logging console**
- **logging history**
- **logging mail**
- **logging monitor**
- **logging trap**

例

次の例は、ロギングをイネーブルにする方法を示しています。**show logging** コマンドの出力は、使用可能な各ロギング先を個別にイネーブルにする必要がある状況を示しています。

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

関連コマンド

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

logging facility

syslog サーバに送信されるメッセージに使用するロギング ファシリティを指定するには、グローバル コンフィギュレーション モードで **logging facility** コマンドを使用します。ロギング ファシリティをデフォルトの 20 にリセットするには、このコマンドの **no** 形式を使用します。

logging facility*facility*

no logging facility

シンタックスの説明

facility	syslog ファシリティを指定します。有効値は 16 ～ 23 です。

デフォルト

デフォルト ファシリティは 20（LOCAL4）です。

コマンド モード

次の表は、コマンドを入力できるモードを示しています。例外については、上記の「シンタックスの説明」の項を参照してください。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

syslog サーバは、メッセージの *facility* 番号をもとに、メッセージをファイルします。使用可能なファシリティには、16（LOCAL0）～ 23（LOCAL7）の 8 つがあります。

例

次の例は、セキュリティ アプライアンスがロギング ファシリティを 16 としてシステム ログ メッセージに指定するように設定する方法を示しています。**show logging** コマンドの出力には、セキュリティ アプライアンスによって使用されているファシリティが含まれます。

```
hostname(config)# logging facility 16
hostname(config)# show logging
Syslog logging: enabled
    Facility: 16
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: level errors, facility 16, 3607 messages logged
        Logging to infrastructure 10.1.2.3
    History logging: disabled
    Device ID: 'inside' interface IP address "10.1.1.1"
    Mail logging: disabled
    ASDM logging: disabled
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging host	syslog サーバを定義します。
logging trap	syslog サーバへのロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのロギング関連の部分を表示します。

logging flash-bufferwrap

バッファが未保存のメッセージでいっぱいになるたびに、セキュリティ アプライアンスがログ バッファをフラッシュ メモリに書き込めるようにするには、グローバル コンフィギュレーション モードで **logging flash-bufferwrap** コマンドを使用します。ログ バッファをフラッシュ メモリに書き込めないようにするには、このコマンドの **no** 形式を使用します。

logging flash-bufferwrap

no logging flash-bufferwrap

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトは次のとおりです。

- バッファへのロギングはディセーブルです。
- フラッシュ メモリへのログ バッファの書き込みはディセーブルです。
- バッファのサイズは 4 KB です。
- フラッシュ メモリの最小空き容量は 3 MB です。
- バッファ ロギング用のフラッシュ メモリ最大割当量は、1 MB です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスがログ バッファをフラッシュ メモリに書き込めるようにするには、バッファへのロギングをイネーブルにする必要があります。このようにしないと、フラッシュ メモリに書き込むデータがログ バッファに保持されません。バッファへのロギングをイネーブルにするには、**logging buffered** コマンドを使用します。

セキュリティ アプライアンスは、ログ バッファの内容をフラッシュ メモリに書き込む間も、新しいイベント メッセージをログ バッファに継続的に格納します。

セキュリティ アプライアンスは、次のように、デフォルトのタイムスタンプ形式を使用した名前でログ ファイルを作成します。

LOG-*YYYY-MM-DD-HHMMSS*.TXT

YYYY は西暦年、*MM* は月、*DD* は日、*HHMMSS* は時刻の時、分、秒です。

フラッシュ メモリの可用性により、セキュリティ アプライアンスが **logging flash-bufferwrap** コマンドを使用してシステム ログ メッセージを保存するときの方法が異なります。詳細については、**logging flash-maximum-allocation** コマンドと **logging flash-minimum-free** コマンドを参照してください。

例

次の例は、ロギングとログ バッファをイネーブルにし、セキュリティ アプライアンスがログ バッファをフラッシュ メモリに書き込めるようにする方法を示しています。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging flash-bufferwrap
hostname(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファが保持しているシステム ログ メッセージをすべて消去します。
copy	ファイルを、ある位置から TFTP サーバや FTP サーバなどの別の位置にコピーします。
delete	保存済みログ ファイルなどのファイルを、ディスク パーティションから削除します。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging buffer-size	ログ バッファのサイズを指定します。
logging enable	ロギングをイネーブルにします。
logging flash-maximum-allocation	フラッシュ メモリについて、ログ バッファの内容を書き込むために使用できる最大量を指定します。
logging flash-minimum-free	フラッシュ メモリへのログ バッファの書き込みを許可するときに、セキュリティ アプライアンスが使用できるようにしておく必要のある最小限のフラッシュ メモリ量を指定します。
show logging	イネーブルなロギング オプションを表示します。

logging flash-maximum-allocation

セキュリティ アプライアンスがログ データの格納に使用するフラッシュ メモリの最大量を指定するには、グローバル コンフィギュレーション モードで **logging flash-maximum-allocation** コマンドを使用します。このコマンドにより、**logging savelog** コマンドと **logging flash-bufferwrap** コマンドで使用できるフラッシュ メモリの最大量が決まります。この用途に使用するフラッシュ メモリの最大量をデフォルト サイズの 1 MB にリセットするには、このコマンドの **no** 形式を使用します。

logging flash-maximum-allocation *kbytes*

no logging flash-maximum-allocation *kbytes*

シンタックスの説明

kbytes	セキュリティ アプライアンスがログ バッファ データの保存に使用できるフラッシュ メモリの最大量（KB 単位）。

デフォルト

ログ データ用のデフォルトのフラッシュ メモリ最大割当量は、1 MB です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

使用上のガイドライン

logging savelog または **logging flash-bufferwrap** によって保存されるログ ファイルが原因で、ログ ファイル用のフラッシュ メモリの使用量が、**logging flash-maximum-allocation** コマンドで指定された最大量を超える場合、セキュリティ アプライアンスは最も古いログ ファイルを削除して、新しいログ ファイル用に十分な量のメモリを開放します。削除するファイルがない場合や、古いファイルをすべて削除してもメモリの空き容量が新しいログ ファイル用には小さすぎる場合、セキュリティ アプライアンスは新しいログ ファイルを保存できません。

セキュリティ アプライアンスによるフラッシュ メモリの最大割当量がデフォルト サイズと異なっているかどうかを確認するには、**show running-config logging** コマンドを使用します。**logging flash-maximum-allocation** コマンドが表示されない場合、セキュリティ アプライアンスがログ バッファ データの保存に使用する最大サイズは 1 MB です。割り当てられたメモリは、**logging savelog** コマンドと **logging flash-bufferwrap** コマンドの両方に使用されます。

セキュリティ アプライアンスによるログ バッファの使用方法の詳細については、**logging buffered** コマンドを参照してください。

例

次の例は、ロギングとログ バッファをイネーブルにし、セキュリティ アプライアンスがログ バッファをフラッシュ メモリに書き込めるようにし、ログ ファイルの書き込みに使用するフラッシュ メモリの最大量を約 1.2 MB に設定する方法を示しています。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging flash-bufferwrap
hostname(config)# logging flash-maximum-allocation 1200
hostname(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファが保持しているシステム ログ メッセージをすべて消去します。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging enable	ロギングをイネーブルにします。
logging flash-bufferwrap	ログ バッファがいっぱいになったときに、ログ バッファをフラッシュ メモリに書き込みます。
logging flash-minimum-free	フラッシュ メモリへのログ バッファの書き込みを許可するときに、セキュリティ アプライアンスが使用できるようにしておく必要のある最小限のフラッシュ メモリ量を指定します。
logging savelog	ログ バッファの内容をフラッシュ メモリに保存します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在動作しているロギング コンフィギュレーションを表示します。

logging flash-minimum-free

セキュリティ アプライアンスが新しいログ ファイルを保存する前に確保しておく必要のあるフラッシュ メモリの最小空き容量を指定するには、グローバル コンフィギュレーション モードで **logging flash-minimum-free** コマンドを使用します。このコマンドは、**logging savelog** コマンドと **logging flash-bufferwrap** コマンドで作成されたログ ファイルをセキュリティ アプライアンスが保存する前に確保しておく必要のあるフラッシュ メモリの空き容量に影響を及ぼします。フラッシュ メモリの必要最小限の空き容量をデフォルト サイズの 3 MB にリセットするには、このコマンドの **no** 形式を使用します。

logging flash-minimum-free *kbytes*

no logging flash-minimum-free *kbytes*

シンタックスの説明

kbytes	セキュリティ アプライアンスが新しいログ ファイルを保存する前に使用可能にしておく必要のあるフラッシュ メモリの最小量（KB 単位）。

デフォルト

デフォルトのフラッシュ メモリの最小空き容量は 3 MB です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

使用上のガイドライン

logging flash-minimum-free コマンドは、**logging savelog** コマンドと **logging flash-bufferwrap** コマンド用に常に確保しておく必要のあるフラッシュ メモリ量を指定します。

logging savelog または **logging flash-bufferwrap** によって保存されるログ ファイルが原因で、フラッシュ メモリの空き容量が、**logging flash-minimum-free** コマンドで指定された限度を下回る場合、セキュリティ アプライアンスは最も古いログ ファイルを削除して、新しいログ ファイルの保存後もメモリの最小空き容量が保持されることを保証します。削除するファイルがない場合や、古いファイルをすべて削除してもメモリの空き容量が限度を下回る場合、セキュリティ アプライアンスは新しいログ ファイルを保存できません。

例

次の例は、ロギングとログ バッファをイネーブルにし、セキュリティ アプライアンスがログ バッファをフラッシュ メモリに書き込めるようにし、フラッシュ メモリの最小空き容量を 4,000 KB にする必要があることを指定する方法を示しています。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging flash-bufferwrap
hostname(config)# logging flash-minimum-free 4000
hostname(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファが保持しているシステム ログ メッセージをすべて消去します。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging enable	ロギングをイネーブルにします。
logging flash-bufferwrap	ログ バッファがいっぱいになったときに、ログ バッファをフラッシュ メモリに書き込みます。
logging flash-maximum-allocation	フラッシュ メモリについて、ログ バッファの内容を書き込むために使用できる最大量を指定します。
logging savelog	ログ バッファの内容をフラッシュ メモリに保存します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在動作しているロギング コンフィギュレーションを表示します。

logging from-address

セキュリティ アプライアンスによって電子メールで送信されるシステム ログ メッセージの送信者の電子メール アドレスを指定するには、グローバル コンフィギュレーション モードで **logging from-address** コマンドを使用します。電子メールで送信されるシステム ログ メッセージはすべて、指定したアドレスから送信されたように表示されます。送信者の電子メール アドレスを削除するには、このコマンドの **no** 形式を使用します。

logging from-address *from-email-address*

no logging from-address *from-email-address*

シンタックスの説明

from-email-address	送信元の電子メール アドレス（syslog 電子メールの送信元として表示される電子メール アドレス）。たとえば、cdb@example.com です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

使用上のガイドライン

システム ログ メッセージを電子メールで送信できるようにするには、**logging mail** コマンドを使用します。

このコマンドで指定するアドレスは、既存の電子メール アカウントに対応している必要はありません。

例

次の基準に従って、ロギングをイネーブルにし、システム ログ メッセージを電子メールで送信するようにセキュリティ アプライアンスを設定します。

- critical、alerts、および emergencies のメッセージを送信する。
- メッセージを送信するときに、ciscosecurityappliance@example.com を送信者のアドレスとして使用する。
- メッセージを admin@example.com に送信する。
- SMTP を使用して、メッセージをプライマリ サーバ pri-smtp-host およびセカンダリ サーバ sec-smtp-host に送信する。

次のコマンドを入力します。

```
hostname(config)# logging enable
hostname(config)# logging mail critical
hostname(config)# logging from-address ciscosecurityappliance@example.com
hostname(config)# logging recipient-address admin@example.com
hostname(config)# smtp-server pri-smtp-host sec-smtp-host
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging mail	セキュリティ アプライアンスがシステム ログ メッセージを電子メールで送信できるようにし、どのメッセージを電子メールで送信するかを決定します。
logging recipient-address	電子メールで送信されるシステム ログ メッセージの送信先となる電子メール アドレスを指定します。
smtp-server	SMTP サーバを設定します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在動作しているロギング コンフィギュレーションを表示します。

logging ftp-bufferwrap

バッファが未保存のメッセージでいっぱいになるたびに、セキュリティ アプライアンスがログ バッファを FTP サーバに送信できるようにするには、グローバル コンフィギュレーション モードで **logging ftp-bufferwrap** コマンドを使用します。ログ バッファを FTP サーバに送信しないようにするには、このコマンドの **no** 形式を使用します。

logging ftp-bufferwrap

no logging ftp-bufferwrap

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトは次のとおりです。

- バッファへのロギングはディセーブルです。
- FTP サーバへのログ バッファの送信はディセーブルです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

使用上のガイドライン

logging ftp-bufferwrap がイネーブルの場合、セキュリティ アプライアンスは、**logging ftp-server** コマンドで指定された FTP サーバにログ バッファ データを送信します。セキュリティ アプライアンスは、ログ データを FTP サーバに送信する間も、新しいイベント メッセージをログ バッファに継続的に格納します。

セキュリティ アプライアンスがログ バッファの内容を FTP サーバに送信できるようにするには、バッファへのロギングをイネーブルにする必要があります。このようにしないと、フラッシュ メモリに書き込むデータがログ バッファに保持されません。バッファへのロギングをイネーブルにするには、**logging buffered** コマンドを使用します。

セキュリティ アプライアンスは、次のように、デフォルトのタイムスタンプ形式を使用した名前でログ ファイルを作成します。

LOG-*YYYY-MM-DD-HHMMSS*.TXT

YYYY は西暦年、*MM* は月、*DD* は日、*HHMMSS* は時刻の時、分、秒です。

例

次の例は、ロギングとログ バッファをイネーブルにし、FTP サーバを指定し、セキュリティ アプライアンスがログ バッファを FTP サーバに書き込めるようにする方法を示しています。この例では、logserver-352 というホスト名の FTP サーバを指定しています。このサーバには、ユーザ名 logsupervisor とパスワード 1luvMy10gs を使用してアクセスできます。ログ ファイルは、/syslogs ディレクトリに保存されます。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging ftp-server logserver-352 /syslogs logsupervisor 1luvMy10gs
hostname(config)# logging ftp-bufferwrap
hostname(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファが保持しているシステム ログ メッセージをすべて消去します。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging buffer-size	ログ バッファのサイズを指定します。
logging enable	ロギングをイネーブルにします。
logging ftp-server	**logging ftp-bufferwrap** コマンドで使用する FTP サーバ パラメータを指定します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在動作しているロギング コンフィギュレーションを表示します。

logging ftp-server

logging ftp-bufferwrap がイネーブルの場合にセキュリティ アプライアンスがログ バッファ データを送信する FTP サーバについての詳細を指定するには、グローバル コンフィギュレーション モードで **logging ftp-server** コマンドを使用します。FTP サーバについての詳細をすべて削除するには、このコマンドの **no** 形式を使用します。

logging ftp-server *ftp-server ftp_server path username password*

no logging ftp-server *ftp-server ftp_server path username password*

シンタックスの説明

ftp-server	外部 FTP サーバの IP アドレスまたはホスト名。 **（注）** ホスト名を指定する場合は、ネットワーク上で DNS が正しく動作していることを確認してください。
path	ログ バッファ データの保存先となる FTP サーバ上のディレクトリ パス。このパスは、FTP ルート ディレクトリに対する相対パスです。次の例を参考にしてください。 `/security_appliances/syslogs/appliance107`
username	FTP サーバへのロギングに有効なユーザ名。
password	指定したユーザ名に対応するパスワード。

デフォルト

FTP サーバは、デフォルトでは指定されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

使用上のガイドライン

指定できる FTP サーバは 1 つのみです。ロギング FTP サーバがすでに指定されている場合、**logging ftp-server** コマンドを使用すると、その FTP サーバ コンフィギュレーションが、入力した新しいコンフィギュレーションに置き換えられます。

セキュリティ アプライアンスは、指定された FTP サーバ情報を確認しません。詳細を誤って設定した場合、セキュリティ アプライアンスはログ バッファ データを FTP サーバに送信できません。

例

次の例は、ロギングとログ バッファをイネーブルにし、FTP サーバを指定し、セキュリティ アプライアンスがログ バッファを FTP サーバに書き込めるようにする方法を示しています。この例では、logserver-352 というホスト名の FTP サーバを指定しています。このサーバには、ユーザ名 logsupervisor とパスワード 1luvMy10gs を使用してアクセスできます。ログ ファイルは、/syslogs ディレクトリに保存されます。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging ftp-server logserver-352 /syslogs logsupervisor 1luvMy10gs
hostname(config)# logging ftp-bufferwrap
hostname(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファが保持しているシステム ログ メッセージをすべて消去します。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging buffer-size	ログ バッファのサイズを指定します。
logging enable	ロギングをイネーブルにします。
logging ftp-bufferwrap	ログ バッファがいっぱいになったときに、ログ バッファを FTP サーバに送信します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在動作しているロギング コンフィギュレーションを表示します。

logging history

SNMP ロギングをイネーブルにし、SNMP サーバに送信されるメッセージを指定するには、グローバル コンフィギュレーション モードで **logging history** コマンドを使用します。SNMP ロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

logging history [*logging_list* | *level*]

no logging history

シンタックスの説明

level	システム ログ メッセージの最大レベルを設定します。たとえば、レベルを 3 に設定すると、セキュリティ アプライアンスはレベル 3、2、1、および 0 のシステム ログ メッセージを生成します。次の数値または名前で指定できます。 • **0** または **emergencies**：システムが使用不能 • **1** または **alerts**：ただちに処置が必要 • **2** または **critical**：クリティカルな状態 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：正常だが、注意が必要な状態 • **6** または **informational**：情報 • **7** または **debugging**:デバッグ メッセージ、ログ FTP コマンド、WWW URL
logging_list	SNMP サーバに送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

デフォルト

セキュリティ アプライアンスは、デフォルトでは SNMP サーバにロギングしません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル 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
既存	このコマンドは既存のものです。

使用上のガイドライン

logging history コマンドを使用すると、SNMP サーバへのロギングをイネーブルにし、SNMP メッセージ レベルまたはイベント リストを設定することができます。

例

次の例は、SNMP ロギングをイネーブルにし、レベル 0、1、2、および 3 のメッセージが設定済みの SNMP サーバに送信されるよう指定する方法を示しています。

```
hostname(config)# logging enable
hostname(config)# snmp-server host infrastructure 10.2.3.7 trap community gam327
hostname(config)# snmp-server enable traps syslog
hostname(config)# logging history errors
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging list	再使用可能なメッセージ選択基準リストを作成します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのロギング関連の部分を表示します。
snmp-server	SNMP サーバの詳細を指定します。

logging host

syslog サーバを定義するには、グローバル コンフィギュレーション モードで **logging host** コマンドを使用します。syslog サーバの定義を削除するには、このコマンドの **no** 形式を使用します。

logging host *interface_name syslog_ip* [***tcp****/port* | ***udp****/port*] [**format emblem**]

logging host *interface_name syslog_ip*

シンタックスの説明

format emblem	（オプション）syslog サーバに対して EMBLEM 形式のロギングをイネーブルにします。
interface_name	syslog サーバが常駐するインターフェイス。
syslog_ip	syslog サーバの IP アドレス。
tcp	メッセージを syslog サーバに送信するときに、セキュリティ アプライアンスが TCP を使用することを指定します。
udp	メッセージを syslog サーバに送信するときに、セキュリティ アプライアンスが TCP を使用することを指定します。
port	syslog サーバがメッセージをリッスンするポート。有効となるポート値の範囲は、どちらのプロトコルの場合も 1025 ～ 65535 です。

デフォルト

デフォルトは次のとおりです。

- デフォルトのポート番号は次のとおりです。
  - UDP ポートは 514
  - TCP ポートは 1470
- デフォルト プロトコルは UDP です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル 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
既存	このコマンドは既存のものです。

使用上のガイドライン

logging host *ip_address* **format emblem** コマンドを使用すると、各 syslog サーバに対して EMBLEM 形式のロギングをイネーブルにできます。EMBLEM 形式のロギングは、UDP システム ログ メッセージに対してだけ利用できます。EMBLEM 形式のロギングを特定の syslog ホストに対してイネーブルにすると、メッセージがそのホストに送信されます。**logging timestamp** キーワードもイネーブルにすると、タイムスタンプ付きのメッセージが送信されます。

複数の **logging host** コマンドを使用して複数の追加サーバを指定すると、追加したサーバすべてがシステム ログ メッセージを受信します。ただし、サーバは UDP か TCP のどちらか一方を受信するように指定でき、両方を受信するようには指定できません。

（注）　*tcp* オプションが **logging host** コマンドで使用されている場合、syslog サーバに到達できないと、セキュリティ アプライアンスはファイアウォールを越える接続をドロップします。

以前入力した *port* と *protocol* の値のみを表示するには、**show running-config logging** コマンドを使用して、リストでコマンドを見つけます（TCP プロトコルは 6、UDP プロトコルは 17 として示されます）。TCP ポートは、セキュリティ アプライアンス syslog サーバに対してのみ動作します。*port* は、syslog サーバがリッスンするポートと一致している必要があります。

例

次の例は、内部インターフェイス上にあってデフォルトのプロトコルとポート番号を使用する syslog サーバに対して、レベル 0、1、2、および 3 のシステム ログ メッセージを送信する方法を示しています。

```
hostname(config)# logging enable
hostname(config)# logging host inside 10.2.2.3
hostname(config)# logging trap errors
hostname(config)#
```

関連コマンド

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

logging list

各種の基準（ロギング レベル、イベント クラス、およびメッセージ ID）でメッセージを指定するため、他のコマンドで使用するロギング リストを作成するには、グローバル コンフィギュレーション モードで **logging list** コマンドを使用します。リストを削除するには、このコマンドの **no** 形式を使用します。

logging list *name* {**level** *level* [**class** *event_class*] | **message** *start_id*[*-end_id*]}

no logging list *name*

シンタックスの説明

class *event_class*	（オプション）システム ログ メッセージのイベント クラスを設定します。指定されたレベルに対応する、指定されたクラスのシステム ログ メッセージのみが、コマンドによって特定されます。クラスのリストについては、「使用上のガイドライン」を参照してください。
level *level*	システム ログ メッセージの最大レベルを設定します。たとえば、レベルを 3 に設定すると、セキュリティ アプライアンスはレベル 3、2、1、および 0 のシステム ログ メッセージを生成します。次の数値または名前で指定できます。 • **0** または **emergencies**：システムが使用不能 • **1** または **alerts**：ただちに処置が必要 • **2** または **critical**：クリティカルな状態 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：正常だが、注意が必要な状態 • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、WWW URL
message *start_id*[*-end_id*]	メッセージ ID または ID の範囲を指定します。メッセージのデフォルト レベルを確認するには、**show logging** コマンドを使用するか、『*Cisco Security Appliance System Log Messages*』を参照してください。
name	ロギング リストの名前を設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル 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)	このコマンドがサポートされるようになりました。

使用上のガイドライン　リストを使用できるロギング コマンドは、次のとおりです。

- **logging asdm**
- **logging buffered**
- **logging console**
- **logging history**
- **logging mail**
- **logging monitor**
- **logging trap**

event_class に指定できる値は、次のとおりです。

- **auth**：ユーザ認証。
- **bridge**：透過ファイアウォール。
- **ca**：PKI 認証局。
- **config**：コマンド インターフェイス。
- **eap**：Extensible Authentication Protocol（EAP）。ネットワーク アドミッション コントロールをサポートするために、EAP セッションの状態変化、EAP ステータス クエリー イベント、および EAP ヘッダーとパケット内容の 16 進ダンプをログに記録します。
- **eapoudp**：Extensible Authentication Protocol（EAP）over UDP。ネットワーク アドミッション コントロールをサポートするための EAPoUDP イベントをログに記録し、EAPoUDP ヘッダーとパケット内容の完全なレコードを生成します。
- **email**：電子メール プロキシ。
- **ha**：フェールオーバー。
- **ids**：侵入検知システム。
- **ip**：IP スタック。
- **nac**：ネットワーク アドミッション コントロール。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 の適用、および再検証の各イベントをログに記録します。
- **np**：ネットワーク プロセッサ。
- **ospf**：OSPF ルーティング。
- **rip**：RIP ルーティング。
- **session**：ユーザ セッション。
- **snmp**：SNMP。
- **sys**：システム。
- **vpn**：IKE および IPSec。
- **vpnc**：VPN クライアント。
- **vpnfo**：VPN フェールオーバー。
- **vpnlb**：VPN ロード バランシング。

例　次の例は、logging list コマンドを使用する方法を示しています。

```
hostname(config)# logging list my-list 100100-100110
hostname(config)# logging list my-list level critical
hostname(config)# logging list my-list level warning class vpn
hostname(config)# logging buffered my-list
```

上記の例は、指定された基準に一致するシステム ログ メッセージがロギング バッファに送信されることを示しています。この例で指定されている基準は、次のとおりです。

1. 100100 ～ 100110 の範囲内にあるシステム ログ メッセージ ID
2. critical レベル以上（emergency、alert、または critical）にあるすべてのシステム ログ メッセージ
3. warning レベル以上（emergency、alert、critical、error、または warning）にある VPN クラスのすべてのシステム ログ メッセージ

システム ログ メッセージがこれらの条件のいずれかを満たしている場合、そのメッセージはバッファにロギングされます。

（注）　リストの基準を設計する場合、メッセージを重複して指定する基準にしてもかまいません。複数の基準に一致するシステム ログ メッセージも正常にロギングされます。

関連コマンド

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

logging mail

セキュリティ アプライアンスがシステム ログ メッセージを電子メールで送信したり、電子メールで送信するメッセージを判別したりできるようにするには、グローバル コンフィギュレーション モードで **logging mail** コマンドを使用します。システム ログ メッセージを電子メールで送信しないようにするには、このコマンドの **no** 形式を使用します。

logging mail [*logging_list* | *level*]

no logging mail [*logging_list* | *level*]

シンタックスの説明

level	システム ログ メッセージの最大レベルを設定します。たとえば、レベルを 3 に設定すると、セキュリティ アプライアンスはレベル 3、2、1、および 0 のシステム ログ メッセージを生成します。次の数値または名前で指定できます。 • **0** または **emergencies**：システムが使用不能 • **1** または **alerts**：ただちに処置が必要 • **2** または **critical**：クリティカルな状態 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：正常だが、注意が必要な状態 • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、WWW URL
logging_list	電子メールの受信者に送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

デフォルト

電子メールへのロギングは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル 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
既存	このコマンドは既存のものです。

使用上のガイドライン

電子メールで送信されたシステム ログ メッセージは、送信済み電子メールの件名欄に表示されます。

例

次の基準に従って、システム ログ メッセージを電子メールで送信するようにセキュリティ アプライアンスを設定します。

- critical、alerts、および emergencies のメッセージを送信する。
- メッセージを送信するときに、ciscosecurityappliance@example.com を送信者のアドレスとして使用する。
- メッセージを admin@example.com に送信する。
- SMTP を使用して、メッセージをプライマリ サーバ pri-smtp-host およびセカンダリ サーバ sec-smtp-host に送信する。

次のコマンドを入力します。

```
hostname(config)# logging mail critical
hostname(config)# logging from-address ciscosecurityappliance@example.com
hostname(config)# logging recipient-address admin@example.com
hostname(config)# smtp-server pri-smtp-host sec-smtp-host
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging from-address	電子メールで送信されるシステム ログ メッセージの送信元として表示する電子メール アドレスを指定します。
logging list	再使用可能なメッセージ選択基準リストを作成します。
logging recipient-address	電子メールで送信されるシステム ログ メッセージの送信先となる電子メール アドレスを指定します。
smtp-server	SMTP サーバを設定します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在動作しているロギング コンフィギュレーションを表示します。

logging message

システム ログ メッセージのロギング レベルを指定するには、グローバル コンフィギュレーション モードで **logging message** コマンドを ***level*** キーワードと組み合せて使用します。メッセージのロギング レベルをデフォルト レベルにリセットするには、このコマンドの **no** 形式を使用します。セキュリティ アプライアンスが特定のシステム ログ メッセージを生成しないようにするには、グローバル コンフィギュレーション モードで **logging message** コマンドの **no** 形式を使用します(***level*** キーワードは指定しません)。セキュリティ アプライアンスが特定のシステム ログ メッセージを生成できるようにするには、**logging message** コマンドを使用します（***level*** キーワードは指定しません)。これら 2 つの用途の **logging message** コマンドは、並行して実行できます。後述する「例」の項を参照してください。

logging message *syslog_id* **level** *level*

no logging message *syslog_id* **level** *level*

logging message *syslog_id*

no logging message *syslog_id*

シンタックスの説明

level *level*	システム ログ メッセージの最大レベルを設定します。たとえば、レベルを 3 に設定すると、セキュリティ アプライアンスはレベル 3、2、1、および 0 のシステム ログ メッセージを生成します。次の数値または名前で指定できます。 • **0** または **emergencies**：システムが使用不能 • **1** または **alerts**：ただちに処置が必要 • **2** または **critical**：クリティカルな状態 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：正常だが、注意が必要な状態 • **6** または **informational**：情報 • **7** または **debugging**:デバッグ メッセージ、ログ FTP コマンド、WWW URL
syslog_id	イネーブルまたはディセーブルにするシステム ログ メッセージ、または重大度を変更するシステム ログ メッセージの ID。メッセージのデフォルト レベルを確認するには、**show logging** コマンドを使用するか、『*Cisco Security Appliance System Log Messages*』を参照してください。

デフォルト

デフォルトでは、システム ログ メッセージはすべてイネーブルになっており、すべてのメッセージの重大度はデフォルト レベルに設定されています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル 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
既存	このコマンドは既存のものです。

使用上のガイドライン

logging message コマンドは、次の 2 つの用途に使用できます。

- メッセージをイネーブルとディセーブルのどちらにするかを制御する。
- メッセージの重大度を制御する。

メッセージに現在割り当てられているレベルや、メッセージがイネーブルになっているかどうかを判別するには、**show logging** コマンドを使用します。

例

次の例にある一連のコマンドは、**logging message** コマンドを使用して、メッセージをイネーブルにするかどうか、およびメッセージの重大度の両方を制御する方法を示しています。

```
hostname(config)# show logging message 403503
syslog 403503: default-level errors (enabled)

hostname(config)# logging message 403503 level 1
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)

hostname(config)# no logging message 403503
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (disabled)

hostname(config)# logging message 403503
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)

hostname(config)# no logging message 403503 level 3
hostname(config)# show logging message 403503
syslog 403503: default-level errors (enabled)
```

関連コマンド

コマンド	説明
clear configure logging	ロギング コンフィギュレーションすべてまたはメッセージ コンフィギュレーションのみを消去します。
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのロギング関連の部分を表示します。

logging monitor

セキュリティ アプライアンスがシステム ログ メッセージを SSH および Telnet セッションに表示できるようにするには、グローバル コンフィギュレーション モードで **logging monitor** コマンドを使用します。システム ログ メッセージを SSH および Telnet セッションに表示しないようにするには、このコマンドの **no** 形式を使用します。

logging monitor [*logging_list* | *level*]

no logging monitor

シンタックスの説明

level	システム ログ メッセージの最大レベルを設定します。たとえば、レベルを 3 に設定すると、セキュリティ アプライアンスはレベル 3、2、1、および 0 のシステム ログ メッセージを生成します。次の数値または名前で指定できます。 • **0** または **emergencies**：システムが使用不能 • **1** または **alerts**：ただちに処置が必要 • **2** または **critical**：クリティカルな状態 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：正常だが、注意が必要な状態 • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、WWW URL
logging_list	SSH または Telnet セッションに送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

デフォルト

セキュリティ アプライアンスは、デフォルトでは、システム ログ メッセージを SSH および Telnet セッションに表示しません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル 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
既存	このコマンドは既存のものです。

使用上のガイドライン

logging monitor コマンドを使用すると、現在のコンテキスト内のセッションすべてに対してシステム ログ メッセージをイネーブルにできます。ただし、セッションにシステム ログ メッセージを表示するかどうかは、セッションごとに **terminal** コマンドで制御します。

例

次の例は、システム ログ メッセージをコンソール セッションに表示できるようにする方法を示しています。***errors*** キーワードを使用することは、レベル 0、1、2、および 3 のメッセージを SSH および Telnet セッションに表示する必要があることを示しています。**terminal** コマンドを使用すると、現在のセッションにメッセージを表示できます。

```
hostname(config)# logging enable
hostname(config)# logging monitor errors
hostname(config)# terminal monitor
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging list	再使用可能なメッセージ選択基準リストを作成します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのロギング関連の部分を表示します。
terminal	端末回線のパラメータを設定します。

logging permit-hostdown

TCP ベースの syslog サーバの状態が新しいユーザ セッションとは無関係になるように指定するには、グローバル コンフィギュレーション モードで **logging permit-hostdown** コマンドを使用します。TCP ベースの syslog サーバが使用不能のときにセキュリティ アプライアンスが新しいユーザ セッションを拒否するように設定するには、このコマンドの **no** 形式を使用します。

logging permit-hostdown

no logging permit-hostdown

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトでは、TCP 接続を使用する syslog サーバへのロギングをイネーブルにした場合、何らかの理由で syslog サーバが使用不能になったときは、セキュリティ アプライアンスは新しいネットワーク アクセス セッションを許可しません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1) (1)	このコマンドが導入されました。

使用上のガイドライン

syslog サーバにメッセージを送信するためのロギング転送プロトコルとして TCP を使用する場合、セキュリティ アプライアンスは、syslog サーバに到達できないときは、セキュリティ保護手段として、新しいネットワーク アクセス セッションを拒否します。この制限を削除するには、**logging permit-hostdown** コマンドを使用します。

例

次の例では、TCP ベースの syslog サーバの状態が、セキュリティ アプライアンスが新しいセッションを許可するかどうかとは無関係になるように指定します。show running-config logging コマンドの出力に show running-config logging コマンドが含まれている場合、TCP ベースの syslog サーバの状態は新しいネットワーク アクセス セッションとは無関係になっています。

```
hostname(config)# logging permit-hostdown
hostname(config)# show running-config logging
logging enable
logging trap errors
logging host infrastructure 10.1.2.3 6/1470
logging permit-hostdown
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging host	syslog サーバを定義します。
logging trap	syslog サーバへのロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのロギング関連の部分を表示します。

logging queue

セキュリティ アプライアンスがロギング コンフィギュレーションに従って処理する前にシステム ログ メッセージ キューに保持できるシステム ログ メッセージの数を指定するには、グローバル コンフィギュレーション モードで **logging queue** コマンドを使用します。ロギング キューのサイズをデフォルトの 512 メッセージにリセットするには、このコマンドの **no** 形式を使用します。

logging queue *queue_size*

no logging queue *queue_size*

シンタックスの説明

queue_size	処理前に格納するためのキューに入れることができるシステム ログ メッセージの数。有効な値は 0 ～ 8,192 メッセージです。ロギング キューが 0 に設定されている場合、キューは設定可能な最大サイズ（8192 メッセージ）になります。

デフォルト

デフォルトのキュー サイズは 512 メッセージです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル 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
既存	このコマンドは既存のものです。

使用上のガイドライン

トラフィックが重いためにキューがいっぱいになった場合、セキュリティ アプライアンスはメッセージを廃棄することがあります。

例

次の例は、**logging queue** コマンドと **show logging queue** コマンドの出力を表示する方法を示しています。

```
hostname(config)# logging queue 0
hostname(config)# show logging queue
Logging Queue length limit : Unlimited
Current 5 msg on queue, 3513 msgs most on queue, 1 msg discard.
```

この例では、**logging queue** コマンドは 0 に設定されています。つまり、キューは最大サイズの 8192 に設定されています。キュー内のシステム ログ メッセージは、セキュリティ アプライアンスによって、ロギング コンフィギュレーションで指定される方法で処理されます。たとえば、システム ログ メッセージを電子メール受信者に送信する方法やフラッシュ メモリに保存する方法などがあります。

この例における **show logging queue** コマンドの出力は、キューにあるメッセージが 5 つ、セキュリティ アプライアンスが最後にブートされてから同時にキューに存在したメッセージの最大数が 3,513、廃棄されたメッセージが 1 つであることを表示しています。キューは無制限になるように設定されていましたが、メッセージをキューに追加するためのブロック メモリが使用できなかったため、メッセージは廃棄されました。

関連コマンド

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

logging rate-limit

システム ログ メッセージの生成レートを制限するには、特権 EXEC モードで **logging rate-limit** コマンドを使用します。レート制限をディセーブルにするには、特権 EXEC モードでこのコマンドの **no** 形式を使用します。

logging rate-limit {***unlimited*** | {*num* [*interval*]}} ***message*** *syslog_id* | ***level*** *severity_level*

[no] logging rate-limit [***unlimited*** | {*num* [*interval*]}} ***message*** *syslog_id*] ***level*** *severity_level*

シンタックスの説明

interval	（オプション）メッセージの生成レートの測定に使用される時間間隔（秒単位）。*interval* の有効値の範囲は 0 ～ 2,147,483,647 です。
level *severity_level*	設定されたレート制限を、特定の重大度に属するすべてのシステム ログ メッセージに適用します。指定された重大度のすべてのシステム ログ メッセージは、個別にレート制限されます。*severity_level* の有効な範囲は 1 ～ 7 です。
message	このシステム ログ メッセージのレポートを抑制します。
num	指定した時間間隔が経過するまでに生成できるシステム メッセージの数。*num* の有効値の範囲は 0 ～ 2,147,483,647 です。
syslog_id	抑制するシステム ログ メッセージの ID。*syslog_id* の有効値の範囲は 100000 ～ 999999 です。
unlimited	レート制限をディセーブルにします。これは、ロギング レートが制限されないことを意味します。

デフォルト

interval のデフォルト設定は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

使用上のガイドライン

システム メッセージの重大度は次のとおりです。

•0：システムが使用不可

•1：ただちに処置が必要

•2：クリティカルな状態

•3：エラー メッセージ

•4：警告メッセージ

•5：正常だが、注意が必要な状態

•6：情報

•7：デバッグ メッセージ

例

システム ログ メッセージの生成レートを制限するために、特定のメッセージ ID を入力できます。次の例は、特定のメッセージ ID および時間間隔を使用して、システム ログ メッセージの生成レートを制限する方法を示しています。

```
hostname(config)# logging rate-limit 100 600 message 302020
```

この例では、指定された 600 秒間隔でレート制限 100 に達すると、システム ログ メッセージ 302020 はホストに送信されなくなります。

システム ログ メッセージの生成レートを制限するために、特定の重大度を入力できます。次の例は、特定の重大度および時間間隔を使用して、システム ログ メッセージの生成レートを制限する方法を示しています。

```
hostname(config)# logging rate-limit 1000 600 level 6
```

この例では、重大度 6 のすべてのシステム ログ メッセージが、指定された 600 秒間隔で指定の生成レート 1000 に制限されます。重大度 6 の各システム ログ メッセージのレート制限は、1000 です。

関連コマンド

コマンド	説明
clear running-config logging rate-limit	ロギング レート制限の設定をデフォルトにリセットします。
show logging	内部バッファ内の現在のメッセージ、またはロギング コンフィギュレーションの設定を表示します。
show running-config logging rate-limit	現在のロギング レート制限の設定を表示します。

logging recipient-address

セキュリティ アプライアンスによって電子メールで送信されるシステム ログ メッセージの受信者の電子メール アドレスを指定するには、グローバル コンフィギュレーション モードで **logging recipient-address** コマンドを使用します。受信者の電子メール アドレスを削除するには、このコマンドの **no** 形式を使用します。受信者のアドレスは最大 5 つまで設定できます。必要に応じて、受信者のアドレスごとに、**logging mail** コマンドで指定されたメッセージ レベルとは別のレベルを指定できます。

logging recipient-address *address* [**level** *level*]

no logging recipient-address *address* [**level** *level*]

シンタックスの説明

address	システム ログ メッセージを電子メールで送信する場合の受信者の電子メール アドレスを指定します。
level	この後にロギング レベルが続くことを示します。
level	システム ログ メッセージの最大レベルを設定します。たとえば、レベルを 3 に設定すると、セキュリティ アプライアンスはレベル 3、2、1、および 0 のシステム ログ メッセージを生成します。次の数値または名前で指定できます。 • **0** または **emergencies**：システムが使用不能 • **1** または **alerts**：ただちに処置が必要 • **2** または **critical**：クリティカルな状態 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：正常だが、注意が必要な状態 • **6** または **informational**：情報 • **7** または **debugging**:デバッグ メッセージ、ログ FTP コマンド、WWW URL **（注）** **logging recipient-address** コマンドでは、3 より大きなレベルを使用することはお勧めできません。ロギング レベルを高くすると、バッファ オーバーフローによってシステム ログ メッセージがドロップされることがあります。 **logging recipient-address** コマンドで指定されたメッセージ レベルは、**logging mail** コマンドで指定されたメッセージ レベルを上書きします。たとえば、**logging recipient-address** コマンドでレベル 7 が指定された場合、**logging mail** コマンドでレベル 3 が指定されていたときは、セキュリティ アプライアンスはレベル 4、5、6、および 7 のメッセージを含むすべてのメッセージを受信者に送信します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1) (1)	このコマンドが導入されました。

使用上のガイドライン

システム ログ メッセージを電子メールで送信できるようにするには、**logging mail** コマンドを使用します。

logging recipient-address コマンドは最大 5 つまで設定できます。コマンドごとに、別々のロギング レベルを指定できます。この方法は、緊急性の高いメッセージを緊急性の低いメッセージよりも多くの受信者に送信する場合に便利です。

例

次の基準に従って、システム ログ メッセージを電子メールで送信するようにセキュリティ アプライアンスを設定します。

- critical、alerts、および emergencies のメッセージを送信する。
- メッセージを送信するときに、ciscosecurityappliance@example.com を送信者のアドレスとして使用する。
- メッセージを admin@example.com に送信する。
- SMTP を使用して、メッセージをプライマリ サーバ pri-smtp-host およびセカンダリ サーバ sec-smtp-host に送信する。

次のコマンドを入力します。

```
hostname(config)# logging mail critical
hostname(config)# logging from-address ciscosecurityappliance@example.com
hostname(config)# logging recipient-address admin@example.com
hostname(config)# smtp-server pri-smtp-host sec-smtp-host
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging from-address	電子メールで送信されるシステム ログ メッセージの送信元として表示する電子メール アドレスを指定します。
logging mail	セキュリティ アプライアンスがシステム ログ メッセージを電子メールで送信できるようにし、どのメッセージを電子メールで送信するかを決定します。
smtp-server	SMTP サーバを設定します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在動作しているロギング コンフィギュレーションを表示します。

logging savelog

ログ バッファをフラッシュ メモリに保存するには、特権 EXEC モードで **logging savelog** コマンドを使用します。

logging savelog [*savefile*]

シンタックスの説明

savefile	（オプション）保存するフラッシュ メモリ ファイルの名前。ファイル名が指定されない場合、セキュリティ アプライアンスは、次のように、デフォルトのタイムスタンプ形式を使用してファイルを保存します。 LOG-*YYYY-MM-DD-HHMMSS*.TXT *YYYY* は西暦年、*MM* は月、*DD* は日、*HHMMSS* は時刻の時、分、秒です。

デフォルト

デフォルトは次のとおりです。

- バッファのサイズは 4 KB です。
- フラッシュ メモリの最小空き容量は 3 MB です。
- バッファ ロギング用のフラッシュ メモリ最大割当量は、1 MB です。
- デフォルトのログ ファイル名は、上記の表のとおりです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

使用上のガイドライン

ログ バッファをフラッシュ メモリに保存するには、事前にバッファへのロギングをイネーブルにしておく必要があります。このようにしないと、フラッシュ メモリに保存するデータがログ バッファに保持されません。バッファへのロギングをイネーブルにするには、**logging buffered** コマンドを使用します。

（注）　**logging savelog** コマンドは、バッファを消去しません。バッファを消去するには、**clear logging buffer** コマンドを使用します。

例

次の例では、ロギングとログ バッファをイネーブルにし、グローバル コンフィギュレーション モードを終了し、latest-logfile.txt というファイル名を使用してログ バッファをフラッシュ メモリに保存します。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# exit
hostname# logging savelog latest-logfile.txt
hostname#
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファが保持しているシステム ログ メッセージをすべて消去します。
copy	ファイルを、ある位置から TFTP サーバや FTP サーバなどの別の位置にコピーします。
delete	保存済みログ ファイルなどのファイルを、ディスク パーティションから削除します。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。

logging standby

フェールオーバー スタンバイ セキュリティ アプライアンスがこのセキュリティ アプライアンスのシステム ログ メッセージをロギング先に送信できるようにするには、グローバル コンフィギュレーション モードで **logging standby** コマンドを使用します。syslog および SNMP ロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

logging standby

no logging standby

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

logging standby コマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル 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
既存	このコマンドは既存のものです。

使用上のガイドライン

logging standby をイネーブルにすると、フェールオーバーが発生しても、フェールオーバー スタンバイ セキュリティ アプライアンスのシステム ログ メッセージが同期されたままになることが保証されます。

（注）　**logging standby** コマンドを使用すると、syslog サーバ、SNMP サーバ、および FTP サーバなどの共有ロギング先に対するトラフィックが 2 倍になります。

例

次の例では、セキュリティ アプライアンスがシステム ログ メッセージをフェールオーバー スタンバイ セキュリティ アプライアンスに送信できるようにします。**show logging** コマンドの出力は、この機能がイネーブルになっていることを示しています。

```
hostname(config)# logging standby
hostname(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: enabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: disabled
    History logging: disabled
    Device ID: 'inside' interface IP address "10.1.1.1"
    Mail logging: disabled
    ASDM logging: disabled
```

関連コマンド

コマンド	説明
failover	フェールオーバー機能をイネーブルにします。
logging enable	ロギングをイネーブルにします。
logging host	syslog サーバを定義します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのロギング関連の部分を表示します。

logging timestamp

システム ログ メッセージにメッセージの生成日時を含めるよう指定するには、グローバル コンフィギュレーション モードで **logging timestamp** コマンドを使用します。システム ログ メッセージから日時を削除するには、このコマンドの **no** 形式を使用します。

logging timestamp

no logging timestamp

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

セキュリティ アプライアンスは、デフォルトでは、日時をシステム ログ メッセージに含めません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

logging timestamp コマンドは、セキュリティ アプライアンスがすべてのシステム ログ メッセージにタイムスタンプを含めるように指定します。

例

次の例では、すべてのシステム ログ メッセージにタイムスタンプ情報を含めることをイネーブルにします。

```
hostname(config)# logging enable
hostname(config)# logging timestamp
hostname(config)#
```

関連コマンド

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

logging trap

セキュリティ アプライアンスが syslog サーバに送信するシステム ログ メッセージを指定するには、グローバル コンフィギュレーション モードで **logging trap** コマンドを使用します。このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

logging trap [*logging_list* | *level*]

no logging trap

シンタックスの説明

level	システム ログ メッセージの最大レベルを設定します。たとえば、レベルを 3 に設定すると、セキュリティ アプライアンスはレベル 3、2、1、および 0 のシステム ログ メッセージを生成します。次の数値または名前で指定できます。 • **0** または **emergencies**：システムが使用不能 • **1** または **alerts**：ただちに処置が必要 • **2** または **critical**：クリティカルな状態 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：正常だが、注意が必要な状態 • **6** または **informational**：情報 • **7** または **debugging**:デバッグ メッセージ、ログ FTP コマンド、WWW URL
logging_list	syslog サーバに送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

デフォルト

デフォルトの syslog トラップは定義されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル 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
既存	このコマンドは既存のものです。

使用上のガイドライン

ロギング転送プロトコルとして TCP を使用する場合、セキュリティ アプライアンスが syslog サーバに到達できないとき、syslog サーバが誤って設定されているとき、またはディスクがいっぱいのときは、セキュリティ アプライアンスはセキュリティ保護手段として、新しいネットワーク アクセス セッションを拒否します。

UDP ベースのロギングは、syslog サーバに障害が発生しても、セキュリティ アプライアンスによるトラフィックの送信を妨げません。

例

次の例は、内部インターフェイス上にあってデフォルトのプロトコルとポート番号を使用する syslog サーバに対して、レベル 0、1、2、および 3 のシステム ログ メッセージを送信する方法を示しています。

```
hostname(config)# logging enable
hostname(config)# logging host inside 10.2.2.3
hostname(config)# logging trap errors
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging host	syslog サーバを定義します。
logging list	再使用可能なメッセージ選択基準リストを作成します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのロギング関連の部分を表示します。

login

ローカル ユーザ データベースを使用して特権 EXEC モードに入る場合や、ユーザ名を変更する場合は、ユーザ EXEC モードで **login** コマンドを使用します。

login

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

login コマンドを使用すると、ユーザ EXEC モードから特権 EXEC モードに、ローカル データベース内の任意のユーザ名としてログインできます。イネーブル認証をオンにした場合、**login** コマンドは **enable** コマンドと類似したものになります（**aaa authentication console** コマンドを参照）。ただし、イネーブル認証とは異なり、**login** コマンドはローカル ユーザ名データベースのみを使用できます。このコマンドでは、常に認証が要求されます。また、**login** コマンドを使用すると、任意の CLI モードからユーザを変更できます。

ユーザがログイン時に特権 EXEC モード（およびすべてのコマンド）にアクセスできるようにするには、ユーザの特権レベルを 2（デフォルト）～ 15 に設定します。ローカル コマンド認可を設定した場合、ユーザは、その特権レベル以下のレベルに割り当てられているコマンドのみを入力できます。詳細については、**aaa authorization コマンド**を参照してください。

注意　CLI にアクセスできるユーザや特権 EXEC モードに入らせないようにするユーザをローカル データベースに追加する場合は、コマンド認可を設定する必要があります。コマンド認可が設定されていない場合、ユーザは、特権レベルが 2 以上（2 がデフォルト）であれば、各自のパスワードを使用して CLI で特権 EXEC モード（およびすべてのコマンド）にアクセスできます。または、RADIUS または TACACS+ 認証を使用することもできます。あるいは、すべてのローカル ユーザをレベル 1 に設定して、システムのイネーブル パスワードを使用して特権 EXEC モードにアクセスできるユーザを制御することもできます。

例

次の例では、**login** コマンドを入力した後のプロンプトを示します。

```
hostname> login
Username:
```

関連コマンド

コマンド	説明
aaa authorization command	CLI アクセスのコマンド認可をイネーブルにします。
aaa authentication console	コンソール、Telnet、HTTP、SSH、または **enable** コマンド アクセスに対して認証を要求します。
logout	CLI からログアウトします。
username	ユーザをローカル データベースに追加します。

login-button

WebVPN ユーザがセキュリティ アプライアンスに接続するときに表示される WebVPN ページのログイン ボックスの Login ボタンをカスタマイズするには、webvpn カスタマイゼーション モードで **login-button** コマンドを使用します。

login-button {**text** | **style**} *value*

[**no**] **login-button** {**text** | **style**} *value*

このコマンドをコンフィギュレーションから削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

シンタックスの説明

text	テキストを変更することを指定します。
style	スタイルを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

デフォルトの Login ボタンのテキストは「Login」です。

デフォルトの Login ボタンのスタイルは、次のとおりです。

border: 1px solid black;background-color:white;font-weight:bold; font-size:80%

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは、有効な Cascading Style Sheet（CSS）パラメータとして表現されます。このパラメータの説明は、このマニュアルでは取り扱いません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト www.w3.org の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手可能です。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）について 0 ～ 255 の範囲で 10 進値を入力します。このカンマ区切りのエントリは、他の 2 色と混合する各色の輝度のレベルを示しています。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番目は赤を、3 番目と 4 番目は緑を、5 番目と 6 番目は青を表しています。

（注） WebVPN ページを簡単にカスタマイズするには、ASDM を使用することをお勧めします。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するのに便利な機能があります。

例

次の例では、Login ボタンのテキストを「OK」にカスタマイズします。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# login-button text OK
```

関連コマンド

コマンド	説明
login-title	WebVPN ページのログイン ボックスのタイトルをカスタマイズします。
group-prompt	WebVPN ページのログイン ボックスのグループ プロンプトをカスタマイズします。
password-prompt	WebVPN ページのログイン ボックスのパスワード プロンプトをカスタマイズします。
username-prompt	WebVPN ページのログイン ボックスのユーザ名プロンプトをカスタマイズします。

login-message

WebVPN ユーザがセキュリティ アプライアンスに接続するときに表示される WebVPN ページのログイン メッセージをカスタマイズするには、webvpn カスタマイゼーション モードで **login-message** コマンドを使用します。

login-message {**text** | **style**} *value*

[**no**] **login-message** {**text** | **style**} *value*

このコマンドをコンフィギュレーションから削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

シンタックスの説明

text	テキストを変更することを指定します。
style	スタイルを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

デフォルトのログイン メッセージは「Please enter your username and password」です。

デフォルトのログイン メッセージのスタイルは、background-color:#CCCCCC;color:black です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは、有効な Cascading Style Sheet（CSS）パラメータとして表現されます。このパラメータの説明は、このマニュアルでは取り扱いません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト www.w3.org の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手可能です。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）について 0 ～ 255 の範囲で 10 進値を入力します。このカンマ区切りのエントリは、他の 2 色と混合する各色の輝度のレベルを示しています。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番目は赤を、3 番目と 4 番目は緑を、5 番目と 6 番目は青を表しています。

（注）　WebVPN ページを簡単にカスタマイズするには、ASDM を使用することをお勧めします。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するのに便利な機能があります。

例

次の例では、ログイン メッセージのテキストを「username and password」に設定します。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# login-message text username and password
```

関連コマンド

コマンド	説明
login-title	WebVPN ページのログイン ボックスのタイトルをカスタマイズします。
username-prompt	WebVPN ページのログイン ボックスのユーザ名プロンプトをカスタマイズします。
password-prompt	WebVPN ページのログイン ボックスのパスワード プロンプトをカスタマイズします。
group-prompt	WebVPN ページのログイン ボックスのグループ プロンプトをカスタマイズします。

login-title

WebVPN ユーザに表示される WebVPN ページのログイン ボックスのタイトルをカスタマイズするには、webvpn カスタマイゼーション モードで **login-title** コマンドを使用します。

login-title {**text** | **style**} *value*

[**no**] **login-title** {**text** | **style**} *value*

このコマンドをコンフィギュレーションから削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

シンタックスの説明

text	テキストを変更することを指定します。
style	HTML スタイルを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

デフォルトのログイン テキストは「Login」です。

ログイン タイトルのデフォルト HTML スタイルは、background-color: #666666; color: white です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは、有効な Cascading Style Sheet（CSS）パラメータとして表現されます。このパラメータの説明は、このマニュアルでは取り扱いません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト www.w3.org の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手可能です。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）について 0 ～ 255 の範囲で 10 進値を入力します。このカンマ区切りのエントリは、他の 2 色と混合する各色の輝度のレベルを示しています。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番目は赤を、3 番目と 4 番目は緑を、5 番目と 6 番目は青を表しています。

（注）　WebVPN ページを簡単にカスタマイズするには、ASDM を使用することをお勧めします。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するのに便利な機能があります。

例

次の例では、ログイン タイトルのスタイルを設定します。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# login-title style background-color:
rgb(51,51,255);color: rgb(51,51,255); font-family: Algerian; font-size: 12pt;
font-style: italic; font-weight: bold
```

関連コマンド

コマンド	説明
login-message	WebVPN ページのログイン メッセージをカスタマイズします。
username-prompt	WebVPN ページのログイン ボックスのユーザ名プロンプトをカスタマイズします。
password-prompt	WebVPN ページのログイン ボックスのパスワード プロンプトをカスタマイズします。
group-prompt	WebVPN ページのログイン ボックスのグループ プロンプトをカスタマイズします。

logo

WebVPN ユーザがセキュリティ アプライアンスに接続するときに表示される WebVPN ページのロゴをカスタマイズするには、webvpn カスタマイゼーション モードで **logo** コマンドを使用します。

logo {**none** | **file** {*path value*}}
[**no**] **logo** {**none** | **file** {*path value*}}

シンタックスの説明

none	ロゴを使用しないことを指定します。ヌル値を設定して、ロゴを拒否します。ロゴを継承しないようにします。
file	ロゴを含むファイルを指定することを示します。
path	ファイル名のパス。可能なパスは disk0:、disk1:、または flash: です。
value	ロゴのファイル名を指定します。最大長は 255 文字です（スペースは含めません）。ファイル タイプには JPG、PNG、または GIF を指定し、サイズは 100 KB 未満にする必要があります。

デフォルト

デフォルトのロゴは、シスコのロゴです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

ロゴをコンフィギュレーションから削除してデフォルト（シスコのロゴ）にリセットするには、このコマンドの **no** 形式を使用します。

ロゴを削除するには、**logo none** コマンドを使用します。

指定したファイル名が存在しない場合は、エラー メッセージが表示されます。ロゴ ファイルを削除した場合、コンフィギュレーションが引き続きそのファイルを指していても、ロゴは表示されません。

ファイル名にスペースを含めることはできません。

例

次の例では、cisco_logo.gif というファイルにカスタム ロゴが含まれています。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)#logo file disk0:cisco_logo.gif
```

関連コマンド

コマンド	説明
title	WebVPN ページのタイトルをカスタマイズします。
page style	Cascading Style Sheet（CSS）パラメータを使用して WebVPN ページをカスタマイズします。

logout

CLI を終了するには、ユーザ EXEC モードで **logout** コマンドを使用します。

logout

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトの動作や値はありません。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン　**logout** コマンドを使用すると、セキュリティ アプライアンスからログアウトできます。ユーザ モードに戻るには、**exit** コマンドまたは **quit** コマンドを使用します。

例　次の例は、セキュリティ アプライアンスからログアウトする方法を示しています。

```
hostname> logout
```

関連コマンド

コマンド	説明
login	ログイン プロンプトを開始します。
exit	アクセス モードを終了します。
quit	コンフィギュレーション モードまたは特権モードを終了します。

logout-message

WebVPN ユーザが WebVPN サービスからログアウトするときに表示される WebVPN ログアウト画面のログアウト メッセージをカスタマイズするには、webvpn カスタマイゼーション モードで **logout-message** コマンドを使用します。

logout-message {**text** | **style**} *value*

[**no**] **logout-message** {**text** | **style**} *value*

このコマンドをコンフィギュレーションから削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

シンタックスの説明

text	テキストを変更することを指定します。
style	スタイルを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

デフォルトのログアウト メッセージのテキストは「Goodbye」です。

デフォルトのログアウト メッセージのスタイルは、background-color:#999999;color:black です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは、有効な Cascading Style Sheet（CSS）パラメータとして表現されます。このパラメータの説明は、このマニュアルでは取り扱いません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト www.w3.org の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手可能です。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）について 0 ～ 255 の範囲で 10 進値を入力します。このカンマ区切りのエントリは、他の 2 色と混合する各色の輝度のレベルを示しています。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番目は赤を、3 番目と 4 番目は緑を、5 番目と 6 番目は青を表しています。

（注）　WebVPN ページを簡単にカスタマイズするには、ASDM を使用することをお勧めします。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するのに便利な機能があります。

例

次の例では、ログアウト メッセージのスタイルを設定します。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# logout-message style background-color:
rgb(51,51,255);color: rgb(51,51,255); font-family: Algerian; font-size: 12pt;
font-style: italic; font-weight: bold
```

関連コマンド

コマンド	説明
logout-title	WebVPN ページのログアウト タイトルをカスタマイズします。
group-prompt	WebVPN ページのログイン ボックスのグループ プロンプトをカスタマイズします。
password-prompt	WebVPN ページのログイン ボックスのパスワード プロンプトをカスタマイズします。
username-prompt	WebVPN ページのログイン ボックスのユーザ名プロンプトをカスタマイズします。