log – lz

- log （3 ページ）
- log-adjacency-changes （5 ページ）
- log-adj-changes （9 ページ）
- log-adjacency-changes （11 ページ）
- logging asdm （13 ページ）
- logging asdm-buffer-size （16 ページ）
- logging buffered （18 ページ）
- logging buffer-size （21 ページ）
- logging class （23 ページ）
- logging console （27 ページ）
- logging debug-trace （29 ページ）
- logging debug-trace persistent （31 ページ）
- logging device-id （33 ページ）
- logging emblem （36 ページ）
- logging enable （38 ページ）
- logging facility （40 ページ）
- logging flash-bufferwrap （42 ページ）
- logging flash-maximum-allocation （44 ページ）
- logging flash-minimum-free （46 ページ）
- logging flow-export-syslogs （48 ページ）
- logging from-address （50 ページ）
- logging ftp-bufferwrap （52 ページ）
- logging ftp-server （54 ページ）
- logging hide username （56 ページ）
- logging history （58 ページ）
- logging host （61 ページ）
- logging list （65 ページ）
- logging mail （69 ページ）
- logging message （72 ページ）
- logging message standby （75 ページ）

- logging monitor （77 ページ）
- logging permit-hostdown （79 ページ）
- logging queue （81 ページ）
- logging rate-limit （83 ページ）
- logging recipient-address （87 ページ）
- logging savelog （91 ページ）
- logging standby （93 ページ）
- logging timestamp （95 ページ）
- logging trap （97 ページ）
- login （99 ページ）
- login-button （101 ページ）
- login-message （103 ページ）
- login-title （105 ページ）
- logo （107 ページ）
- logout （109 ページ）
- logout-message （110 ページ）
- lsp-full suppress （112 ページ）
- lsp-gen-interval （117 ページ）
- lsp-refresh-interval （122 ページ）

log

モジュラ ポリシー フレームワークを使用する場合は、一致またはクラスコンフィギュレーション モードで **log** コマンドを使用して、**match** コマンドまたはクラスマップと一致するパケットをログに記録します。このログアクションは、アプリケーション トラフィックのインスペクション ポリシー マップ（**policy-map type inspect** コマンド）で利用できます。このアクション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。

log
nolog

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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド 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。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
一致コンフィギュレーションおよびクラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

インスペクション ポリシー マップは、1 つ以上の **match** コマンドと **class** コマンドで構成されます。インスペクション ポリシー マップで使用できる実際のコマンドは、アプリケーションによって異なります。**match** コマンドまたは **class** コマンドを入力してアプリケーション トラフィックを指定した後（**class** コマンドは、**match** コマンドを含む既存の **class-map type inspect** コマンドを参照します）、**log** コマンドを入力して、**match** コマンドまたは **class** コマンドに一致するすべてのパケットをログに記録できます。

レイヤ 3/4 ポリシー マップ（**policy-map** コマンド）で **inspect** コマンドを使用してアプリケーション インスペクションをイネーブルにする場合、このアクションを含むインスペクション ポリシー マップをイネーブルにできます。たとえば、**inspect http http_policy_map** コマンドを入力します。http_policy_map は、インスペクション ポリシー マップの名前です。

例

次に、パケットが http-traffic クラス マップに一致する場合にログを送信する例を示します。

```
ciscoasa(config-cmap)# policy-map type inspect http http-map1
ciscoasa(config-pmap)# class http-traffic
ciscoasa(config-pmap-c)# log
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
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。

log-adjacency-changes

NLSP IS-IS 隣接がステートを変更（アップまたはダウン）する際に IS-IS が syslog メッセージを送信することを可能にするには、ルータ ISIS コンフィギュレーション モードで **log-adjacency-changes** コマンドを使用します。この機能をオフにするには、このコマンドの **no** 形式を使用します。

log-adjacency-changes [**all**]
no log-adjacency-changes [**all**]

構文の説明

all	（オプション）non_IIH イベントによって生成される変更を含みます。

コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。

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。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
IPv6 ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドにより、IS-IS 隣接のステート変更のモニタリングが可能になります。これは、大規模なネットワークをモニタリングする場合に非常に役立つことがあります。メッセージは、システム エラー メッセージ機能を使用してロギングされます。メッセージは次の形式になります。

```
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Up, new adjacency
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Down, hold time expired
```

例

次に、隣接の変更をログに記録するように ルータ に指示する例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# log-adjacency-changes
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
authentication key	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。

コマンド	説明
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更（アップまたはダウン）する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。

コマンド	説明
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト（TLV）を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

log-adj-changes

OSPF ネイバーが起動または停止したときに syslog メッセージを送信するようにルータを設定するには、ルータ コンフィギュレーション モードで **log-adj-changes** コマンドを使用します。この機能をオフにするには、このコマンドの **no** 形式を使用します。

log-adj-changes [**detail**]
no log-adj-changes [**detail**]

構文の説明

detail （任意）ネイバーが起動または停止した場合だけでなく、状態が変わるたびに syslog メッセージを送信します。

コマンド デフォルト

このコマンドは、デフォルトでイネーブルになっています。

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。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

log-adj-changes コマンドはデフォルトで有効になっているため、コマンドの **no** 形式を指定して削除しない限り、実行コンフィギュレーションに表示されます。

例

次に、OSPF ネイバーが起動または停止したときに syslog メッセージを送信しないようにする例を示します。

```
ciscoasa(config)# router ospf 5
ciscoasa(config-router)# no log-adj-changes
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードを開始します。
show ospf	OSPF ルーティング プロセスに関する一般情報を表示します。

log-adjacency-changes

OSPFv3 ネイバーが起動または停止したときに syslog メッセージを送信するようにルータを設定するには、IPv6 ルータ コンフィギュレーション モードで **log-adjacency-changes** コマンドを使用します。この機能をオフにするには、このコマンドの **no** 形式を使用します。

log-adjacency-changes [**detail**]
no log-adjacency-changes [**detail**]

構文の説明

detail （任意）ネイバーが起動または停止した場合だけでなく、状態が変わるたびに syslog メッセージを送信します。

コマンド デフォルト

このコマンドは、デフォルトでイネーブルになっています。

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。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

log-adjacency-changes コマンドはデフォルトで有効になっているため、コマンドの **no** 形式を指定して削除しない限り、実行コンフィギュレーションに表示されます。

例

次に、OSPFv3 ネイバーが起動または停止したときに syslog メッセージを送信しないようにする例を示します。

```
ciscoasa(config)# ipv6
 router ospf 5
ciscoasa(config-router)# no log-adjacency-changes
```

関連コマンド

コマンド	説明
ipv6 router ospf	ルータ 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 ipv6 ospf	OSPFv3 ルーティング プロセスに関する一般情報を表示します。

logging asdm

syslog メッセージを ASDM ログバッファに送信するには、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無効にするには、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*]

構文の説明

level syslog メッセージの最大重大度を設定します。たとえば、重大度を 3 に設定すると、ASA は重大度 3、2、1、0 の syslog メッセージを生成します。次のように、数値または名前のいずれかを指定できます。

- **0** または **emergencies**：システムが使用不能。
- **1** または **alerts**：すぐに対処が必要。
- **2** または **critical**：重大な状態。
- **3** または **errors**：エラー状態。
- **4** または **warnings**：警告状態。
- **5** または **notifications**：通常の状態だが、重要な状態。
- **6** または **informational**：Informational（情報提供）メッセージ。
- **7** または **debugging**：Debug（デバッグ）メッセージ。

（注） 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、**debugging** 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。また、このコマンドは、ネットワークトラフィックやユーザーが少ない時間帯に使用してください。デバッギングをこのような時間帯に行うと、システムの使用に影響が及ぶ処理のオーバーヘッドが増加する可能性が低くなります。

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。

コマンド デフォルト

ASDM ロギングはデフォルトで無効になっています。

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。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

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有効にしておく必要があります。

ASDM ログバッファがいっぱいになると、ASA 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領域をバッファに確保します。ASDM ログバッファに保持される syslog メッセージの数を制御するには、**logging asdm-buffer-size** コマンドを使用します。

ASDM ログバッファは、**logging buffered** コマンドで有効にするログバッファとは異なります。

例

次に、ロギングを有効にして、ASDM に重大度 0、1、および 2 のログバッファメッセージを送信し、ASDM ログバッファのサイズを 200 メッセージに設定する例を示します。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging asdm 2
ciscoasa(config)# logging asdm-buffer-size 200
ciscoasa(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 ログバッファから、保持されているすべてのメッセージをクリアします。

コマンド	説明
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	メッセージ選択基準の再使用可能な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	ロギング設定を表示します。

logging asdm-buffer-size

ASDM ログバッファに保持される syslog メッセージの数を指定するには、グローバル コンフィギュレーション モードで **logging asdm-buffer-size** コマンドを使用します。ASDM ログバッファをデフォルトのサイズの 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。

loggingasdm-buffer-size*num_of_msgs*
no logging asdm-buffer-size *num_of_msgs*

構文の説明

num_of_msgs	ASA によって ASDM ログバッファに保持される syslog メッセージの数を指定します。

コマンド デフォルト

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

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ASDM ログバッファがいっぱいになると、ASA 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領域をバッファに確保します。ASDM ログバッファへのロギングを有効にするかどうかを制御する、または ASDM ログバッファに保持される syslog メッセージの種類を制御するには、**logging asdm** コマンドを使用します。

ASDM ログバッファは、**logging buffered** コマンドで有効にするログバッファとは異なります。

例

次に、ロギングを有効にして、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し、ASDM ログバッファのサイズを 200 メッセージに設定する例を示します。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging asdm 2
```

```
ciscoasa(config)# logging asdm-buffer-size 200
ciscoasa(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 ログバッファから、保持されているすべてのメッセージをクリアします。
logging asdm	ASDM ログバッファへのロギングを有効にします。
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	現在実行中のロギング コンフィギュレーションを表示します。

logging buffered

ASA から syslog メッセージをログバッファに送信できるようにするには、グローバル コンフィギュレーション モードで **logging buffered** コマンドを使用します。ログバッファへのロギングを無効にするには、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*]

構文の説明

level syslog メッセージの最大重大度を設定します。たとえば、重大度を 3 に設定すると、ASA は重大度 3、2、1、0 の syslog メッセージを生成します。次のように、数値または名前のいずれかを指定できます。

- **0** または **emergencies**：システムが使用不能。
- **1** または **alerts**：すぐに対処が必要。
- **2** または **critical**：重大な状態。
- **3** または **errors**：エラー状態。
- **4** または **warnings**：警告状態。
- **5** または **notifications**：通常の状態だが、重要な状態。
- **6** または **informational**：Informational（情報提供）メッセージ。
- **7** または **debugging**：Debug（デバッグ）メッセージ。

（注） 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、**debugging** 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。また、このコマンドは、ネットワークトラフィックやユーザーが少ない時間帯に使用してください。デバッギングをこのような時間帯に行うと、システムの使用に影響が及ぶ処理のオーバーヘッドが増加する可能性が低くなります。

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。

コマンド デフォルト

デフォルトの設定は次のとおりです。

- バッファへのロギングはディセーブルです。
- バッファ 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。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

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有効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、ASA によってバッファがクリアされてから、メッセージの追加が続行されます。ログバッファがいっぱいになると、ASA によって最も古いメッセージが削除されて、バッファに新しいメッセージ用の領域が確保されます。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** および **logging ftp-bufferwrap** コマンドを参照してください。

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

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

例

次に、重大度レベルが 0 および 1 のイベントに対して、バッファへのロギングを設定する例を示します。

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

次の例では、最大重大度 7 の「notif-list」というリストを作成し、「notif-list」リストで識別される syslog メッセージに対して、バッファへのロギングを設定します。

```
ciscoasa(config)# logging list notif-list level 7
ciscoasa(config)# logging buffered notif-list
ciscoasa(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 syslog メッセージをすべて消去します。
logging buffer-size	ログ バッファ 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 list	メッセージ選択基準の再使用可能な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。

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。ログバッファをメモリの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。

loggingbuffer-size*bytes*
no logging buffer-size *bytes*

構文の説明

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、8192 を指定した場合、ASA によってログバッファに 8 KB のメモリが使用されます。

コマンド デフォルト

デフォルトのログ バッファ サイズは 4 KB のメモリです。

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。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

デフォルトのバッファサイズと異なるサイズのログバッファが ASA によって使用されているか確認するには、**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、ASA によって 4 KB のログバッファが使用されています。

ASA 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

次に、ロギングを有効にし、ロギングバッファを有効にし、ログバッファ用に 16 KB のメモリが ASA で使用されることを指定する例を示します。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging buffer-size 16384
ciscoasa(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 syslog 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ている場合に、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。

logging class

メッセージクラスに対して、ロギング先ごとの最大重大度を設定するには、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重大度レベル構成を削除するには、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*

構文の説明

class	ロギング先ごとに最大重大度レベルを設定するメッセージ クラスを指定します。*class* の有効な値については、「使用上のガイドライン」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。ロギング先について、*destination* に送信される最大重大度レベルは *level* によって決まります。*destination* の有効な値については、後述する「使用上のガイドライン」を参照してください。
level	syslog メッセージの最大重大度を設定します。たとえば、重大度を 3 に設定すると、ASA は重大度 3、2、1、0 の syslog メッセージを生成します。次のように、数値または名前のいずれかを指定できます。 • **0** または **emergencies**：システムが使用不能。 • **1** または **alerts**：すぐに対処が必要。 • **2** または **critical**：重大な状態。 • **3** または **errors**：エラー状態。 • **4** または **warnings**：警告状態。 • **5** または **notifications**：通常の状態だが、重要な状態。 • **6** または **informational**：Informational（情報提供）メッセージ。 • **7** または **debugging**：Debug（デバッグ）メッセージ。 （注） 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、**debugging** 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。また、このコマンドは、ネットワークトラフィックやユーザーが少ない時間帯に使用してください。デバッギングをこのような時間帯に行うと、システムの使用に影響が及ぶ処理のオーバーヘッドが増加する可能性が低くなります。

コマンド デフォルト

ASA のデフォルトでは、重大度レベルはロギング先およびメッセージクラスに基づいて適用されません。代わりに、イネーブルにされた各ロギング先では、logging list で決定された重大度

レベル、または各ロギング先をイネーブルにしたときに指定された重大度レベルで、すべてのクラスに対するメッセージが受信されます。

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。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
8.0(2)	有効な class の値に **eigrp** オプションが追加されました。
8.2(1)	有効な class の値に **dap** オプションが追加されました。
9.12(1)	有効な class の値に **bfd, bgp, idb, ipv6, multicast, routing, object-group-search, pbr, sla** オプションが追加されました。

使用上のガイドライン

class の有効な値は次のとおりです。

- **auth**：ユーザー認証。
- **bfd**：BFD ルーティング
- **bgp**：BGP ルーティング
- **bridge**：トランスペアレント 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。
- **dap—**：ダイナミック アクセス ポリシー。
- **eap**：Extensible Authentication Protocol（EAP; 拡張可能認証プロトコル）。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、EAP セッション状態の変更、EAP ステータスのクエリー イベントといったタイプのイベント、および EAP ヘッダーおよびパケット内容の 16 進ダンプをログに記録します。
- **eapoudp**：拡張可能認証プロトコル（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 EAPoUDP のイベントをログに記録し、EAPoUDP ヘッダーおよびパケット内容の完全な記録を生成します。

- **eigrp**：EIGRP ルーティング。
- **email**：電子メールプロキシ。
- **ha**：フェールオーバー。
- **idb**：インターフェイス
- **ids**：侵入検知システム。
- **ip**：IP スタック。
- **ipaa—**IP アドレスの割り当て
- **ipv6**：IPv6 スタック
- **multicast**：マルチキャストルーティング
- **nac**：ネットワークアドミッションコントロール。初期化、例外リスト照合、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 適用、および再評価といったタイプのイベントのログを記録します。
- **np**：ネットワークプロセッサ。
- **object-group-search**：オブジェクトグループの検索
- **ospf**：OSPF ルーティング。
- **pbr**：ポリシーベースルーティング
- **rip**：RIP ルーティング。
- **rm**：Resource Manager。
- **routing**：すべてのルーティング
- **session**：ユーザーセッション。
- **sla**：SLA オブジェクトトラッキング
- **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**：この宛先については、**logging asdm** コマンドを参照してください。
- **buffered**：この宛先については、**logging buffered** コマンドを参照してください。

- **console**：この宛先については、**logging console** コマンドを参照してください。
- **history**：この宛先については、**logging history** コマンドを参照してください。
- **mail**：この宛先については、**logging mail** コマンドを参照してください。
- **monitor**：この宛先については、**logging monitor** コマンドを参照してください。
- **trap**：この宛先については、**logging trap** コマンドを参照してください。

例

次に、フェールオーバー関連のメッセージについて、ASDM ログ バッファの最大重大度が 2 で、syslog バッファの最大重大度が 7 であることを指定する例を示します。

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

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グ関連部分を表示します。

logging console

ASA で syslog メッセージをコンソールセッションに表示できるようにするには、グローバル コンフィギュレーション モードで **logging console** コマンドを使用します。コンソールセッションへの syslog メッセージの表示を無効にするには、このコマンドの **no** 形式を使用します。

logging console [*logging_list* | *level*]
nologgingconsole

（注） バッファ オーバーフローによって数多くの syslog メッセージがドロップされる可能性があるため、このコマンドは使用しないことを推奨します。詳細については、「使用上のガイドライン」セクションを参照してください。

構文の説明

level syslog メッセージの最大重大度を設定します。たとえば、重大度を 3 に設定すると、ASA は重大度 3、2、1、0 の syslog メッセージを生成します。次のように、数値または名前のいずれかを指定できます。

- **0** または **emergencies**：システムが使用不能。
- **1** または **alerts**：すぐに対処が必要。
- **2** または **critical**：重大な状態。
- **3** または **errors**：エラー状態。
- **4** または **warnings**：警告状態。
- **5** または **notifications**：通常の状態だが、重要な状態。
- **6** または **informational**：Informational（情報提供）メッセージ。
- **7** または **debugging**：Debug（デバッグ）メッセージ。

（注） 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、**debugging** 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。また、このコマンドは、ネットワークトラフィックやユーザーが少ない時間帯に使用してください。デバッギングをこのような時間帯に行うと、システムの使用に影響が及ぶ処理のオーバーヘッドが増加する可能性が低くなります。

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。

コマンド デフォルト

デフォルトでは、ASA によって syslog メッセージはコンソールセッションに表示されません。

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。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

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有効にする必要があります。

⚠

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 コマンド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ます。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クリアします。

例

次に、重大度レベル 0、1、2、および 3 の syslog メッセージをコンソール セッションに表示できるようにする例を示します。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging console errors
ciscoasa(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	メッセージ選択基準の再使用可能な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グ関連部分を表示します。

logging debug-trace

デバッグメッセージを重大度レベル 7 で発行される 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。デバッグメッセージのログへ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。

loggingdebug-trace
nologgingdebug-trace

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。

コマンド デフォルト

ASA のデフォルトでは、デバッグ出力は syslog メッセージに含まれません。

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。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

デバッグ メッセージは重大度レベル 7 のメッセージとして生成されます。syslog メッセージ番号 711001 でログに表示されますが、モニタリング セッションには表示されません。

例

次に、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例を示します。

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

次に、ログに表示されるデバッグ メッセージの出力例を示します。

```
%ASA-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グ関連部分を表示します。

logging debug-trace persistent

特定のセッションでアクティブなデバッグ syslog をセッションの終了後もログに記録されるようにするには、グローバル コンフィギュレーション モードで **logging debug-trace persistent** コマンドを使用します。特定の永続的なデバッグ設定を無効にするには、このコマンドの **no** 形式を使用します。これにより、ローカルセッションと永続的なデバッグからエントリがクリアされます。

loggingdebug-tracepersistent
nologgingdebug-tracepersistent

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。

コマンド デフォルト

デフォルトでは、セッションが終了すると、その特定のセッションでイネーブルになっているすべてのデバッグ コマンドが設定から削除され、syslog サーバーにログが記録されなくなります。

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。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

logging debug-trace persistent コマンドがイネーブルになっている場合、セッションで入力されたデバッグ コマンドはグローバルに保存され、すべてのセションで表示できます。このコマンドは、実行コンフィギュレーションに保存され、再起動後も保持されます。

例

次に、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 アクティビティの永続的なデバッグをオンにする例を示します。

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

次に、ログに表示されるデバッグ メッセージの出力例を示します。

```
%ASA-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グ関連部分を表示します。

logging device-id

EMBLEM 形式でない syslog メッセージにデバイス ID を含めるように ASA 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 の使用を無効にするには、このコマンドの **no** 形式を使用します。

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

構文の説明

cluster-id	クラスタにある個別の ASA ユニットに関する一意の名前をデバイス ID として指定します。
hostname	ASA のホスト名をデバイス ID として指定します。
ipaddress *interface_name*	デバイス ID または *interface_name* のインターフェイスの IP アドレスを指定します。ipaddress キーワードを使用すると、ログデータを外部サーバーに送信するために ASA で使用されるインターフェイスに関係なく、指定したインターフェイスの IP アドレスが外部サーバーに送信される syslog メッセージに含まれます。
string *text*	デバイス ID として *text* に含める文字を指定します。最大 16 文字です。スペースおよび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 • <：未満 • >：より大きい • ?：疑問符
system	（オプション）クラスタ環境において、インターフェイスのシステムの IP アドレスをデバイス ID として指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	**cluster-id** および **system** キーワードが追加されました。

使用上のガイドライン

ipaddress キーワードを使用すると、メッセージが送信されるインターフェイスに関係なく、デバイス ID が指定した ASA インターフェイスの IP アドレスになります。このキーワードにより、そのデバイスから送信されるすべてのメッセージに対して、単一の一貫したデバイス ID が指定されます。**system** キーワードを使用すると、クラスタのユニットのローカル IP アドレスではなく、システムの IP アドレスが指定した ASA で使用されます。**cluster-id** および **system** キーワードは、ASA 5580 と 5585-X のみに適用されます。

例

次に、「secappl-1」というホストを設定する例を示します。

```
ciscoasa(config)# logging device-id hostname
ciscoasa(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"
```

ホスト名は、次のメッセージに示すように、syslog メッセージの先頭に表示されます。

```
secappl-1 %ASA-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。

コマンド	説明
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging emblem

syslog サーバー以外の宛先に送信される syslog メッセージに EMBLEM 形式を使用するには、グローバル コンフィギュレーション モードで **logging emblem** コマンドを使用します。EMBLEM 形式の使用を無効にするには、このコマンドの **no** 形式を使用します。

loggingemblem
nologgingemblem

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。

コマンド デフォルト

ASA のデフォルトでは、syslog メッセージに EMBLEM 形式は使用されません。

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。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは **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 サーバー以外のすべてのロギング先に対して、EMBLEM形式のロギングを有効にできます。**logging timestamp** キーワードも有効にする場合、タイムスタンプが付いたメッセージが送信されます。

syslog サーバーに対して EMBLEM 形式のロギングを有効にするには、**logging host** コマンドで **format emblem** オプションを使用します。

（注） EMBLEM 形式のタイムスタンプ文字列には年は含まれません。イベント syslog に年を表示するには、**logging timestamp rfc5424** コマンドを使用して RFC 5424 に従ってタイムスタンプを有効にします。次に、RFC 5424 形式の出力例を示します。

```
<166>2018-06-27T12:17:46Z asa : %ASA-6-110002: Failed to locate egress interface for
protocol from src interface :src IP/src port to dest IP/dest port
```

または、**logging device-id** コマンドを使用できます。

例

次に、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例を示します。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging emblem
ciscoasa(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グ関連部分を表示します。

logging enable

設定済みのすべての出力場所に対してロギングを有効にするには、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。ロギングを無効にするには、このコマンドの **no** 形式を使用します。

loggingenable
nologgingenable

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。

コマンド 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。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**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への syslog メッセージの送信を有効または無効にできます。no logging enable コマンドを使用して、すべてのロギングを停止できます。

次のコマンドを使用して、個別のロギング先へのロギングをイネーブルにすることができます。

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

例

次に、ロギングをイネーブルにする例を示します。**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有効にする必要がある状況を示しています。

```
ciscoasa
(config)#
logging enable
ciscoasa
(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グ関連部分を表示します。

logging facility

syslog サーバー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。

loggingfacility*facility*
nologgingfacility

構文の説明

facility	ロギング ファシリティを指定します。有効な値は、16 ～ 23 です。

コマンド デフォルト

デフォルトのファシリティは 20（LOCAL4）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。例外については、「構文の説明」を参照してください。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

Syslog サーバは、メッセージ内のファシリティ番号に応じてメッセージをファイルに送信します。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

次に、ASA によってロギングファシリティが syslog メッセージに 16 として示されるように指定する例を示します。**show logging** コマンドの出力には、ASA によって使用されているファシリティが含まれます。

```
ciscoasa(config)# logging facility 16
ciscoasa(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 サーバーを定義します。
logging trap	syslog サーバー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グ関連部分を表示します。

logging flash-bufferwrap

未保存のメッセージでログバッファがいっぱいになるたびに、 ASA 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。フラッシュメモリへのログバッファの書き込みを無効にするには、このコマンドの **no** 形式を使用します。

loggingflash-bufferwrap
nologgingflash-bufferwrap

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。

コマンド デフォルト

デフォルトの設定は次のとおりです。

- 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 サイズは 4 KB です。
- フラッシュ メモリの最小の空き容量は 3 MB です。
- バッファ ロギングに対するフラッシュ メモリの最大割り当て容量は 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。

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	トランスペアレント	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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ASAによってログバッファがフラッシュメモリに書き込まれるようにするには、バッファへのロギングを有効にする必要があります。有効にしないと、ログバッファのデータはフラッシュメモリに書き込まれません。バッファへのロギングを有効にするには、**logging buffered** コマンドを使用します。ただし、設定されたロギングバッファサイズが 2MB を超える場合、内部ログバッファはフラッシュメモリに書き込まれません。

ASA では、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がログバッファに保存されます。

ASA では、次のようなデフォルトのタイムスタンプ形式を使用した名前のログファイルが作成されます。

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

YYYY は年、*MM* は月、*DD* は日付、*HHMMSS* は時間、分、および秒で示された時刻です。

logging flash-bufferwrap コマンドを使用する場合、フラッシュメモリの可用性が、ASA による syslog メッセージの保存方法に影響します。詳細については、**logging flash-maximum-allocation** および **logging flash-minimum-free** コマンドを参照してください。

例

次に、ロギングとログバッファを有効にし、ASA によるフラッシュメモリへのログバッファの書き込みを有効にする例を示します。

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

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 syslog メッセージをすべて消去します。
copy	TFTP サーバーまたは FTP サーバーを使用して、ファイルをある場所から別の場所にコピーします。
delete	保存されたログ 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 サイズを指定します。

logging flash-maximum-allocation

ログデータを保管するために ASA で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。この目的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。

loggingflash-maximum-allocation*kbytes*
nologgingflash-maximum-allocation*kbytes*

構文の説明

kbytes ログバッファデータを保存するために ASA で使用できるフラッシュメモリの最大量（KB 単位）。

コマンド デフォルト

ログ データ用のデフォルトの最大フラッシュ メモリ割り当ては 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。

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	トランスペアレント	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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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量が決まります。

logging savelog または **logging flash-bufferwrap** で保存されるログファイルにより、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、ASAによって最も古いログファイルが削除され、新しいログファイル用に十分な量のメモリが解放されます。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空きメモリが新しいログ ァイルには小さすぎる場合は、ASA で新しいログファイルを保存できません。

デフォルトサイズとは異なるサイズの最大フラッシュメモリ割り当て量が ASA にあるか確認するには、**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、ASA では保存されるログバッファデータに対して最大 1 MB が

使用されます。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。

ASA 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

次に、ロギングとログバッファを有効にし、ASA によるフラッシュメモリへのログバッファの書き込みを有効にし、ログファイルの書き込みに使用されるフラッシュメモリの最大量を約 1.2 MB に設定する例を示します。

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

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファに含まれているすべての syslog メッセージをクリアします。
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ている場合に、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ために、ASA で使用可能にする必要があるフラッシュメモリの最小量を指定します。

logging flash-minimum-free

ASA で新しいログファイルを保存するために必要なフラッシュメモリの最小空き領域を指定するには、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。フラッシュメモリの必要最小空き領域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。

loggingflash-minimum-free*kbytes*
nologgingflash-minimum-free*kbytes*

構文の説明

kbytes ASA で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）。

コマンド デフォルト

フラッシュ メモリのデフォルトの最小空き領域は 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。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

logging flash-minimum-free コマンドでは、**logging savelog** コマンドと **logging flash-bufferwrap** コマンド用に常に保持しておく必要があるフラッシュメモリの量を指定します。

logging savelog または **logging flash-bufferwrap** で保存されるログファイルにより、フラッシュメモリの空き領域が **logging flash-minimum-free** コマンドで指定された制限を下回る場合、ASA によって最も古いログファイルが削除され、新しいログファイルの保存後も最低限の空き容量がメモリに残るようにします。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空きメモリの量がまだ制限を下回っている場合、ASA で新しいログファイルを保存できません。

例

次に、ロギングを有効にし、ログバッファを有効にし、ASA によるフラッシュメモリへのログバッファの書き込みを有効にし、フラッシュメモリの最小空き領域を 4000 KB に指定する例を示します。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging flash-bufferwrap
ciscoasa(config)# logging flash-minimum-free 4000
ciscoasa(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 syslog 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ている場合に、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	ログ バッファの内容の書き込みに使用できるフラッシュ メモリの最大量を指定します。

logging flow-export-syslogs

NetFlow によってキャプチャされるすべての syslog メッセージを有効または無効にするには、グローバル コンフィギュレーション モードで **logging flow-export-syslogs** コマンドを使用します。

logging flow-export-syslogs { **enable** | **disable** }

構文の説明

enable	NetFlow によってキャプチャされるすべての syslog メッセージをイネーブルにします。
disable	NetFlow によってキャプチャされるすべての syslog メッセージをディセーブルにします。

コマンド デフォルト

デフォルトでは、NetFlow によってキャプチャされるすべての syslog はイネーブルになっています。

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。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.1(1)	このコマンドが追加されました。

使用上のガイドライン

セキュリティアプライアンスが NetFlow データをエクスポートするように設定されている場合、パフォーマンス向上のため、**logging flow-export-syslogs disable** コマンドを入力して（NetFlow でキャプチャされた）冗長な syslog メッセージをディセーブルにすることを推奨します。ディセーブルにされる syslog メッセージは、次のとおりです。

syslog メッセージ	説明
106015	最初のパケットが SYN パケットではなかったため、TCP フローが拒否されました。
106023	**access-group** コマンドを使用してインターフェイスに付加される入力 ACL または出力 ACL によって拒否されたフロー。

syslog メッセージ	説明
106100	ACL によって許可または拒否されたフロー。
302013 および 302014	TCP 接続および削除。
302015 および 302016	UDP 接続および削除。
302017 および 302018	GRE 接続および削除。
302020 および 302021	ICMP 接続および削除。
313001	セキュリティ アプライアンスへの ICMP パケットが拒否されました。
313008	セキュリティアプライアンスへの ICMPv6 パケットが拒否されました。
710003	セキュリティ アプライアンスへの接続試行が拒否されました。

（注） これはコンフィギュレーションモードのコマンドですが、コンフィギュレーションに格納されません。**no logging message xxxxxx** コマンドのみが、構成に保存されます。

例

次に、NetFlow によってキャプチャされる冗長な syslog メッセージをディセーブルにする例と表示される出力例を示します。

```
ciscoasa(config)# logging flow-export-syslogs disable
ciscoasa(config)# show running-config logging
no logging message xxxxx1
no logging message xxxxx2
```

xxxxx1 および *xxxxx2* は、NetFlow によって同じ情報がキャプチャされているために冗長である syslog メッセージです。このコマンドはコマンド エイリアスに似ており、no logging message xxxxxx コマンドのバッチに変換されます。syslog メッセージは、無効にした後、**logging message xxxxxx** コマンドを使用して個別に有効にできます。*xxxxxx* は特定の syslog メッセージ番号です。

関連コマンド

コマンド	説明
flow-export destination	NetFlow コレクタの IP アドレスまたはホスト名と、NetFlow コレクタがリッスンする UDP ポートを指定します。
flow-export template timeout-rate	テンプレート情報が NetFlow コレクタに送信される間隔を制御します。
show flow-export counters	NetFlow のランタイム カウンタのセットを表示します。

logging from-address

ASA によって送信される syslog メッセージの送信者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。送信されるすべての syslog メッセージは、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。

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

構文の説明

from-email-address	送信元電子メール アドレス。つまり、syslog メッセージの送信元として表示される電子メール アドレス（cdb@example.com など）。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

電子メールによる syslog メッセージの送信は、**logging mail** コマンドで有効にします。

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

ロギングを有効にし、syslog メッセージを電子メールで送信するように ASA を設定するには、次の基準を使用します。

- critical、alert、または emergency レベルのメッセージを送信する
- ciscosecurityappliance@example.com を送信元アドレスに使用して、メッセージを送信する
- admin@example.com にメッセージを送信する

- プライマリ サーバー pri-smtp-host およびセカンダリ サーバー sec-smtp-host を使用して、SMTP でメッセージを送信する

次のコマンドを入力します。

```
ciscoasa
(config)#
logging enable
ciscoasa
(config)#
logging mail critical
ciscoasa
(config)#
logging from-address ciscosecurityappliance@example.com
ciscoasa
(config)#
logging recipient-address admin@example.com
ciscoasa
(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	ASA の電子メールによる syslog メッセージの送信を有効にし、電子メールで送信するメッセージを決定します。
logging recipient-address	syslog メッセージの送信先の電子メール アドレスを指定します。
smtp-server	SMTP サーバーを設定します。
show logging	イネーブルなロギング オプションを表示します。

logging ftp-bufferwrap

未保存のメッセージでログバッファがいっぱいになるたびに、ASA が FTP サーバーにログバッファを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。FTP サーバーへのログバッファの送信を無効にするには、このコマンドの **no** 形式を使用します。

loggingftp-bufferwrap
no logging ftp-bufferwrap

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。

コマンド デフォルト

デフォルトの設定は次のとおりです。

- バッファへのロギングはディセーブルです。
- FTP サーバーへのログ 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。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

logging ftp-bufferwrap を有効にすると、ASA により、ログバッファデータは **logging ftp-server** コマンドで指定した FTP サーバーに送信されます。ASA は、ログデータを FTP サーバーに送信する間も、新しいイベントメッセージをログバッファに保管し続けます。

ASA によってログバッファの内容が FTP サーバーに送信されるようにするには、バッファへのロギングを有効にする必要があります。有効にしないと、ログバッファのデータはフラッシュメモリに書き込まれません。バッファへのロギングを有効にするには、**logging buffered** コマンドを使用します。

ASA では、次のようなデフォルトのタイムスタンプ形式を使用した名前のログファイルが作成されます。

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

YYYY は年、*MM* は月、*DD* は日付、*HHMMSS* は時間、分、および秒で示された時刻です。

例

次に、ロギングとログバッファを有効にし、FTP サーバーを指定して、ASA が FTP サーバーにログバッファを書き込めるようにする例を示します。この例では、ホスト名が logserver-352 である FTP サーバーを指定しています。サーバーには、ユーザー名 logsupervisor およびパスワード 1luvMy10gs でアクセスできます。ログ ファイルは /syslogs ディレクトリに保存されます。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging ftp-server logserver-352 /syslogs logsupervisor 1luvMy10gs
ciscoasa(config)# logging ftp-bufferwrap
ciscoasa(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 syslog 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 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 サーバーパラメータを指定します。

logging ftp-server

logging ftp-bufferwrap が有効になっている場合に ASA からログバッファデータが送信される FTP サーバー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 サーバー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 path username* [*0* | *8*] *password*
no logging ftp-server *ftp_server path username* [*0* | *8*] *password*

構文の説明

0	（任意）暗号化されていない（クリアテキストの）ユーザーパスワードが続くことを指定します。
8	（任意）暗号化されたユーザー パスワードが続くことを指定します。
ftp-server	外部 FTP サーバーの IP アドレスまたはホスト名。 （注） ホスト名を指定した場合、DNS がご使用のネットワークで適切に運用されていることを確認してください。
password	指定したユーザー名のパスワード。最大 64 文字です。
path	ログ バッファ データが保存される FTP サーバー上のディレクトリ 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。次に例を示します。 `/security_appliances/syslogs/appliance107`
username	FTP サーバーへのログインに有効なユーザー名。

コマンド デフォルト

デフォルトでは、FTP サーバー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。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

リリース	変更内容
8.3(1)	パスワード暗号化のサポートが追加されました。

使用上のガイドライン

FTP サーバは 1 つのみ指定できます。ロギング FTP サーバー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、この FTP サーバー構成は入力した新しい構成に置き換えられます。

指定した FTP サーバー情報は ASA によって検証されません。詳細を誤って設定した場合、ASA から FTP サーバーにログバッファデータを送信できません。

ASA の起動やアップグレードでは、1 桁のパスワードや、数字で始まりその後にスペースが続くパスワードはサポートされません。たとえば、0 pass や 1 は不正なパスワードです。

例

次に、ロギングとログバッファを有効にし、FTP サーバーを指定して、ASA が FTP サーバーにログバッファを書き込めるようにする例を示します。この例では、logserver というホスト名の FTP サーバーを指定します。サーバーは、ユーザー名 user1 とパスワード pass1 でアクセスできるものとします。ログ ファイルは /path1 ディレクトリに保存されます。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging ftp-server logserver /path1 user1 pass1
ciscoasa(config)# logging ftp-bufferwrap
```

次に、暗号化されたパスワードを入力する例を示します。

```
ciscoasa(config)# logging ftp-server logserver /path1 user1 8
JPAGWzIIFVlheXv2I9nglfytOzHU
```

次に、暗号化されていない（クリア テキストの）パスワードを入力する例を示します。

```
ciscoasa(config)# logging ftp-server logserver /path1 user1 0 pass1
```

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 syslog 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 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 サーバーに送信します。

logging hide username

ユーザー名の有効性が不明である場合に syslog のユーザー名を非表示（「*****」など）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 hide username** コマンドを使用します。非表示にしたユーザー名を表示するには、このコマンドの **no** 形式を使用します。

logginghideusername
no logging hide username

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。

コマンド デフォルト

デフォルトでは、ユーザー名は非表示です。

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		
	ルーテッド	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(3)	このコマンドが追加されました。

使用上のガイドライン

logging hide username コマンドにより、有効性が確認されていないユーザーのユーザー名を syslog で非表示にできます。

（注） このコマンドは、バージョン 9.4(1) では使用できません。

例

次に、有効性が確認されていないユーザー名を syslog で非表示にする例を示します。

```
ciscoasa(config)# logging hide username
ciscoasa# show logging
Syslog logging: enabled
...
Hide Username logging: enabled | 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。
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グ関連部分を表示します。

logging history

SNMP ロギングを有効にし、SNMP サーバーに送信す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 ロギングを無効にするには、このコマンドの **no** 形式を使用します。

logging history [**rate-limit** *number interval* **level** *level* | *logging_list* | *level*]
no logging history

構文の説明

interval	**rate-limit** でログ間隔を秒単位で指定し、ログが SNMP に転送されるレートを制限します。**logging rate-limit** コマンドを設定すると、この設定よりも優先されます。
level	履歴レート制限のロギングレベルを指定します。SNMP に転送されるメッセージは、指定された syslog レベルに制限されます。
level	syslog メッセージの最大重大度を設定します。たとえば、重大度を 3 に設定すると、ASA は重大度 3、2、1、0 の syslog メッセージを生成します。次のように、数値または名前のいずれかを指定できます。 • **0** または **emergencies**：システムが使用不能。 • **1** または **alerts**：すぐに対処が必要。 • **2** または **critical**：重大な状態。 • **3** または **errors**：エラー状態。 • **4** または **warnings**：警告状態。 • **5** または **notifications**：通常の状態だが、重要な状態。 • **6** または **informational**：Informational（情報提供）メッセージ。 • **7** または **debugging**：Debug（デバッグ）メッセージ。 （注） 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、**debugging** 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。また、このコマンドは、ネットワークトラフィックやユーザーが少ない時間帯に使用してください。デバッギングをこのような時間帯に行うと、システムの使用に影響が及ぶ処理のオーバーヘッドが増加する可能性が低くなります。
logging_list	SNMP サーバー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。

number	**rate-limit** を使用する場合は、インターバル期間中にログに記録するメッセージの数を指定します。
rate-limit	SNMP に転送されるログを制限します。syslog にログを記録する **rate-limit** を秒単位で指定します。

コマンド デフォルト

デフォルトでは、ASA によって SNMP サーバーにロギングされません。

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。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.20(1)	SNMP に送信されるログをレート制限する **rate-limit** キーワードが追加されました。

使用上のガイドライン

logging history コマンドを使用すると、SNMP サーバーへのロギングを有効にし、SNMP メッセージレベルまたはイベントリストを設定できます。

例

次に、SNMP ロギングをイネーブルにし、重大度レベル 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ことを指定する例を示します。

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

例

次に、SNMP に送信されるクリティカル syslog のレートを 15 メッセージ/15 秒に制限する例を示します。

```
ciscoasa(config)# logging history rate-limit 15 15 level critical
```

no logging history コマンドを使用して、デバイスのメモリリークを軽減します。このコマンドは、syslog サーバーへの通常のロギングには影響しません。

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	メッセージ選択基準の再使用可能な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グ関連部分を表示します。
snmp-server	SNMP サーバーの詳細を指定します。

logging host

syslog サーバーを定義するには、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 サーバー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**]] [**secure** [**reference-identity** *reference_identity_name*]]
no logging host *interface_name syslog_ip* [**tcp** [*/ port*] | **udp** [*/ port*] [**format emblem**]] [**secure** [**reference-identity** *reference_identity_name*]]

構文の説明

format emblem	（任意）syslog サーバーに対して EMBLEM 形式のロギングをイネーブルにします。EMBLEM 形式のロギングは、UDP syslog メッセージのみに使用できます。
interface_name	syslog サーバーが配置されているインターフェイスを指定します。
port	syslog サーバーがメッセージをリッスンするポートを指定します。有効なポート値は、いずれのプロトコルも 1025 ～ 65535 です。ポート番号として 0 を入力したり、無効な文字や記号を使用したりすると、エラーが発生します。
secure	（オプション）リモート ロギング ホストへの接続に SSL/TLS を使用するように指定します。このオプションは、選択されたプロトコルが TCP の場合にだけ有効です。 （注） セキュアなロギング接続は、SSL/TLS 対応の syslog サーバーとのみ確立できます。SSL/TLS 接続を確立できない場合、新しい接続はすべて拒否されます。このデフォルトの動作は、**logging permit-hostdown** コマンドを入力して変更できます。
syslog_ip	syslog サーバーの IP アドレス（IPv4 または IPv6）を指定します。
tcp	ASA が TCP を使用して syslog サーバーにメッセージを送信するよう指定します。
udp	ASA が UDP を使用して syslog サーバーにメッセージを送信するよう指定します。
reference_identity_name	セキュリティを強化するための RFC 6125 参照アイデンティティ チェックを可能にする参照アイデンティティ オブジェクトの名前を指定します。受信したサーバー証明書に関するアイデンティティ チェックは、この事前に設定された参照アイデンティティ オブジェクトに基づいて実行されます。

timestamp [**legacy** | **rfc5424**]	（任意）従来の形式またはRFC5424形式（yyyy-MM-THH:mm:ssZ、文字ZはUTCタイムゾーンを示す）で指定できるタイムスタンプ形式を有効にします。

コマンド デフォルト

デフォルト プロトコルは UDP です。

format emblem オプションのデフォルト設定は false です。

secure オプションのデフォルト設定は false です。

デフォルトのポート番号は次のとおりです。

- UDP：514
- TCP：1470

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが追加されました。
8.0(2)	**secure** キーワードが追加されました。
8.4(1)	接続のブロッキングをイネーブルまたはディセーブルにできるようになりました。
9.6.2	**reference-identity** オプションが追加されました。
9.7(1)	syslog サーバーに IPv6 アドレスを使用できるようになりました。直接接続された syslog サーバーがある場合、ASA および syslog サーバーの /31 サブネットを使用してポイントツーポイント接続を作成できます。

使用上のガイドライン

logging host *syslog_ip* format emblem コマンドを使用すると、各 syslog サーバーに対して EMBLEM 形式のロギングを有効にできます。EMBLEM 形式のロギングは、UDP syslog メッセージのみに使用できます。EMBLEM 形式のロギングを特定の syslog サーバーに対してイネーブルにすると、メッセージはそのサーバーに送信されます。**logging timestamp** コマンドを使用すると、タイムスタンプが付与されたメッセージも送信されます。

複数の logging host コマンドを使用して、追加サーバーを指定できます。それらすべてで syslog メッセージが受信されます。ただし、UDP と TCP 両方ではなく、いずれかの syslog メッセージのみが受信されるようにサーバーを指定できます。

サーバー証明書で提示されるアイデンティティが、設定済みの **reference-identity** と一致しない場合、接続は確立されず、エラーがログに記録されます。

接続のブロッキングに対するデフォルト設定は、 syslog サーバーへのメッセージ送信に TCP を使用するように、**logging host** コマンドが設定されている場合にのみ有効になります。TCP ベースの syslog サーバーが設定されている場合、 **logging permit-hostdown** コマンドを使用して、接続のブロッキングを無効にできます。

（注） **logging host** コマンドで **tcp** オプションを使用すると、syslog サーバーに到達できない場合、ファイアウォールを通過する接続は ASA によってドロップされます。

以前に入力した *port* 値と *protocol* 値のみを表示するには、 **show running-config logging** コマンドを使用して、リストからコマンドを見つけます。TCP は 6、UDP は 17 として表示されます。TCP ポートは syslog サーバーのみで機能します。*port* は、syslog サーバーがリッスンするポートと同じである必要があります。

（注） **logging host** コマンドと **secure** キーワードを UDP で使用しようとすると、エラーメッセージが表示されます。

TCP での syslog の送信は、スタンバイ ASA ではサポートされていません。

例

次に、重大度レベル 0、1、2、および 3 の syslog メッセージを、デフォルトのプロトコルとポート番号を使用する内部インターフェイス上の syslog サーバーに送信する例を示します。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging host inside 10.2.2.3
ciscoasa(config)# logging trap errors
ciscoasa(config)#
ciscoasa(config)# logging enable
ciscoasa(config)# logging host inside 2001:192:168:88::111
ciscoasa(config)# logging trap errors
ciscoasa(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 サーバー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。

コマンド	説明
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging list

さまざまな基準（ログレベル、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に、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*

構文の説明

class *event_class*	（任意）syslog メッセージのイベントのクラスを設定します。指定したレベルについて、指定したクラスの syslog メッセージのみがコマンドによって識別されます。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*	syslog メッセージの最大重大度を設定します。たとえば、重大度を 3 に設定すると、ASA は重大度 3、2、1、0 の syslog メッセージを生成します。次のように、数値または名前のいずれかを指定できます。 • **0** または **emergencies**：システムが使用不能。 • **1** または **alerts**：すぐに対処が必要。 • **2** または **critical**：重大な状態。 • **3** または **errors**：エラー状態。 • **4** または **warnings**：警告状態。 • **5** または **notifications**：通常の状態だが、重要な状態。 • **6** または **informational**：Informational（情報提供）メッセージ。 • **7** または **debugging**：Debug（デバッグ）メッセージ。 （注） 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、**debugging** 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。また、このコマンドは、ネットワークトラフィックやユーザーが少ない時間帯に使用してください。デバッギングをこのような時間帯に行うと、システムの使用に影響が及ぶ処理のオーバーヘッドが増加する可能性が低くなります。

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レベルを調べるには、**show logging** コマンドを使用するか、syslog メッセージガイドを参照してください。
name	ロギング リスト名を設定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

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 で使用できる値は、次のとおりです。

- **auth**：ユーザー認証。
- **bridge**：トランスペアレント 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; 拡張可能認証プロトコル）。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、EAP セッション状態の変更、EAP ステータスのクエリー イベントといったタイプのイベント、および EAP ヘッダーおよびパケット内容の 16 進ダンプをログに記録します。
- **eapoudp**：拡張可能認証プロトコル（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 EAPoUDP のイベントをログに記録し、EAPoUDP ヘッダーおよびパケット内容の完全な記録を生成します。
- **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、例外リスト照合、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 適用、および再評価といったタイプのイベントのログを記録します。
- **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**：ユーザーセッション。
- **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

次に、logging list コマンドの使用例を示します。

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

上記の例は、指定された基準と一致する syslog メッセージがロギング バッファに送信されることを示しています。この例で指定されている基準は、次のとおりです。

- 100100 ～ 100110 の範囲の syslog メッセージ ID
- critical レベル以上のすべての syslog メッセージ（emergency、alert、または critical）

- warning レベル以上のすべての VPN クラスの syslog メッセージ（emergency、alert、critical、error、または warning）

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

（注） リストの基準を設計する場合、メッセージを重複して指定する基準でも構いません。複数の基準と一致する syslog メッセージも正常にロギングされます。

関連コマンド

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

logging mail

ASA でsyslogメッセージを電子メールで送信できるようにし、電子メールで送信するメッセージを決定できるようにするには、グローバル コンフィギュレーション モードで **logging mail** コマンドを使用します。syslog メッセージの電子メール送信を無効にするには、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*]

構文の説明

level syslog メッセージの最大重大度を設定します。たとえば、重大度を 3 に設定すると、ASA は重大度 3、2、1、0 の syslog メッセージを生成します。次のように、数値または名前のいずれかを指定できます。

- **0** または **emergencies**：システムが使用不能。
- **1** または **alerts**：すぐに対処が必要。
- **2** または **critical**：重大な状態。
- **3** または **errors**：エラー状態。
- **4** または **warnings**：警告状態。
- **5** または **notifications**：通常の状態だが、重要な状態。
- **6** または **informational**：Informational（情報提供）メッセージ。
- **7** または **debugging**：Debug（デバッグ）メッセージ。

（注） 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、**debugging** 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。また、このコマンドは、ネットワークトラフィックやユーザーが少ない時間帯に使用してください。デバッギングをこのような時間帯に行うと、システムの使用に影響が及ぶ処理のオーバーヘッドが増加する可能性が低くなります。

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。

コマンド 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。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

電子メールで送信される syslog メッセージは、送信された電子メールの件名欄に表示されます。

例

電子メールで syslog メッセージを送信するように ASA を設定するには、次のような基準を使用します。

- critical、alert、または emergency レベルのメッセージを送信する
- ciscosecurityappliance@example.com を送信元アドレスに使用して、メッセージを送信する
- admin@example.com にメッセージを送信する
- プライマリ サーバー pri-smtp-host およびセカンダリ サーバー sec-smtp-host を使用して、SMTP でメッセージを送信する

次のコマンドを入力します。

```
ciscoasa
(config)#
logging mail critical
ciscoasa
(config)#
logging from-address ciscosecurityappliance@example.com
ciscoasa
(config)#
logging recipient-address admin@example.com
ciscoasa
(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。

コマンド	説明
logging from-address	電子メールで送信される syslog メッセージの送信元として表示される電子メール アドレスを指定します。
logging list	メッセージ選択基準の再使用可能なリストを作成します。
logging recipient-address	電子メールで送信される syslog メッセージの送信先の電子メール アドレスを指定します。
smtp-server	SMTP サーバーを設定します。

logging message

syslog メッセージのロギングを有効にする、またはメッセージのレベルを変更するには、グローバル コンフィギュレーション モードで **logging message** コマンドを使用します。メッセージのロギングを無効にする、またはメッセージをデフォルトのレベルに設定するには、このコマンドの **no** 形式を使用します。

logging message *syslog_id* [**level** *level* | **standby**]
no logging message *syslog_id* [**level** *level* | **standby**]

構文の説明

level *level*
（オプション）指定された syslog メッセージの重大度レベルを設定します。次のように、数値または名前のいずれかを指定できます。

- **0** または **emergencies**：システムが使用不能。
- **1** または **alerts**：すぐに対処が必要。
- **2** または **critical**：重大な状態。
- **3** または **errors**：エラー状態。
- **4** または **warnings**：警告状態。
- **5** または **notifications**：通常の状態だが、重要な状態。
- **6** または **informational**：Informational（情報提供）メッセージ。
- **7** または **debugging**：Debug（デバッグ）メッセージ。

（注） 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、**debugging** 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。また、このコマンドは、ネットワークトラフィックやユーザーが少ない時間帯に使用してください。デバッギングをこのような時間帯に行うと、システムの使用に影響が及ぶ処理のオーバーヘッドが増加する可能性が低くなります。

メッセージのデフォルレベルを調べるには、**show logging** コマンドを使用するか、syslog メッセージガイドを参照してください。

syslog_id
イネーブルまたはディセーブルにする syslog メッセージまたは重大度レベルを変更する syslog メッセージの ID。

standby
（任意）スタンバイユニットで特定の syslog メッセージが生成されないようにするには、このコマンドの **no** 形式を **standby** キーワードとともに指定します。

コマンド デフォルト

デフォルトでは、すべてのsyslogメッセージはイネーブルであり、すべてのメッセージの重大度レベルはデフォルトの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。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.4(1)	**standby** キーワードが追加されました。

使用上のガイドライン

logging message コマンドは次の目的に使用できます。

- メッセージをイネーブルにするかディセーブルにするかを指定します。
- スタンバイ ユニットでの syslog メッセージの生成をディセーブルにします。
- メッセージの重大度レベルを指定します。

show logging コマンドを使用して、メッセージに現在割り当てられているレベルや、メッセージが有効かどうかを判別できます。

ASA で特定の syslog メッセージを生成しないようにするには、グローバル コンフィギュレーション モードで **logging message** コマンドの **no** 形式を使用します（**level** キーワードは不要）。ASA で特定の syslog メッセージを生成できるようにするには、**logging message** コマンドを使用します（**level** キーワードは不要）。これら 2 つの種類の **logging message** コマンドは、並行して実行できます。

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、メッセージを有効にするかどうか、およびメッセージの重大度を指定する方法を示しています。

```
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors (enabled)
ciscoasa(config)# logging message 403503 level 1
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)
ciscoasa(config)# no
logging message 403503
ciscoasa(config)# show logging message 403503
```

```
syslog 403503: default-level errors, current-level alerts (disabled)
ciscoasa(config)# logging message 403503
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)
ciscoasa(config)# no
logging message 403503 standby
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors (enabled),standby logging (disabled)
ciscoasa(config)# no logging message 403503 level 3
ciscoasa(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	すべてのロギング コンフィギュレーションまたはメッセージ コンフィギュレーションのみをクリアします。
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グ関連部分を表示します。

logging message standby

スタンバイユニットでの生成を以前にブロックした特定のsyslogメッセージのブロックを解除するには、**logging message standby** コマンドを使用します。スタンバイ装置で特定の syslog メッセージが生成されないようにブロックするには、このコマンドの **no** 形式を使用します。

logging message *syslog_id* **standby**
no logging message *syslog_id* **standby**

構文の説明

syslog_id	スタンバイ ユニットでイネーブルまたはディセーブルにする syslog メッセージの ID。

コマンド デフォルト

デフォルトでは、すべての syslog メッセージがスタンバイ ユニットで生成されます（logging standby コマンドがイネーブルの場合のみ）。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

[no] logging message *syslog_id* **standby** コマンドを使用して、スタンバイユニットで syslog メッセージを有効にするか無効にするかを指定できます。

show logging コマンドを使用して、syslog メッセージが有効になっているかどうかを確認できます。

例

次に、**logging message** *syslog_id* **standby** コマンドの使用例を示します。この一連の例では、スタンバイユニットで syslog メッセージが有効になっているかどうかを確認しています。

```
ciscoasa(config)# no logging message 403503 standby
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled), standby logging
disabled
```

関連コマンド

コマンド	説明
clear configure logging	すべてのロギング コンフィギュレーションまたはsyslog メッセージ コンフィギュレーションのみをクリアします。
logging enable	ロギングをイネーブルにします。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging monitor

ASA で syslog メッセージを SSH セッションおよび 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。SSH セッションおよび Telnet セッションへの syslog メッセージの表示を無効にするには、このコマンドの **no** 形式を使用します。

logging monitor [*logging_list* | *level*]
nologgingmonitor

構文の説明

level syslog メッセージの最大重大度を設定します。たとえば、重大度を 3 に設定すると、ASA は重大度 3、2、1、0 の syslog メッセージを生成します。次のように、数値または名前のいずれかを指定できます。

- **0** または **emergencies**：システムが使用不能。
- **1** または **alerts**：すぐに対処が必要。
- **2** または **critical**：重大な状態。
- **3** または **errors**：エラー状態。
- **4** または **warnings**：警告状態。
- **5** または **notifications**：通常の状態だが、重要な状態。
- **6** または **informational**：Informational（情報提供）メッセージ。
- **7** または **debugging**：Debug（デバッグ）メッセージ。

（注） 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、**debugging** 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。また、このコマンドは、ネットワークトラフィックやユーザーが少ない時間帯に使用してください。デバッギングをこのような時間帯に行うと、システムの使用に影響が及ぶ処理のオーバーヘッドが増加する可能性が低くなります。

logging_list SSH セッションまたは 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。

コマンド デフォルト

ASA のデフォルトでは、syslog メッセージは SSH セッションや Telnet セッションに表示されません。

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。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

logging monitor コマンドにより、現在のコンテキストのセッションすべてに対して syslog メッセージが有効になります。ただし、各セッションに syslog メッセージが表示されるかどうかは、**terminal** コマンドによって制御されます。

例

次に、コンソール セッションで syslog メッセージの表示をイネーブルにする例を示します。**errors** キーワードの使用は、重大度レベル 0、1、2、および 3 のメッセージが SSH セッションおよび Telnet セッションに表示されることを示しています。**terminal** コマンドを使用すると、メッセージを現在のセッションに表示できます。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging monitor errors
ciscoasa(config)# terminal monitor
ciscoasa(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	メッセージ選択基準の再使用可能な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グ関連部分を表示します。
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 サーバーのステータスを新しいユーザーセッションと無関係にするには、グローバル コンフィギュレーション モードで **logging permit-hostdown** コマンドを使用します。TCP ベースの syslog サーバーが使用できないときに ASA で新しいユーザーセッションを拒否するには、このコマンドの **no** 形式を使用します。

loggingpermit-hostdown
nologgingpermit-hostdown

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。

コマンド デフォルト

デフォルトでは、TCP 接続を使用する syslog サーバーへのロギングを有効にした場合、何らかの理由で syslog サーバーが使用できないと、ASA では新しいネットワーク アクセス セッションが許可されません。**logging permit-hostdown** コマンドのデフォルト設定は false 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		
	ルーテッド	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

syslog サーバーにメッセージを送信するためのロギング トランスポート プロトコルとして TCP を使用している場合、ASA は、syslog サーバーに到達できない際、セキュリティ対策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。**logging permit-hostdown** コマンドを使用して、この制限を削除できます。

例

次に、TCP ベースの syslog サーバーのステータスを、ASA で新しいセッションが許可されるかどうかと無関係にする例を示します。**show running-config logging** コマンドの出力に **logging permit-hostdown** コマンドが含まれている場合、TCP ベースの syslog サーバーのステータスは、新しいネットワーク アクセス セッションと無関係です。

```
ciscoasa(config)# logging permit-hostdown
ciscoasa(config)# show running-config logging
```

```
logging enable
logging trap errors
logging host infrastructure 10.1.2.3 6/1470
logging permit-hostdown
ciscoasa(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 サーバーを定義します。
logging trap	syslog サーバー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グ関連部分を表示します。

logging queue

ロギング構成に従って処理する前に ASA のキューに保持できる syslog メッセージの数を指定するには、グローバル コンフィギュレーション モードで **logging queue** コマンドを使用します。ロギングキューのサイズをデフォルトの 512 メッセージにリセットするには、このコマンドの **no** 形式を使用します。

logging queue *queue_size*
no logging queue *queue_size*

構文の説明

queue_size 処理前の syslog メッセージを保管するために使用されるキューで許可される syslog メッセージの数。有効な値は、プラットフォームの種類に応じて 0 ～ 8192 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、プラットフォームに応じて、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。ASA-5505 では、キューの最大サイズは 1024 です。ASA-5510 では 2048 です。その他のすべてのプラットフォームでは 8192 です。

コマンド 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。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

トラフィックが多いためにキューがいっぱいになった場合、ASA によってメッセージが破棄される場合があります。ASA-5505 では、キューの最大サイズは 1024 です。ASA-5510 では 2048 です。その他のすべてのプラットフォームでは 8192 です。

⚠

注意 ローエンドプラットフォーム上のロギングキューサイズを大きくすると、ASDM、WebVPN、DHCPサーバーなど、他の機能に使用可能なDMAメモリ容量が減少します。これらの機能は、システムがDMAメモリを使い果たした場合に機能を停止することができます。MEMPOOL_DMAプール内の DMA メモリの空き容量を確認するには、**show memory detail** コマンドを使用します。

例

次に、logging queue コマンドおよび show logging queue コマンドの出力を表示する例を示します。

```
ciscoasa(config)# logging queue 0
ciscoasa(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、キューは最大の 8192 に設定されます。キュー内の syslog メッセージは、ロギング構成で指定された方法で ASA によって処理されます。たとえば、syslog メッセージがメールの受信者に送信されたり、フラッシュメモリに保存されたりします。

この例の show logging queue コマンドの出力には、5 つのメッセージがキューにあり、ASA が最後に起動されて以降、同時にキューにあった最大メッセージ数は 3513 であり、1 つのメッセージが廃棄されたことが示されています。キューのメッセージは無制限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 メモリを使用できなかったために、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グ関連部分を表示します。

logging rate-limit

syslog 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。レート制限を無効にするには、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** | **dynamic** { **block** *value* [**message limit** *value*] } | { *num* [*interval*] } | **message** { *syslog_id* | **level** *severity_level* } }
[**no**] **logging rate-limit** { **unlimited** | **dynamic** { **block** *value* [**message limit** *value*] } | { *num* [*interval*] } | **message** { *syslog_id* | **level** *severity_level* } }

構文の説明

block*value*	レート制限のしきい値として機能するブロックのパーセンテージ。
dynamic	ブロック使用量が指定されたしきい値（256）を超えたときにロギングレートを制限します。ブロックの使用量が通常の値に戻ったときにレート制限を無効にします。
interval	（任意）メッセージの生成レートを測定するために使用する時間間隔（秒単位）。*interval* 値の有効な範囲は、0 ～ 2147483647 です。
level *severity_level*	設定されたレート制限を、特定の重大度レベルに属するすべての syslog メッセージに適用します。指定した重大度レベルのすべての syslog 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 syslog メッセージのレポートを抑制します。
message limit*value*	動的レート制限で許可されるメッセージの数。
num	指定した時間間隔で生成できる syslog メッセージの数。*num* 値の有効な範囲は、0 ～ 2147483647 です。
syslog_id	抑制する syslog メッセージの ID。有効な値の範囲は 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。

コマンド デフォルト

interval のデフォルト設定は 1 です。

message limit*value* のデフォルト設定は 10 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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが追加されました。
9.18(1)	レート制限の動的オプションが追加されました。

使用上のガイドライン

syslog メッセージの重大度レベルは、次のとおりです。

- 0：システムが使用不能
- 1：すぐに対処が必要
- 2：重大な状態
- 3：エラー状態
- 4：警告状態
- 5：通常の状態だが、重要な状態
- 6：情報メッセージ
- 7：デバッグ メッセージ

（注） 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、**debugging** 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。また、このコマンドは、ネットワークトラフィックやユーザーが少ない時間帯に使用してください。デバッギングをこのような時間帯に行うと、システムの使用に影響が及ぶ処理のオーバーヘッドが増加する可能性が低くなります。

例

syslog 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。次に、特定のメッセージ ID と時間間隔を使用して syslog メッセージの生成レートを制限する例を示します。

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

この例では、指定した 600 秒の間隔でレート制限 100 に達すると、syslog メッセージ 302020 はホストに送信されなくなります。

syslog メッセージの生成レートを制限するために、特定の重大度レベルを入力できます。次に、特定の重大度レベルと時間間隔を使用して syslog メッセージの生成レートを制限する例を示します。

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

この例では、重大度レベル 6 のすべての syslog メッセージは、指定した 600 秒の時間間隔で指定したレート制限 1000 に抑制されます。重大度レベル 6 の各 syslog メッセージには、レート制限 1000 があります。

サイズ 256 のブロック使用率が高い場合にメッセージの動的レート制限を有効にするには、**dynamic** キーワードを使用します。動的レート制限をトリガーするためのしきい値として、サイズ 256 の空きブロックの割合を指定できます。また、**message limit** キーワードを使用して、動的レート制限のメッセージ数を許可できます。デフォルト値は 10 です。

```
asa(config)# logging rate-limit ?

configure mode commands/options:
  <1-2147483647>  Specify logging rate-limit number
  dynamic         Specify dynamic option for rate-limit
  unlimited       Specify unlimited option for rate-limit

asa(config)# logging rate-limit dynamic ?

configure mode commands/options:
  block  Dynamic rate-limit for block usage

asa(config)# logging rate-limit dynamic block ?

configure mode commands/options:
  <1-100>  Specify 256 blocks free percentage to trigger dynamic rate-limit
asa(config)# logging rate-limit dynamic block 50 ?

configure mode commands/options:
  messagelimit  Specify the number of messages allowed for dynamic rate-limit

asa(config)# logging rate-limit dynamic block 50 messagelimit ?

configure mode commands/options:
  <1-100>  Specify logging rate-limit interval
```

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。

コマンド	説明
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

ASA によって送信される syslog メッセージの受信者の電子メールアドレスを指定するには、グローバル コンフィギュレーション モードで **logging recipient-address** コマンドを使用します。受信者の電子メールアドレスを削除するには、このコマンドの **no** 形式を使用します。

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

構文の説明

address	syslog メッセージを電子メールで送信するときの受信者の電子メール アドレスを指定します。
level	重大度レベルが後に続くことを示します。

level syslog メッセージの最大重大度を設定します。たとえば、重大度を 3 に設定すると、ASA は重大度 3、2、1、0 の syslog メッセージを生成します。次のように、数値または名前のいずれかを指定できます。

- **0** または **emergencies**：システムが使用不能。
- **1** または **alerts**：すぐに対処が必要。
- **2** または **critical**：重大な状態。
- **3** または **errors**：エラー状態。
- **4** または **warnings**：警告状態。
- **5** または **notifications**：通常の状態だが、重要な状態。
- **6** または **informational**：Informational（情報提供）メッセージ。
- **7** または **debugging**：Debug（デバッグ）メッセージ。

（注） 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、**debugging** 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。また、このコマンドは、ネットワークトラフィックやユーザーが少ない時間帯に使用してください。デバッギングをこのような時間帯に行うと、システムの使用に影響が及ぶ処理のオーバーヘッドが増加する可能性が低くなります。

（注） **logging recipient-address** コマンドで 3 よりも大きい重大度レベルを使用することは推奨しません。重大度レベルを大きくすると、バッファ オーバーフローによって syslog メッセージがドロップされる可能性があります。

logging recipient-address コマンドで指定するメッセージ重大度レベルによって、**logging mail** コマンドで指定するメッセージ重大度レベルは上書きされます。たとえば、**logging recipient-address** コマンドで重大度レベル 7 を指定するが、**logging mail** コマンドで重大度レベル 3 を指定している場合、ASA によって、重大度レベル 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が受信者に送信されます。

コマンド デフォルト デフォルトでは、errors ログ レベルに設定されます。

コマンド モード 次の表は、このコマンドを入力できるモードを示しています。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

最大 5 つの受信者アドレスを設定できます。必要に応じて、受信者アドレスごとに、**logging mail** コマンドで指定されたメッセージレベルとは異なるメッセージレベルを指定できます。電子メールによる syslog メッセージの送信は、**logging mail** コマンドで有効にします。

このコマンドは、緊急性の高いメッセージを多数の受信者に送信する場合に使用します。

例

電子メールで syslog メッセージを送信するように ASA を設定するには、次のような基準を使用します。

- critical、alert、または emergency レベルのメッセージを送信する
- ciscosecurityappliance@example.com を送信元アドレスに使用して、メッセージを送信する
- admin@example.com にメッセージを送信する
- プライマリ サーバー pri-smtp-host およびセカンダリ サーバー sec-smtp-host を使用して、SMTP でメッセージを送信する

次のコマンドを入力します。

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

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging from-address	syslog メッセージの送信元として表示される電子メール アドレスを指定します。
logging mail	ASA の電子メールによる syslog メッセージの送信を有効にし、電子メールで送信するメッセージを決定します。
smtp-server	SMTP サーバーを設定します。
show logging	イネーブルなロギング オプションを表示します。

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*]

構文の説明

savefile （任意）保存するフラッシュ メモリ ファイルの名前。ファイル名を指定しない場合は、次に示すように、ログファイルはASAによってデフォルトのタイムスタンプ形式を使用して保存されます。

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

YYYY は年、*MM* は月、*DD* は日付、*HHMMSS* は時間、分、および秒で示された時刻です。

コマンド デフォルト

デフォルトの設定は次のとおりです。

- バッファ サイズは 4 KB です。
- フラッシュ メモリの最小の空き容量は 3 MB です。
- バッファ ロギングに対するフラッシュ メモリの最大割り当て容量は 1 MB です。
- デフォルトのログ ファイル名については、「構文の説明」を参照してください。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ログ バッファをフラッシュ メモリに保存する前に、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。イネーブルにしないと、ログ バッファのデータはフラッシュ メモリに保

存されません。バッファへのロギングを有効にするには、**logging buffered** コマンドを使用します。

（注） **logging savelog** コマンドによってバッファはクリアされません。バッファをクリアするには、**clear logging buffer** コマンドを使用します。

例

次に、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、ファイル名 latest-logfile.txt を使用してログ バッファをフラッシュ メモリに保存する例を示します。

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

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 syslog メッセージをすべて消去します。
copy	TFTP サーバーまたは FTP サーバーを使用して、ファイルをある場所から別の場所にコピーします。
delete	保存されたログ 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。

logging standby

フェールオーバースタンバイ ASA で syslog メッセージをロギング先に送信できるようにするには、グローバル コンフィギュレーション モードで **logging standby** コマンドを使用します。syslog メッセージングと SNMP ロギングを無効にするには、このコマンドの **no** 形式を使用します。

loggingstandby
nologgingstandby

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。

コマンド デフォルト

logging standby コマンドは、デフォルトでディセーブルです。

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。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

フェールオーバー発生時に、フェールオーバースタンバイ ASA の syslog メッセージの同期を継続させるために、**logging standby** コマンドを有効にできます。

（注） **logging standby** コマンドを使用すると、syslog サーバー、SNMP サーバー、FTP サーバーなどの共有ロギング先でのトラフィックは 2 倍になります。

例

次に、ASA で syslog メッセージをフェールオーバースタンバイ ASA に送信できるようにする例を示します。**show logging** コマンドの出力は、この機能が有効になっていることを示しています。

```
ciscoasa(config)# logging standby
ciscoasa(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 サーバーを定義します。
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グ関連部分を表示します。

logging timestamp

メッセージが生成された日付と時刻をsyslogメッセージに含めることを指定するには、グローバル コンフィギュレーション モードで **logging timestamp** コマンドを使用します。日付と時刻を syslog メッセージから削除するには、このコマンドの **no** 形式を使用します。

logging timestamp [**rfc5424**]
nologgingtimestamp

構文の説明

rfc5424 （任意）syslog メッセージのすべてのタイムスタンプには、RFC 5424 形式に従って時刻が表示されます。

```
YYYY
-MM
-DD
THH:MM:SS
Z
```

YYYY は年、*MM* は月、*DD* は日付、*HHMMSS* は時間、分、および秒で示された時刻です。

コマンド デフォルト

ASA のデフォルトでは、日付と時刻は syslog メッセージに含まれません。

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。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.10(1)	**The option to enable timestamp as per RFC 5424 format was added**

使用上のガイドライン

logging timestamp コマンドを使用すると、ASA によってすべての syslog メッセージにタイムスタンプが含まれます。バージョン 9.10(1) までは、syslog のタイムスタンプは RFC 3164 に準拠しており、タイムスタンプは「MM DD YYYY HH:MM:SS」形式で表示されていました。

この形式は SIEM では優先されないため、9.10(1) では、RFC 5424 オプションが導入されました。

logging timestamp コマンドで RFC 5424 オプションを使用して、RFC 5424 に従って syslog サポート タイムゾーンを有効にします。

例

次に、すべての syslog メッセージにタイムスタンプ情報が含まれるようにする例を示します。

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

次に、すべての syslog メッセージに RFC 5424 形式のタイムスタンプ情報が含まれるようにする例を示します。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging timestamp rfc5424
ciscoasa(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グ関連部分を表示します。

logging trap

ASA によって syslog サーバーに送信される syslog メッセージを指定するには、グローバル コンフィギュレーション モードで **logging trap** コマンドを使用します。構成からこのコマンドを削除するには、このコマンドの **no** 形式を使用します。

logging trap [*logging_list* | *level*]
nologgingtrap

構文の説明

level syslog メッセージの最大重大度を設定します。たとえば、重大度を 3 に設定すると、ASA は重大度 3、2、1、0 の syslog メッセージを生成します。次のように、数値または名前のいずれかを指定できます。

- **0** または **emergencies**：システムが使用不能。
- **1** または **alerts**：すぐに対処が必要。
- **2** または **critical**：重大な状態。
- **3** または **errors**：エラー状態。
- **4** または **warnings**：警告状態。
- **5** または **notifications**：通常の状態だが、重要な状態。
- **6** または **informational**：Informational（情報提供）メッセージ。
- **7** または **debugging**：Debug（デバッグ）メッセージ。

（注） 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、**debugging** 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。また、このコマンドは、ネットワークトラフィックやユーザーが少ない時間帯に使用してください。デバッギングをこのような時間帯に行うと、システムの使用に影響が及ぶ処理のオーバーヘッドが増加する可能性が低くなります。

logging_list syslog サーバー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。

コマンド デフォルト

デフォルトの syslog メッセージ 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。

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ロギング トランスポート プロトコルとして TCP を使用している場合、ASA が syslog サーバーに到達できないか、syslog サーバーが誤って設定されているか、ディスクがいっぱいになると、ASA はセキュリティ対策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 ベースのロギングでは、syslog サーバーに障害が発生しても、ASA によるトラフィックの送信は停止されません。

例

次に、重大度レベル 0、1、2、および 3 の syslog メッセージを、内部インターフェイス上に配置されていてデフォルトのプロトコルとポート番号を使用している syslog サーバに送信する例を示します。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging host inside 10.2.2.3
ciscoasa(config)# logging trap errors
ciscoasa(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 サーバーを定義します。
logging list	メッセージ選択基準の再使用可能な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グ関連部分を表示します。

login

ローカル ユーザー データベースを使用して特権 EXEC モードにログインするか（username コマンドを参照）、ユーザー名を変更するには、ユーザー EXEC モードで **login** コマンドを使用します。

login

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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド 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。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ユーザー EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ユーザーEXECモードから、**login**コマンドを使用して、ローカルデータベース内の任意のユーザー名で特権 EXEC モードにログインできます。認証をオンにした場合、**login** コマンドは **enable** コマンドと類似しています（**aaa authentication console** コマンドを参照）。enable 認証と異なり、**login** コマンドではローカルユーザー名データベースのみを使用でき、常に認証が必要です。CLI モードから **login** コマンドを使用して、ユーザーを変更することもできます。

ユーザー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、ユーザーの特権レベルを 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、ユーザーは、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 command** を参照してください。

⚠

注意 CLI にアクセスできるユーザーや特権 EXEC モードを開始できないようにするユーザー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。コマンド許可がない場合、特権レベルが 2 以上（2 がデフォルト）のユーザーは、CLI で自分のパスワードを使用して特権 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+ 認証を使用できます。あるいは、すべてのローカル ユーザーをレベル 1 に設定して、システム 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ーを制御できます。

例

次に、**login** コマンドを入力した後のプロンプトの例を示します。

```
ciscoasa> login
Username:
```

関連コマンド

コマンド	説明
aaa authorization command	CLI アクセスのため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	ユーザーをローカル データベースに追加します。

login-button

WebVPN ユーザー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[ログイン（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 コンフィギュレーション モードで **login-button** コマンドを使用します。コンフィギュレーションからコマンドを削除し、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。

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

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

構文の説明

style	スタイルを変更することを指定します。
text	テキスト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。

コマンド デフォルト

デフォルトのログイン ボタン テキストは「Login」です。

デフォルトのログイン ボタン 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

次の表に、コマンドを入力できるモードを示します。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
webvpn カスタマイゼーション コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

style オプションは有効なカスケーディング スタイル シート（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの

詳細については、World Wide Web コンソーシアム（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 で入手できます。

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）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番め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 を使用することを推奨します。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ための便利な機能があります。

例

次に、ログイン ボタンをテキスト「OK」でカスタマイズする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(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 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 ボックスのユーザー名プロンプトをカスタマイズします。

login-message

WebVPN ユーザー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 コンフィギュレーション モードで **login-message** コマンドを使用します。コンフィギュレーションからコマンドを削除し、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。

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

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

構文の説明

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。

コマンド 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

次の表に、コマンドを入力できるモードを示します。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
WebVPN カスタマイゼーション コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

style オプションは有効なカスケーディング スタイル シート（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web コンソーシアム（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 で入手できます。

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）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番め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を使用することを推奨します。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ための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は「username and password」に設定されます。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(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 ログインのユーザー名プロンプトをカスタマイズします。
password-prompt	WebVPN ページ ログインのパスワード プロンプトをカスタマイズします。
group-prompt	WebVPN ページ ログインのグループ プロンプトをカスタマイズします。

login-title

WebVPN ユーザーに表示される 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 コンフィギュレーション モードで **login-title** コマンドを使用します。コンフィギュレーションからコマンドを削除し、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。

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

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

構文の説明

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。

コマンド 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の HTML スタイルは、background-color: #666666; color: white 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。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
webvpn カスタマイゼーション コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

style オプションは有効なカスケーディング スタイル シート（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web コンソーシアム（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 で入手できます。

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）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番め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を使用することを推奨します。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ための便利な機能があります。

例

次に、ログイン タイトルのスタイルを設定する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(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 ログイン 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 ログイン ページのユーザー名プロンプトをカスタマイズします。
password-prompt	WebVPN ログイン ページのパスワード プロンプトをカスタマイズします。
group-prompt	WebVPN ログイン ページのグループ プロンプトをカスタマイズします。

logo

WebVPN ユーザー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。構成からロゴを削除してデフォルト（Cisco 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。

logo { **none** | **file** { *path value* } }

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

構文の説明

file	ロゴを含むファイルを指定することを示します。
none	ロゴが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。
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（スペースを含めることはできません）。ファイル タイプは JPG、PNG、または GIF であり、100 KB 未満である必要があります。

コマンド デフォルト

デフォルトのロゴは Cisco ロゴです。

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。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
webvpn カスタマイゼーション コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

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が、コンフィギュレーションがまだそのファイルを指している場合、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、ファイル cisco_logo.gif にカスタム ロゴが含まれています。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(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	カスケーディング スタイル シート（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、ユーザー EXEC モードで **logout** コマンドを使用します。

logout

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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド 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。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ユーザー EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

logout コマンドを使用すると、ASA からログアウトできます。**exit** コマンドまたは **quit** コマンドを使用して、非特権モードに戻ることができます。

例

次に、ASA からログアウトする例を示します。

```
ciscoasa> 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 ユーザーが 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 コンフィギュレーション モードで **logout-message** コマンドを使用します。コンフィギュレーションからコマンドを削除し、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。

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

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

構文の説明

style	スタイルを変更することを指定します。
text	テキスト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。

コマンド デフォルト

デフォルトのログアウト メッセージ 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

次の表に、コマンドを入力できるモードを示します。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
WebVPN カスタマイゼーション コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

style オプションは有効なカスケーディング スタイル シート（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web コンソーシアム（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 で入手できます。

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）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番め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を使用することを推奨します。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ための便利な機能があります。

例

次に、ログアウト メッセージのスタイルを設定する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(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 ボックスのユーザー名プロンプトをカスタマイズします。

lsp-full suppress

リンクステート プロトコル データ ユニット（PDU）がフルになった場合に、抑制するルートを制御するには、ルータ ISIS コンフィギュレーション モードで **lsp-full suppress** コマンドを使用します。再配布されたルートの抑制を停止するには、このコマンドの **no** 形式を指定します。

lsp-full suppress { **external** [**interlevel**] | **interlevel** [**external**] | **none** }
nolsp-fullsuppress

構文の説明

external	この ASA 上にある再配布済みルートを抑制します。
interlevel	他のレベルからのルートを抑制します。たとえば、レベル 2 の LSP がフルになると、レベル 1 からのルートが抑制されます。
none	ルートを抑制しません。

コマンド デフォルト

再配布済みルートは抑制されます。

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。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドにより、IS-IS 隣接のステート変更のモニタリングが可能になります。これは、大規模なネットワークをモニタリングする場合に非常に役立つことがあります。メッセージは、システム エラー メッセージ機能を使用してロギングされます。メッセージは次の形式になります。

```
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Up, new adjacency
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Down, hold time expired
```

例

次に、LSP がフルになった場合に、再配布ルートと別のレベルからのルートの両方が LSP によって抑制される例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# lsp-full suppress interlevel external
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
authentication key	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。

コマンド	説明
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更（アップまたはダウン）する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。

コマンド	説明
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト（TLV）を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
pnrotocol shutdow	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。

コマンド	説明
summary-address	IS-IS の集約アドレスを作成します。

lsp-gen-interval

LSP 生成の IS-IS スロットリングをカスタマイズするには、ルータ ISIS コンフィギュレーション モードで **lsp-gen-interval** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

lsp-gen-interval [**level-1** | **level-2**] *lsp-max-wait* [*lsp-initial-wait lsp-second-wait*
nolsp-gen-interval

構文の説明

level-1	（オプション）レベル 1 エリアだけに間隔を適用します。
level-2	（オプション）レベル 2 エリアだけに間隔を適用します。
lsp-max-wait	2 つの LSP が連続して生成される最大間隔を示します。範囲は、1 ～ 120 秒です。
lsp-initial-wait	（オプション）初期 LSP 生成の遅延を示します。値の範囲は 1 ～ 120,000 ミリ秒です。
lsp-second-wait	（オプション）最初と 2 番めの LSP 生成間のホールド タイムを示します。値の範囲は 1 ～ 120,000 ミリ秒です。

コマンド デフォルト

lsp-max-wait：5 秒

lsp-initial-wait：50 ミリ秒

lsp-second-wait：5000 ミリ秒

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。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

次の説明を参照して、このコマンドのデフォルト値を変更するかどうか決定する際の参考にしてください。

- l*sp-initial-wait* 引数は、最初の LSP を生成する前の初期待機時間を表します。
- 3 番めの引数は、最初と 2 番めの LSP 生成間の待機時間を示します。
- 後続の各待機時間は、*lsp-max-wait* 時間の指定値に到達するまで、直前の間隔の 2 倍になります。したがって、初回および2回目の間隔後にLSPの生成は減速されます。最大時間に到達すると、ネットワークが安定するまで、待機時間は最大値のままとなります。
- ネットワークが安定し、*lsp-max-wait* 時間 2 回の間トリガーがなければ、高速動作（最初の待機時間）に戻ります。

例

次に、LSP 生成スロットリングの時間の間隔を設定する例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# lsp-gen-interval 2 50 100
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
authentication key	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルなIS-ISインスタンスでは、送信される（受信ではなく）IS-ISパケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-ISプロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。

コマンド	説明
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。

コマンド	説明
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更（アップまたはダウン）する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト（TLV）を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。

コマンド	説明
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

lsp-refresh-interval

LSP の更新間隔を設定するには、ルータ ISIS コンフィギュレーション モードで **lsp-refresh-interval** コマンドを使用します。デフォルトのリフレッシュ間隔に戻すには、このコマンドの **no** 形式を使用します。

lsp-refresh-interval *seconds*
no lsp-refresh-interval

構文の説明

seconds	LSP がリフレッシュされる間隔。範囲は 1 ～ 65535 秒です。

コマンド デフォルト

デフォルト値は 900 秒（15 分）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。

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	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

リフレッシュ間隔によって、ソフトウェアが定期的に LSP で発信元のルート トポロジ情報を送信するレートが決定されます。これは、データベース情報が古くなるのを避けるために実行されます。

（注） LSP は、ライフタイムが経過するまで定期的にリフレッシュされる必要があります。**lsp-refresh-interval** コマンドに対して設定される値は、**max-lsp-lifetime** コマンドに対して設定される値よりも小さな値である必要があり、そうでない場合、リフレッシュされる前に LSP がタイムアウトします。LSP 間隔と比べて LSP ライフタイムを大幅に少なく設定する場合、ソフトウェアが LSP リフレッシュ間隔を減らして、LSP がタイムアウトしないようにします。

例

次に、IS-IS LSP リフレッシュ間隔を 1080 秒に設定する例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# lsp-refresh-interval 1080
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
authentication key	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。

コマンド	説明
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更（アップまたはダウン）する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。

コマンド	説明
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が ASA のデータベースに更新されずに存在する最長時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト（TLV）を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。

コマンド	説明
summary-address	IS-IS の集約アドレスを作成します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。