ロギング

この章では、システム メッセージを記録して、トラブルシューティングに使用する方法について説明します。

ロギングの概要

システム ロギングは、デバイスから syslog デーモンを実行するサーバへのメッセージを収集する方法です。中央の syslog サーバへロギングは、ログおよびアラートの集約に役立ちます。シスコ デバイスでは、これらのログ メッセージを UNIX スタイルの syslog サービスに送信できます。syslog サービスは、シンプル コンフィギュレーション ファイルに従って、メッセージを受信してファイルに保存するか、出力します。この形式のロギングは、保護された長期的な保存場所をログに提供します。ログは、ルーチン トラブルシューティングおよびインシデント処理の両方で役立ちます。

ASAのシステム ログにより、ASAのモニタリングおよびトラブルシューティングで必要な情報を得ることができます。ロギング機能を使用して、次の操作を実行できます。

- ログに記録する syslog メッセージを指定する。
- Syslog メッセージの重大度のディセーブル化または変更
- 次を含む、syslog メッセージ送信先となる、1 つ以上の場所を指定する。
  - 内部バッファ
  - 1 台以上の syslog サーバ
  - ASDM
  - SNMP 管理ステーション

- 指定の電子メール アドレス
- コンソール
- Telnet と SSH セッション

- 重大度レベルやメッセージ クラスなどによる、グループ内での syslog メッセージを設定および管理する。
- syslog の生成にレート制限を適用するかどうかを指定する。
- 内部ログ バッファがいっぱいになった場合に、その内容に対して実行する処理（バッファを上書きする、バッファの内容を FTP サーバに送信する、または内容を内部フラッシュ メモリに保存する）を指定する。
- 場所、重大度レベル、クラス、またはカスタム メッセージ リストにより、syslog メッセージをフィルタリングする。

マルチ コンテキスト モードでのロギング

それぞれのセキュリティ コンテキストには、独自のロギング コンフィギュレーションが含まれており、独自のメッセージが生成されます。システム コンテキストまたは管理コンテキストにログインし、別のコンテキストに変更した場合、セッションで表示されるメッセージは現在のコンテキストに関連するメッセージに限定されます。

システム実行スペースで生成されるフェールオーバー メッセージなどの syslog メッセージは、管理コンテキストで生成されるメッセージとともに管理コンテキストで表示できます。システム実行スペースでは、ロギングの設定やロギング情報の表示はできません。

ASA は、各メッセージとともにコンテキスト名を含めるように設定できます。これによって、単一の syslog サーバに送信されるコンテキスト メッセージを区別できます。この機能は、管理コンテキストから送信されたメッセージとシステムから送信されたメッセージの判別にも役立ちます。これが可能なのは、送信元がシステム実行スペースであるメッセージでは**システム**のデバイス ID が使用され、管理コンテキストが送信元であるメッセージではデバイス ID として管理コンテキストの名前が使用されるからです。

syslog メッセージ分析

次に、さまざまな syslog メッセージを確認することで取得できる情報タイプの例を示します。

- ASA セキュリティ ポリシーで許可された接続。これらのメッセージは、セキュリティ ポリシーで開いたままのホールを発見するのに役立ちます。
- ASA セキュリティ ポリシーで拒否された接続。これらのメッセージは、セキュアな内部ネットワークに転送されているアクティビティのタイプを示します。
- ACE 拒否率ロギング機能を使用すると、使用している ASA に対して発生している攻撃が表示されます。

- IDS アクティビティ メッセージには、発生した攻撃が示されます。
- ユーザ認証とコマンドの使用により、セキュリティ ポリシーの変更を監査証跡することができます。
- 帯域幅使用状況メッセージには、確立および切断された各接続のほか、使用された時間とトラフィック量が示されます。
- プロトコル使用状況メッセージには、各接続で使用されたプロトコルとポート番号が示されます。
- アドレス変換監査証跡メッセージは、確立または切断されている NAT または PAT 接続を記録します。この情報は、内部ネットワークから外部に送信される悪意のあるアクティビティのレポートを受信した場合に役立ちます。

syslog メッセージ形式

syslog メッセージはパーセントの記号（%）で始まり、次のように構造化されています。

```
%ASA Level Message_number: Message_text
```

次の表に、フィールドの説明を示します。

ASA	ASA が生成するメッセージの syslog メッセージ ファシリティ コード。この値は常に ASA です。
Level	1 ～ 7。レベルは、syslog メッセージに記述されている状況の重大度を示します。値が低いほどその状況の重大度は高くなります。
Message_number	syslog メッセージを特定する 6 桁の固有の番号。
Message_text	状況を説明するテキスト文字列。syslog メッセージのこの部分には、IP アドレス、ポート番号、またはユーザ名が含まれていることがあります。

重大度

次の表に、syslog メッセージの重大度の一覧を示します。それぞれの重大度にカスタム カラーを割り当て、ASDM ログ ビューアで重大度を識別しやすくできます。syslog メッセージの色設定を行うには、[Tools] > [Preferences] > [Syslog] タブを選択するか、またはログ ビューア自体のツールバーで [Color Settings] をクリックします。

表 *1 : Syslog* メッセージの重大度

レベル番号	重大度	説明
0	**緊急**	システムが使用不可能な状態。
1	**アラート**	すぐに措置する必要があります。

レベル番号	重大度	説明
2	重大	深刻な状況です。
3	エラー	エラー状態です。
4	警告	警告状態。
5	通知	正常ですが、注意を必要とする状況です。
6	情報	情報メッセージです。
7	デバッグ	デバッグ メッセージです。

（注） ASAは、重大度 0（emergencies）の syslog メッセージを生成しません。

syslog メッセージ フィルタリング

生成される syslog メッセージは、特定の syslog メッセージだけが特定の出力先に送信されるようにフィルタリングできます。たとえば、ASAを設定して、すべての syslog メッセージを 1 つの出力先に送信し、それらの syslog メッセージのサブセットを別の出力先に送信することができます。

具体的には、syslog メッセージが次の基準に従って出力先に転送されるようにできます。

- syslog メッセージの ID 番号
- syslog メッセージの重大度
- syslog メッセージ クラス（機能エリアと同等）

これらの基準は、出力先を設定するときに指定可能なメッセージ リストを作成して、カスタマイズできます。あるいは、メッセージ リストとは無関係に、特定のメッセージ クラスを各タイプの出力先に送信するようにASAを設定することもできます。

syslog メッセージ クラス

syslog メッセージのクラスは次の 2 つの方法で使用できます。

- syslog メッセージのカテゴリ全体の出力場所を指定します。**logging class** コマンドを使用します。
- メッセージ クラスを指定するメッセージ リストを作成します。**logging list** コマンドを使用します。

syslog メッセージ クラスは、デバイスの特徴または機能と同等のタイプによって syslog メッセージを分類する方法を提供します。たとえば、RIP クラスは RIP ルーティングを示します。

特定のクラスに属する syslog メッセージの ID 番号はすべて、最初の 3 桁が同じです。たとえば、611 で始まるすべての syslog メッセージ ID は、vpnc（VPN クライアント）クラスに関連付けられています。VPN クライアント機能に関連付けられている syslog メッセージの範囲は、611101 ～ 611323 です。

また、ほとんどの ISAKMP syslog メッセージには先頭に付加されたオブジェクトの共通セットが含まれているため、トンネルを識別するのに役立ちます。これらのオブジェクトは、使用可能なときに、syslog メッセージの説明テキストの前に付加されます。syslog メッセージ生成時にオブジェクトが不明な場合、特定の heading = value の組み合わせは表示されません。

オブジェクトは次のように先頭に付加されます。

Group = *groupname*, Username = *user*, IP = *IP_address*

Group はトンネル グループ、Username はローカル データベースまたは AAA サーバから取得したユーザ名、IP アドレスはリモート アクセス クライアントまたはレイヤ 2 ピアのパブリック IP アドレスです。

次の表に、メッセージ クラスと各クラスのメッセージ ID の範囲をリストします。

表 *2 : syslog* メッセージ クラスおよび関連付けられているメッセージ *ID* 番号

クラス	定義	Syslog メッセージ ID 番号
auth	User Authentication	109、113
—	アクセス リスト	106
—	アプリケーション ファイアウォール	415
bridge	トランスペアレント ファイアウォール	110、220
ca	PKI 認証局	717
citrix	Citrix Client	723
—	クラスタ	747
—	カード管理	323
config	コマンド インターフェイス	111、112、208、308
csd	Secure Desktop	724
cts	Cisco TrustSec	776
dap	ダイナミック アクセス ポリシー	734
eap、eapoudp	ネットワーク アドミッション コントロールの EAP または EAPoUDP	333、334
eigrp	EIGRP ルーティング	336

クラス	定義	Syslog メッセージ ID 番号
電子メール	電子メール プロキシ	719
—	環境モニタリング	735
ha	フェールオーバー	101、102、103、104、105、210、311、709
—	Identity-Based ファイアウォール	746
ids	侵入検知システム	400、733
—	IKEv2 ツールキット	750、751、752
ip	IP スタック	209、215、313、317、408
ipaa	IP アドレス割り当て	735
ips	侵入防御システム	400、401、420
—	IPv6	325
—	ブラック リスト、ホワイト リスト、およびグレー リスト	338
—	ライセンス	444
mdm-proxy	MDM プロキシ	802
nac	ネットワーク アドミッション コントロール	731、732
nacpolicy	NAC ポリシー	731
nacsettings	NAC ポリシーを適用する NAC 設定	732
—	ネットワーク アクセス ポイント	713
np	ネットワーク プロセッサ	319
—	NP SSL	725
ospf	OSPF ルーティング	318、409、503、613
—	パスワードの暗号化	742
—	電話プロキシ	337
rip	RIP ルーティング	107、312
rm	Resource Manager	321
—	Smart Call Home	120

クラス	定義	Syslog メッセージ ID 番号
session	ユーザ セッション	106、108、201、202、204、302、303、304、305、314、405、406、407、500、502、607、608、609、616、620、703、710
snmp	SNMP	212
—	ScanSafe	775
ssl	SSL スタック	725
svc	SSL VPN クライアント	722
sys	システム	199、211、214、216、306、307、315、414、604、605、606、610、612、614、615、701、711、741
—	脅威の検出	733
tre	トランザクション ルール エンジン	780
—	UC-IME	339
tag-switching	サービス タグ スイッチング	779
vm	VLAN マッピング	730
vpdn	PPTP および L2TP セッション	213、403、603
vpn	IKE および IPsec	316、320、402、404、501、602、702、713、714、715
vpnc	VPN クライアント	611
vpnfo	VPN フェールオーバー	720
vpnlb	VPN ロード バランシング	718
—	VXLAN	778
webfo	WebVPN フェールオーバー	721
webvpn	WebVPN と AnyConnect Client	716
—	NAT および PAT	305

カスタム メッセージ リスト

カスタム メッセージ リストを作成して、送信する syslog メッセージとその出力先を柔軟に制御できます。カスタム syslog メッセージのリストで、次の条件のいずれかまたはすべてを使用して syslog メッセージのグループを指定します。

- 重大度
- メッセージ ID
- syslog メッセージ ID の範囲
- メッセージ クラス

たとえば、メッセージ リストを使用して次の操作を実行できます。

- 重大度が 1 および 2 の syslog メッセージを選択し、1 つ以上の電子メール アドレスに送信する。
- メッセージ クラス（「ha」など）に関連付けられたすべての syslog メッセージを選択し、内部バッファに保存する。

メッセージ リストには、メッセージを選択するための複数の基準を含めることができます。ただし、メッセージ選択基準の追加は、それぞれ個別のコマンドエントリで行う必要があります。重複したメッセージ選択基準を含むメッセージ リストが作成される可能性もあります。メッセージリストの 2 つの基準によって同じメッセージが選択される場合、そのメッセージは一度だけログに記録されます。

クラスタ

syslog メッセージは、クラスタリング環境でのアカウンティング、モニタリング、およびトラブルシューティングのための非常に重要なツールです。クラスタ内の各 ASA ユニット（最大 8 ユニットを使用できます）は、syslog メッセージを個別に生成します。特定の **logging** コマンドを使用すると、タイム スタンプおよびデバイス ID を含むヘッダー フィールドを制御できます。syslog サーバは、syslog ジェネレータを識別するためにデバイス ID を使用します。**logging device-id** コマンドを使用すると、同一または異なるデバイス ID 付きで syslog メッセージを生成することができ、クラスタ内の同一または異なるユニットからのメッセージのように見せることができます。

ロギングのガイドライン

この項では、ロギングを設定する前に確認する必要のある制限事項とガイドラインについて説明します。

IPv6 のガイドライン

IPv6 はサポートされません。

その他のガイドライン

- syslogサーバでは、syslogdというサーバプログラムを実行する必要があります。Windowsでは、オペレーティング システムの一部として syslog サーバを提供しています。
- ASAが生成したログを表示するには、ロギングの出力先を指定する必要があります。ロギングの出力先を指定せずにロギングをイネーブルにすると、ASAはメッセージを生成しますが、それらのメッセージは後で表示できる場所に保存されません。各ロギングの出力先は個別に指定する必要があります。たとえば、出力先として複数のsyslogサーバを指定するには、新しいコマンドを入力し、で、個別のエントリを指定します。
- スタンドバイ デバイスでは、TCP 上での syslog の送信はサポートされません。
- 2 つの異なるリストまたはクラスを、異なる syslog サーバまたは同じロケーションに割り当てることはできません。
- 最大 16 台の syslog サーバを設定できます。ただし、マルチ コンテキスト モードでは、コンテキストごとに 4 サーバに制限されています。
- syslog サーバは、ASA 経由で到達できなければなりません。syslog サーバが到達できるインターフェイス上で、デバイスがICMP到達不能メッセージを拒否し、同じサーバにsyslogを送信するように設定する必要があります。すべての重大度に対してロギングがイネーブルであることを確認します。syslog サーバがクラッシュしないようにするため、syslog 313001、 313004、および 313005 の生成を抑制します。
- syslogのUDP接続の数は、ハードウェア プラットフォームのCPUの数と、設定するsyslogサーバの数に直接関連しています。可能な UDP syslog 接続の数は常に、CPU の数と設定するsyslogサーバの数を乗算した値と同じになります。たとえば各syslogサーバでは次のようになります。
  - ASA 5585-SSP-10 では最大 4 つの UDP syslog 接続が可能です。
  - Firepower 4110 では最大 22 の UDP syslog 接続が可能です。
  - Firepower 4120 では最大 46 の UDP syslog 接続が可能です。

  これは予期されている動作です。グローバル UDP 接続アイドル タイムアウトはこれらのセッションに適用され、デフォルトは2分であることに注意してください。これらのセッションをこれよりも短い時間で閉じる場合にはこの設定を調整できますが、タイムアウトは syslog だけでなくすべての UDP 接続に適用されます。
- アクセス リストのヒット数だけを照合するためにカスタム メッセージ リストを使用すると、ロギング重大度がデバッグ（レベル7）のアクセスリストに対しては、アクセスリストのログは生成されません。**logging list** コマンドのロギング重大度のデフォルトは、6 に設定されています。このデフォルト動作は設計によるものです。アクセスリストコンフィギュレーションのロギング重大度をデバッグに明示的に変更する場合は、ロギング コンフィギュレーション自体も変更する必要があります。

  ロギング重大度がデバッグに変更されたため、アクセスリストのヒットが含まれていない **show running-config logging** コマンドの出力例を次に示します。

```
ciscoasa# show running-config logging
logging enable
logging timestamp
logging list test message 106100
logging buffered test
```

次に、アクセス リスト ヒットを含む **show running-config logging** コマンドの出力例を示します。

```
ciscoasa# show running-config logging
logging enable
logging timestamp
logging buffered debugging
```

この場合、アクセス リスト コンフィギュレーションは変更せず、アクセス リスト ヒット数が次の例のように表示されます。

```
ciscoasa(config)# access-list global line 1 extended
permit icmp any host 4.2.2.2 log debugging interval 1 (hitcnt=7) 0xf36b5386
ciscoasa(config)# access-list global line 2 extended
permit tcp host 10.1.1.2 any eq www log informational interval 1 (hitcnt=18) 0xe7e7c3b8
ciscoasa(config)# access-list global line 3 extended
permit ip any any (hitcnt=543) 0x25f9e609
```

- ASA が TCP 経由で syslog を送信すると、syslogd サービスの再起動後、接続の開始に約 1 分かかります。
- syslog サーバから受信したサーバ証明書は、[Extended Key Usage] フィールドに「ServAuth」を含める必要があります。このチェックは、自己署名証明書以外の証明書にのみ実行されます。自己署名証明書の場合、このフィールドに値は表示されません。

ロギングの設定

ここでは、ロギングの設定方法について説明します。

Enable Logging

ロギングをイネーブルにするには、次の手順を実行します。

手順

ロギングをイネーブルにします。

logging enable

例：

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

出力先の設定

トラブルシューティングおよびパフォーマンスのモニタリング用にsyslogメッセージの使用状況を最適化するには、syslog メッセージの送信先（内部ログ バッファ、1 つまたは複数の外部syslogサーバ、ASDM、SNMP管理ステーション、コンソール ポート、指定した電子メール アドレス、または Telnet および SSH セッションなど）を 1 つまたは複数指定することをお勧めします。

外部 syslog サーバへの syslog メッセージの送信

外部 syslog サーバで利用可能なディスク領域に応じてメッセージをアーカイブし、その保存後、ロギング データを操作できます。たとえば、特定タイプの syslog メッセージがログに記録されたり、ログからデータが抽出されてレポート用の別のファイルにその記録が保存されたり、あるいはサイト固有のスクリプトを使用して統計情報が追跡されたりした場合に、特別なアクションが実行されるように指定できます。

外部 syslog サーバに syslog メッセージを送信するには、次の手順を実行します。

手順

ステップ 1 syslog サーバにメッセージを送信するために ASA を設定します。

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

例：

```
ciscoasa(config)# logging host dmz1 192.168.1.5 udp/1026
```

format emblem キーワードは、UDP 限定で syslog サーバでの EMBLEM 形式ロギングを有効にします。*interface_name* 引数には、syslog サーバにアクセスするときのインターフェイスを指定します。*syslog_ip* 引数には、syslog サーバの IP アドレスを指定します。**tcp**[/*port*] または **udp**[/*port*] キーワードと引数のペアは、syslogサーバにsyslogメッセージを送信するためにASAで TCP を使用するか、UDP を使用するかを指定します。

UDP または TCP のいずれかを使用して syslog サーバにデータを送信するように ASA を設定することはできますが、両方を使用するように設定することはできません。プロトコルを指定しない場合、デフォルトのプロトコルは UDP です。

TCP を指定すると、ASA は syslog サーバの障害を検出し、セキュリティ保護として ASA 経由の新しい接続をブロックします。TCP syslog サーバへの接続に関係なく新しい接続を許可するには、手順 3 を参照してください。UDP を指定すると、ASA は、syslog サーバが動作しているかどうかに関係なく新しい接続を許可し続けます。有効なポート値は、どちらのプロトコル

でも 1025 ～ 65535 です。デフォルトの UDP ポートは 514 です。デフォルトの TCP ポートは 1470 です。

ステップ 2 syslog サーバに送信する syslog メッセージを指定します。

logging trap {*severity_level* | *message_list*}

例：

```
ciscoasa(config)# logging trap errors
```

重大度として、値（1 ～ 7）または名前を指定できます。たとえば重大度を 3 に設定すると、ASA は、重大度が 3、2、および 1 の syslog メッセージを送信します。syslog サーバに送信する syslog メッセージを特定したカスタム メッセージ リストを指定することもできます。

ステップ 3 （オプション）TCP接続されたsyslogサーバがダウンした場合、新しい接続をブロックする機能をディセーブルにします。

logging permit-hostdown

例：

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

ASA が syslog メッセージを TCP ベースの syslog サーバに送信するように設定されている場合、およびsyslogサーバがダウンしているか、ログキューがいっぱいの場合、新しい接続はブロックされます。新しい接続は、syslog サーバがバック アップされ、ログ キューがいっぱいでなくなった後に再度許可されます。

ステップ 4 （オプション）ロギング ファシリティを20以外の値に設定します。これは、ほとんどのUNIXシステムで想定されています。

logging facility *number*

例：

```
ciscoasa(config)# logging facility 21
```

セキュア ロギングの有効化

手順

logging host コマンドで **secure** キーワードを指定して、セキュア ロギングを有効にします。また、必要に応じて **reference-identity** を入力します。

logging host *interface_name syslog_ip* [**tcp**/*port* | **udp**/*port*] [**format emblem**] [**secure**[**reference-identity** *reference_identity_name*]]

それぞれの説明は次のとおりです。

- **logging host***interface_name syslog_ip* には、syslog サーバが常駐するインターフェイスと syslog サーバの IP アドレスを指定します。
- [**tcp**/*port* | **udp**/*port*] には、syslog サーバが syslog メッセージをリスンするポート（TCP または UDP）を指定します。**tcp** キーワードは、ASA が TCP を使用して syslog メッセージを syslog サーバに送信することを指定します。**udp** キーワードは、ASA が UDP を使用して syslog メッセージを syslog サーバに送信することを指定します。
- **format emblem** キーワードは、syslog サーバに対して EMBLEM 形式のロギングを有効にします。
- **secure** キーワードは、リモート ロギング ホストへの接続で、TCP の場合にだけ SSL/TLS を使用するように指定します。セキュア ロギングでは UDP をサポートしていないため、このプロトコルを使用しようとするとエラーが発生します。
- [**reference-identity** *reference_identity_name*] は、以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く証明書での RFC 6125 参照アイデンティティ検査を有効にします。参照 ID オブジェクトについて詳しくは、参照 ID の設定を参照してください。

例：

```
ciscoasa(config)# logging host inside 10.0.0.1 TCP/1500 secure  reference-identity
syslogServer
```

syslog サーバに送信する EMBLEM 形式の syslog メッセージの生成

syslog サーバへの EMBLEM 形式の syslog メッセージを生成するには、次の手順を実行します。

手順

EMBLEM 形式の syslog メッセージを、UDP のポート 514 を使用して syslog サーバに送信します。

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

例：

```
ciscoasa(config)# logging host interface_1 127.0.0.1 udp format emblem
ciscoasa(config)# logging host interface_1 2001::1 udp format emblem
```

format emblem キーワードは、syslog サーバでの EMBLEM 形式ロギングを有効にします（UDP 限定）。*interface_name* 引数には、syslog サーバにアクセスするときのインターフェイスを指定します。*ip_address* 引数には、syslog サーバの IP アドレスを指定します。 **tcp**[/*port*] または **udp**[/*port*] キーワードと引数のペアは、syslog サーバに syslog メッセージを送信するために ASA で TCP を使用するか、UDP を使用するかを指定します。

UDP または TCP のいずれかを使用して syslog サーバにデータを送信するように ASA を設定することができます。プロトコルを指定しない場合、デフォルトのプロトコルは UDP です。

複数の **logging host** コマンドを使用して、syslog メッセージを受信するすべての追加サーバを指定できます。2つ以上のロギング サーバを設定する場合は、必ず、すべてのロギング サーバにおいて、ロギングの重大度の上限を warnings にしてください。

TCP を指定すると、ASA は syslog サーバの障害を検出し、セキュリティ保護として ASA を経由する新しい接続をブロックします。UDP を指定すると、ASA は、syslog サーバが動作しているかどうかに関係なく新しい接続を許可し続けます。有効なポート値は、どちらのプロトコルでも 1025 ～ 65535 です。デフォルトの UDP ポートは 514 です。デフォルトの TCP ポートは 1470 です。

他の出力先への EMBLEM 形式の syslog メッセージの生成

他の出力先への EMBLEM 形式の syslog メッセージを生成するには、次の手順を実行します。

手順

syslog サーバ以外の出力先（たとえば Telnet または SSH セッション）に EMBLEM 形式の syslog メッセージを送信します。

logging emblem

例：

```
ciscoasa(config)# logging emblem
```

内部ログ バッファへの syslog メッセージの送信

一時的な保存場所となる内部ログ バッファに送信する syslog メッセージを指定する必要があります。新しいメッセージは、リストの最後に追加されます。バッファがいっぱいになったとき、つまりバッファ ラップが発生した場合、ASA がいっぱいになったバッファを別の場所に保存するように設定されていない限り、古いメッセージは生成される新しいメッセージによって上書きされます。

syslog メッセージを内部ログ バッファに送信するには、次の手順を実行します。

手順

ステップ 1 一時的な保存場所となる内部ログ バッファに送信する syslog メッセージを指定します。

logging buffered {*severity_level* | *message_list*}

例：

```
ciscoasa(config)# logging buffered critical
ciscoasa(config)# logging buffered level 2
```

```
ciscoasa(config)# logging buffered notif-list
```

新しいメッセージは、リストの最後に追加されます。バッファがいっぱいになったとき、つまりバッファ ラップが発生した場合、ASA がいっぱいになったバッファを別の場所に保存するように設定されていない限り、古いメッセージは生成される新しいメッセージによって上書きされます。内部ログ バッファを空にするには、**clear logging buffer** コマンドを入力します。

ステップ 2 内部ログ バッファのサイズを変更します。デフォルトのバッファ サイズは 4 KB です。

logging buffer-size *bytes*

例：

```
ciscoasa(config)# logging buffer-size 16384
```

ステップ 3 次のいずれかのオプションを選択します。

- 新しいメッセージを内部ログ バッファに保存し、いっぱいになったログ バッファの内容を内部フラッシュ メモリに保存します。

  logging flash-bufferwrap

  例：

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

- 新しいメッセージを内部ログ バッファに保存し、いっぱいになったログ バッファの内容を FTP サーバに保存します。

  logging ftp-bufferwrap

  例：

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

  バッファの内容を別の場所に保存するとき、ASA は、次のタイムスタンプ形式を使用する名前でログ ファイルを作成します。

  ```
  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。

- ログ バッファの内容を保存する FTP サーバを指定します。

  logging ftp-server *server pathusername password*

  例：

  ```
  ciscoasa(config)# logging ftp-server 10.1.1.1 /syslogs logsupervisor 1luvMy10gs
  ```

server 引数には、外部 FTP サーバの IP アドレスを指定します。*path* 引数には、ログ バッファのデータを保存する FTP サーバへのディレクトリ パスを指定します。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。*username* 引数には、FTP サーバへのロギングで有効なユーザ名を指定します。*password* 引数は、指定したユーザ名に対するパスワードを示します。

- 現在のログ バッファの内容を内部フラッシュ メモリに保存します。

  logging savelog [*savefile*]

  例：

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

ログの記録で使用可能な内部フラッシュ メモリの容量の変更

ログの記録で使用可能な内部フラッシュ メモリの容量を変更するには、次の手順を実行します。

手順

ステップ 1 ログ ファイルの保存で使用可能な内部フラッシュ メモリの最大容量を指定します。

logging flash-maximum-allocation *kbytes*

例：

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

デフォルトでは、ASAは、内部フラッシュメモリの最大1MBをログデータに使用できます。ASA でログ データを保存するために必要な内部フラッシュ メモリの最小空き容量は 3 MB です。

内部フラッシュ メモリに保存されているログ ファイルにより、内部フラッシュ メモリの空き容量が設定された最小限の容量を下回ってしまう場合、ASA は最も古いログ ファイルを削除し、新しいログファイルの保存後も最小限の容量が確保されるようにします。削除するファイルがない場合、または古いファイルをすべて削除しても空きメモリの容量が最小限の容量を下回っている場合、ASA はその新しいログファイルを保存できません。

ステップ 2 ASAでログファイルを保存するために必要な内部フラッシュメモリの最小空き容量を指定します。

logging flash-minimum-free *kbytes*

例：

```
ciscoasa(config)# logging flash-minimum-free 4000
```

電子メール アドレスへの syslog メッセージの送信

syslog メッセージを電子メール アドレスに送信するには、次の手順を実行します。

手順

ステップ 1 電子メール アドレスに送信する syslog メッセージを指定します。

logging mail {*severity_level* | *message_list*}

例：

```
ciscoasa(config)# logging mail high-priority
```

電子メールで送信される場合、syslogメッセージは電子メールメッセージの件名行に表示されます。このため、このオプションでは、critical、alert、および emergency など、重大度の高い syslog メッセージを管理者に通知するように設定することをお勧めします。

ステップ 2 電子メール アドレスに syslog メッセージを送信するときに使用する送信元電子メール アドレスを指定します。

logging from-address *email_address*

例：

```
ciscoasa(config)# logging from-address xxx-001@example.com
```

ステップ 3 電子メール アドレスに syslog メッセージを送信するときに使用する宛先の電子メール アドレスを指定します。

logging recipient-address *e-mail_address*[*severity_level*]

例：

```
ciscoasa(config)# logging recipient-address admin@example.com
```

ステップ 4 電子メール アドレスに syslog メッセージを送信するときに使用する SMTP サーバを指定します。

例：

```
ciscoasa(config)# smtp-server 10.1.1.24
```

ASDM への syslog メッセージの送信

syslog メッセージを ASDM に送信するには、次の手順を実行します。

手順

ステップ 1 ASDM に送信する syslog メッセージを指定します。

logging asdm {*severity_level* | *message_list*}

例：

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

ASA は、ASDM への送信を待機している syslog メッセージのバッファ領域を確保し、メッセージが生成されるとバッファに保存します。ASDM ログ バッファは、内部ログ バッファとは別のバッファです。ASDM のログバッファがいっぱいになると、ASA は最も古い syslog メッセージを削除し、新しい syslog メッセージのバッファ領域を確保します。最も古い syslog メッセージを削除して新しい syslog メッセージのためのスペースを確保するのは、ASDM のデフォルト設定です。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ために、バッファのサイズを変更できます。

ステップ 2 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。

logging asdm-buffer-size *num_of_msgs*

例：

```
ciscoasa(config)# logging asdm-buffer-size 200
```

ASDM ログ バッファの現在の内容を空にするには、**clear logging asdm** コマンドを入力します。

ロギング キューの設定

ロギング キューを設定するには、次の手順を実行します。

手順

設定された出力先に送信されるまでの間、ASA がそのキューに保持できる syslog メッセージの数を指定します。

logging queue *message_count*

例：

```
ciscoasa(config)# logging queue 300
```

ASA のメモリ内には、設定された出力先への送信を待機している syslog メッセージをバッファするために割り当てられる、一定数のブロックがあります。必要なブロックの数は、syslog メッセージ キューの長さと、指定した syslog サーバの数によって異なります。デフォルトのキューのサイズは 512 syslog メッセージです。キューのサイズは、使用可能なブロック メモリのサイズが上限です。有効値は 0 ～ 8192 メッセージです。値はプラットフォームによって異なります。ロギング キューをゼロに設定した場合、その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。

コンソール ポートへの syslog メッセージの送信

syslog メッセージをコンソール ポートに送信するには、次の手順を実行します。

手順

コンソール ポートに送信する syslog メッセージを指定します。

logging console { *severity_level* | *message_list*}

例：

```
ciscoasa(config)# logging console errors
```

SNMP サーバへの syslog メッセージの送信

SNMP サーバへのロギングをイネーブルにするには、次の手順を実行します。

手順

SNMP ロギングをイネーブルにし、SNMP サーバに送信するメッセージを指定します。

logging history [*logging_list* | *level*]

例：

```
ciscoasa(config)# logging history errors
```

SNMP ロギングを無効にするには、**no logging history** コマンドを入力します。

Telnet または SSH セッションへの syslog メッセージの送信

syslog メッセージを Telnet または SSH セッションに送信するには、次の手順を実行します。

手順

ステップ 1 Telnet または SSH セッションに送信する syslog メッセージを指定します。

logging monitor {*severity_level* | *message_list*}

例：

```
ciscoasa(config)# logging monitor 6
```

ステップ 2 現在のセッションへのロギングだけをイネーブルにします。

terminal monitor

例：

```
ciscoasa(config)# terminal monitor
```

一度ログアウトして再びログインする場合は、このコマンドを再入力する必要があります。現在のセッションへのロギングを無効にするには、**terminal no monitor** コマンドを入力します。

syslog メッセージの設定

Syslog での無効なユーザ名の表示または非表示

ログイン試行に失敗した場合の無効なユーザ名をsyslogメッセージに表示または非表示にできます。デフォルト設定では、ユーザ名が無効な場合、または有効かどうか不明な場合、ユーザ名は非表示です。たとえば、ユーザが誤ってユーザ名の代わりにパスワードを入力した場合、結果として生成されるsyslogメッセージで「ユーザ名」を隠すのが安全です。ログインに関するトラブルシューティングに役立てるために、無効なユーザ名を表示することもできます。

手順

ステップ 1 無効なユーザ名を表示するには、次のようにします。

no logging hide username

ステップ 2 無効なユーザ名を非表示にするには、次のようにします。

logging hide username

syslog メッセージに日付と時刻を含める

syslog メッセージに日付と時刻を含めるには、次の手順を実行します。

手順

syslog メッセージにメッセージが生成された日付と時刻が含まれるように指定します。

logging timestamp

例：

```
ciscoasa(config)# logging timestamp
LOG-2008-10-24-081856.TXT
```

syslog メッセージから日付と時刻を削除するには、**no logging timestamp** コマンドを入力します。

syslog メッセージの無効化

指定した syslog メッセージをディセーブルにするには、次の手順を実行します。

手順

ASA が特定の syslog メッセージを生成しないように指定します。

no logging message *syslog_id*

例：

```
ciscoasa(config)# no logging message 113019
```

無効にした syslog メッセージを再び有効にするには、**logging message** *syslog_id* コマンドを入力します（例：**logging message 113019**）。無効にしたすべての syslog メッセージのロギングを再び有効にするには、**clear configure logging disabled** コマンドを入力します。

syslog メッセージの重大度の変更

syslog メッセージの重大度を変更するには、次の手順を実行します。

手順

syslog メッセージの重大度を指定します。

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

例：

```
ciscoasa(config)# logging message 113019 level 5
```

syslog メッセージの重大度をその設定にリセットするには、**no logging message** *syslog_id* **level** *severity_level* コマンド（**no logging message 113019 level 5** など）を入力します。変更されたすべての syslog メッセージの重大度をそれぞれの設定にリセットするには、**clear configure logging level** コマンドを入力します。

スタンバイ装置の syslog メッセージのブロック

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するには、次の手順を実行します。

手順

スタンバイ装置での生成を以前ブロックされていた特定の syslog メッセージのブロックを解除します。

logging message *syslog-id* **standby**

例：

```
ciscoasa(config)# logging message 403503 standby
```

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。

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 メッセージの同期が継続されるようにするには、**logging standby** コマンドを使用します。

（注） **logging standby** コマンドを使用すると、syslog サーバ、SNMP サーバ、FTP サーバ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。

非 EMBLEM 形式の syslog メッセージにデバイス ID を含める

デバイス ID を非 EMBLEM 形式の syslog メッセージに含めるには、次の手順を実行します。

手順

デバイス ID を非 EMBLEM 形式の syslog メッセージに含めるように ASA を設定します。syslog メッセージに対して指定できるデバイス ID のタイプは 1 つだけです。

logging device-id {**cluster-id** | **context-name** | **hostname** | **ipaddress** *interface_name* [**system**] | **string** *text*}

例：

```
ciscoasa(config)# logging device-id hostname
ciscoasa(config)# logging device-id context-name
```

context-name キーワードは、現在のコンテキストの名前をデバイス ID として使用することを示します（マルチ コンテキスト モードにだけ適用されます）。マルチ コンテキスト モードの管理コンテキストでデバイス ID のロギングをイネーブルにすると、そのシステム実行スペースで生成されるメッセージは**system**のデバイス ID を使用し、管理コンテキストで生成されるメッセージは管理コンテキストの名前をデバイス ID として使用します。

（注） ASA クラスタでは、選択したインターフェイスのマスター ユニットの IP アドレスを常に使用します。

cluster-id キーワードは、デバイス ID として、クラスタの個別の ASA ユニットのブート設定に一意の名前を指定します。**hostname** キーワードは、ASA のホスト名をデバイス ID として使用するように指定します。**ipaddress** *interface_name* キーワード引数のペアは、*interface_name* として指定されたインターフェイスの IP アドレスをデバイス ID として使用することを指定します。**ipaddress** キーワードを使用すると、syslog メッセージの送信元となるインターフェイスに関係なく、そのデバイス ID は指定された ASA のインターフェイス IP アドレスとなります。クラスタ環境では、**system** キーワードは、デバイス ID がインターフェイスのシステム IP アドレスとなることを指定します。このキーワードにより、デバイスから送信されるすべての syslog メッセージに単一の一貫したデバイス ID を指定できます。**string** *text* キーワード引数のペアは、テキスト文字列をデバイス ID として使用することを指定します。文字列の長さは、最大で 16 文字です。

空白スペースを入れたり、次の文字を使用したりすることはできません。

- &（アンパサンド）
- '（一重引用符）
- "（二重引用符）
- <（小なり記号）
- >（大なり記号）
- ?（疑問符）

（注） イネーブルにすると、EMBLEM 形式の syslog メッセージや SNMP トラップにデバイス ID は表示されません。

カスタム イベント リストの作成

イベント リストの定義には、次の 3 つの基準を使用します。

- イベント クラス
- 重大度
- メッセージ ID

特定のロギングの宛先（SNMP サーバなど）に送信するカスタム イベント リストを作成するには、次の手順を実行します。

手順

ステップ 1 内部ログ バッファに保存されるメッセージの選択基準を指定します。たとえば重大度を 3 に設定すると、ASA は、重大度が 3、2、および 1 の syslog メッセージを送信します。

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

例：

```
ciscoasa(config)# logging list list-notif level 3
```

name 引数には、リストの名前を指定します。**level** *level* キーワードと引数のペアは、重大度を指定します。**class** *message_class* キーワードと引数のペアは、特定のメッセージ クラスを指定します。**message** *start_id* [-*end_id*] キーワードと引数のペアは、個々の syslog メッセージ番号または番号の範囲を指定します。

（注） 重大度の名前を syslog メッセージ リストの名前として使用しないでください。使用禁止の名前には、emergencies、alert、critical、error、warning、notification、informational、および debugging が含まれます。同様に、イベント リスト名の先頭にこれらの単語の最初の 3 文字は使用しないでください。たとえば、「err」で始まるイベント リスト名は使用しないでください。

ステップ 2 （オプション）リストにメッセージの選択基準をさらに追加します。

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

例：

```
ciscoasa(config)# logging list list-notif message 104024-105999
ciscoasa(config)# logging list list-notif level critical
ciscoasa(config)# logging list list-notif level warning class ha
```

前回の手順で使用したものと同じコマンドを入力し、既存のメッセージリストの名前と追加基準を指定します。リストに追加する基準ごとに、新しいコマンドを入力します。たとえば、リストに追加される syslog メッセージの基準として、次の基準を指定できます。

- ID が 104024 ～ 105999 の範囲の syslog メッセージ。
- 重大度が critical 以上（emergency、alert、または critical）のすべての syslog メッセージ。
- 重大度が warning 以上（emergency、alert、critical、error、または warning）のすべての ha クラスの syslog メッセージ。

（注） syslog メッセージは、これらの条件のいずれかを満たす場合にログに記録されます。syslog メッセージが複数の条件を満たす場合、そのメッセージは一度だけログに記録されます。

ロギング フィルタの設定

指定した出力先へのクラス内のすべての syslog メッセージの送信

クラス内のすべてのsyslogメッセージを指定した出力先に送信するには、次の手順を実行します。

手順

指定した出力先コマンドでコンフィギュレーションを上書きします。たとえば、重大度 7 のメッセージが内部ログ バッファに送信されるように指定し、重大度 3 の ha クラスのメッセージが内部ログバッファに送信されるように指定すると、後のコンフィギュレーションが優先されます。

logging class*message_class* {**buffered** |**console** |**history** |**mail** |**monitor** |**trap**} [*severity_level*]

例：

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

buffered、**history**、**mail**、**monitor**、および **trap** キーワードは、このクラスの syslog メッセージの出力先を指定します。**history** キーワードは、SNMP でのロギングを有効にします。**monitor** キーワードは、Telnet および SSH でのロギングを有効にします。**trap** キーワードは、syslog サーバでのロギングを有効にします。コマンドラインエントリあたり 1 つの出力先を指定します。1 つのクラスが複数の出力先に送信されるように指定する場合は、出力先ごとに新しいコマンドを入力します。

syslog メッセージの生成レートの制限

syslog メッセージの生成レートを制限するには、次の手順を実行します。

手順

指定された重大度（1～7）を、指定の時間内でメッセージセットまたは個々のメッセージ（出力先ではない）に適用します。

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

例：

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

レート制限は、すべての設定された出力先に送信されるメッセージの量に影響します。ロギング レート制限をデフォルト値にリセットするには、**clear running-config logging rate-limit** コマンドを入力します。ロギング レート制限をリセットするには、**clear configure logging rate-limit** コマンドを入力します。

ログのモニタリング

ロギング ステータスの監視については、次のコマンドを参照してください。

- **show logging**

  このコマンドは、重大度を含む syslog メッセージを表示します。

  （注） 表示できる syslog メッセージの最大数は、1000 です。これはデフォルト設定です。表示できる syslog メッセージの最大数は、2000 です。

- **show logging message**

  このコマンドは、変更された重大度とディセーブルにされた syslog メッセージを含む syslog メッセージのリストを示します。

- **show logging message** *message_ID*

  このコマンドは、特定の syslog メッセージの重大度を示します。

- **show logging queue**

  このコマンドは、ロギング キューとキュー統計情報を示します。

- **show running-config logging rate-limit**

このコマンドは、現在のロギング レート制限の設定を表示します。

ロギングの例

次の例は、**show logging** コマンドで表示されるロギング情報を示しています。

```
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
```

次の例は、syslog メッセージをイネーブルにするかどうかを制御する方法と、指定した syslog メッセージの重大度を制御する方法を示しています。

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

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

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

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

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

ロギングの履歴

表 *3:* ロギングの履歴

機能名	プラットフォーム リリース	説明
Logging	7.0(1)	さまざまな出力先を経由してASAネットワークロギング情報を提供します。ログファイルを表示して保存するオプションも含まれています。
レート制限	7.0(4)	syslog メッセージが生成されるレートを制限します。 **logging rate-limit** コマンドが導入されました。
ロギング リスト	7.2(1)	さまざまな基準（ロギング レベル、イベントクラス、およびメッセージID）でメッセージを指定するために他のコマンドで使用されるロギングリストを作成します。 次のコマンドが導入されました。 **logging list**
セキュア ロギング	8.0(2)	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。 **logging host** コマンドが変更されました。
ロギング クラス	8.0(4)、8.1(1)	ロギング メッセージの ipaa イベントクラスに対するサポートが追加されました。 **logging class** コマンドが変更されました。

機能名	プラットフォーム リリース	説明
ロギング クラスと保存されたロギング バッファ	8.2(1)	ロギング メッセージの dap イベント クラスに対するサポートが追加されました。 **logging class** コマンドが変更されました。 保存されたロギング バッファ（ASDM、内部、FTP、およびフラッシュ）をクリアする追加サポート。 **clear logging queue bufferwrap** コマンドが導入されました。
パスワードの暗号化	8.3(1)	パスワードの暗号化に対するサポートが追加されました。 **logging ftp server** コマンドが変更されました。
ログ ビューア	8.3(1)	送信元 IP アドレスおよび宛先 IP アドレスがログ ビューアに追加されました。

機能名	プラットフォーム リリース	説明
拡張ロギングと接続ブロック	8.3(2)	TCP を使用するように syslog サーバを設定すると、syslog サーバを使用できない場合、ASA はサーバが再び使用可能になるまで syslog メッセージを生成する新しい接続をブロックします（たとえば、VPN、ファイアウォール、カットスループロキシ接続）。この機能は、ASA のロギング キューがいっぱいのときにも新しい接続をブロックするように拡張されました。接続は、ロギング キューがクリアされると再開されます。 この機能は、Common Criteria EAL4+ への準拠のために追加されました。必要でない限り、syslog メッセージを送受信できない場合でも接続を許可することを推奨します。接続を許可するには、**logging permit-hostdown** コマンドを使用します。 414005、414006、414007、414008 の各 syslog メッセージが導入されました。 **show logging** コマンドが変更されました。
syslog メッセージのフィルタリングとソート	8.4(1)	次のサポートが追加されました。 • さまざまなカラムに対応する複数のテキスト文字列に基づく syslog メッセージ フィルタリング。 • カスタム フィルタの作成。 • メッセージのカラムによるソート。詳細については、『ASDM 構成ガイド』を参照してください。 この機能は、すべての ASA バージョンと相互運用性があります。

機能名	プラットフォーム リリース	説明
クラスタ	9.0(1)	ASA 5580 および 5585-X のクラスタリング環境での syslog メッセージ生成のサポートが追加されました。 **logging device-id** コマンドが変更されました。
スタンバイ装置の syslog のブロック	9.4(1)	フェールオーバー コンフィギュレーションのスタンバイ装置で特定の syslog メッセージの生成をブロックするためのサポートを追加しました。 **logging message** *syslog-id* **standby** コマンドが導入されました。
syslog サーバのセキュアな接続のための参照 ID	9.6(2)	TLS クライアント処理は、RFC 6125 のセクション 6 に定義されるサーバ ID の検証ルールをサポートするようになりました。ID 検証は、syslog サーバ サーバへの TLS 接続の PKI 確認中に実行されます。提示された ID が設定されたリファレンス ID と一致しない場合、接続を確立できません。 次のコマンドが追加または変更されました。**[no] crypto ca reference-identity**、**logging host**。
syslog サーバでの IPv6 アドレスのサポート	9.7(1)	TCP と UDP 経由で syslog を記録、送信、受信するために、syslog サーバを IPv6 アドレスで設定できるようになりました。 次のコマンドが変更されました。**logging host**