システムのモニタリング

ASA FirePOWER モジュールは、日常のシステム管理をサポートする多くの便利なモニタリング機能を、単一のページ上で提供します。たとえば、[ホスト統計情報（Host Statistics）] ページで、基本的なホストの統計情報をモニタできます。次の各項では、システムに備わっているモニタリング機能について詳しく説明します。

- ホスト統計情報の表示（47-1 ページ）では、次のようなホスト情報の表示方法について説明します。
- システム稼働時間
- ディスクおよびメモリの使用状況
- システム プロセス
- 侵入イベント情報
- システム ステータスとディスク領域使用率のモニタリング（47-2 ページ）では、基本的なイベントおよびディスク パーティションの情報を表示する方法について説明します。
- システム プロセス ステータスの表示（47-3 ページ）では、基本プロセスのステータスを表示する方法について説明します。
- 実行されるプロセスについて（47-5 ページ）では、アプライアンスで実行する基本システム プロセスについて説明します。

ホスト統計情報の表示

ライセンス：任意（Any）

[統計情報（Statistics）] ページには、次の内容の現在のステータスが表示されます。

- 一般的なホスト統計情報。詳細については、ホスト統計情報の表を参照してください
- 侵入イベント情報（Protection が必要）。詳細については、イベントの表示（37-1 ページ）を参照してください

次の表に、[統計情報（Statistics）] ページにリストされるホスト統計情報を示します。

表 47-1　ホスト統計情報

カテゴリ（Category）	説明
時刻（Time）	システムの現在の時刻。
Uptime（アップタイム）	システムが前回起動してから経過した日数（該当する場合）、時間数、および分数。
メモリ使用率（Memory Usage）	使用中のシステム メモリの割合。
負荷平均（Load Average）	直前の 1 分間、5 分間、15 分間の CPU キュー内の平均プロセス数。
ディスク使用率（Disk Usage）	使用中のディスクの割合。詳細なホスト統計情報を表示するには、矢印をクリックします。詳細については、システム ステータスとディスク領域使用率のモニタリング（47-2 ページ）を参照してください。
プロセス（Processes）	システムで実行されているプロセスの概要。詳細については、システム プロセス ステータスの表示（47-3 ページ）を参照してください。

[統計情報（Statistics）] ページを表示するには、次の手順を実行します。

手順 1　[モニタリング（Monitoring）] > [ASA FirePOWER モニタリング（ASA FirePOWER Monitoring）] > [統計情報（Statistics）] の順に選択します。

[統計情報（Statistics）] ページが表示されます。

システム ステータスとディスク領域使用率のモニタリング

ライセンス：任意（Any）

[統計情報（Statistics）] ページの [ディスク使用率（Disk Usage）] セクションは、カテゴリ別およびパーティション ステータス別に、ディスク使用量のクイック概要を示します。マルウェア ストレージ パックがデバイスにインストールされている場合、そのパーティション ステータスも確認できます。このページを定期的にモニタして、システム プロセスおよびデータベースで十分なディスク領域が使用可能であることを確認できます。

ディスク使用量情報にアクセスするには、次の手順に従います。

手順 1　[モニタリング（Monitoring）] > [ASA FirePOWER モニタリング（ASA FirePOWER Monitoring）] > [統計情報（Statistics）] の順に選択します。

[統計情報（Statistics）] ページが表示されます。

ディスク使用量カテゴリの詳細については、[ディスク使用率（Disk Usage）] ウィジェットについて（40-3 ページ）を参照してください。

手順 2　展開するには、[合計(Total)] の横にある下矢印をクリックします。

[ディスク使用率(Disk Usage)] セクションが展開され、パーティションの使用状況が表示されます。マルウェア ストレージ パックがインストールされている場合は、`/var/storage` パーティションの使用状況も表示されます。

システム プロセス ステータスの表示

ライセンス:任意(Any)

[ホスト統計情報(Host Statistics)] ページの [プロセス(Processes)] セクションでは、アプライアンスで現在実行中のプロセスを表示できます。これは、一般的なプロセス情報と、実行中の各プロセスに固有の情報を提供します。

次の表に、プロセス リストに表示される各列を示します。

表 47-2　プロセス ステータス

カラム	説明
Pid	プロセス ID 番号
[ユーザ名(Username)]	プロセスを実行しているユーザまたはグループの名前
Pri	プロセスの優先度
Nice	*nice* 値。プロセスのスケジューリング優先度を示す値です。値は 20(最も高い優先度)から 19(最も低い優先度)までの範囲になります
Size	プロセスで使用されるメモリ サイズ(値の後ろにメガバイトを表す m がない場合はキロバイト単位)
Res	メモリ内の常駐ページング ファイルの量(値の後ろにメガバイトを表す m がない場合はキロバイト単位)
State	プロセスの状態: • D:プロセスが中断不能スリープ状態(通常は入出力)にある • N:プロセスの nice 値が正の値 • R:プロセスが実行可能である(実行するキュー上で) • S:プロセスがスリープ モードにある • T:プロセスがトレースまたは停止されている • W:プロセスがページングしている • X:プロセスがデッド状態である • Z:プロセスが機能していない • <:プロセスの nice 値が負の値
時刻(Time)	プロセスが実行されてきた時間の長さ(時間数:分数:秒数)
Cpu	プロセスが使用している CPU の割合
コマンド(Command)	プロセスの実行可能ファイル名

プロセス リストを展開するには、次の手順に従います。

手順 1　[モニタリング（Monitoring）] > [ASA FirePOWER モニタリング（ASA FirePOWER Monitoring）] > [統計情報（Statistics）] の順に選択します。

[統計情報（Statistics）] ページが表示されます。

手順 2　[プロセス（Processes）] の横にある下矢印をクリックします。

プロセス リストが展開され、実行中のタスクの数やタイプ、現在の時刻、現在のシステム稼働時間、システムの負荷平均、CPU、メモリ、およびスワップ情報などの、一般的なプロセス ステータス情報と、実行中の各プロセスに関する固有の情報がリストされます。

[CPU（Cpu(s)）] には、以下の CPU 使用状況情報がリストされます。

- ユーザ プロセスの使用状況の割合
- システム プロセスの使用状況の割合
- nice 使用状況の割合（高い優先度を示す、負の nice 値を持つプロセスの CPU 使用状況）

  nice 値は、システム プロセスのスケジュールされた優先度を示しており、20（最も高い優先度）から 19（最も低い優先度）の範囲の値になります。
- アイドル状態の使用状況の割合

[メモリ（Mem）] には、以下のメモリ使用状況情報がリストされます。

- メモリ内の合計キロバイト数
- メモリ内の使用キロバイト数の合計
- メモリ内の空きキロバイト数の合計
- メモリ内のバッファに書き出されたキロバイト数の合計

[スワップ（Swap）] には、以下のスワップ使用状況情報がリストされます。

- スワップ内の合計キロバイト数
- スワップ内の使用キロバイト数の合計
- スワップ内の空きキロバイト数の合計
- スワップ内のキャッシュされたキロバイト数の合計

（注）　アプライアンスで実行されるプロセスのタイプの詳細については、実行されるプロセスについて（47-5 ページ）を参照してください。

プロセス リストを折りたたむには、次の手順に従います。

手順 1　[プロセス（Processes）] の横にある上矢印をクリックします。

プロセス リストが折りたたまれます。

実行されるプロセスについて

ライセンス：任意（Any）

アプライアンスで実行されるプロセスには、デーモンと実行可能ファイルの 2 種類があります。デーモンは常に実行され、実行可能ファイルは必要に応じて実行されます。

詳細については、次の各項を参照してください。

- システム デーモンについて（47-5 ページ）
- 実行可能ファイルおよびシステム ユーティリティについて（47-6 ページ）

システム デーモンについて

ライセンス：任意（Any）

デーモンは、アプライアンスで継続的に実行されます。これにより、サービスが使用可能になり、必要に応じてプロセスが生成されるようになります。次の表では、[プロセスのステータス（Process Status）] ページに表示されるデーモンをリストし、その機能について簡単に説明しています。

（注） 次の表は、アプライアンスで実行される可能性があるすべてのプロセスの包括的なリストではありません。

表 47-3　システム デーモン

デーモン	説明
crond	スケジュールされたコマンド（cron ジョブ）の実行を管理します
dhclient	ダイナミック ホスト IP アドレッシングを管理します
httpd	HTTP（Apache Web サーバ）プロセスを管理します
httpsd	HTTPS（SSL を使用した Apache Web サーバ）サービスを管理し、SSL および有効な証明書の認証が機能しているかチェックし、アプライアンスへの安全な Web アクセスを提供するためにバックグラウンドで実行します
keventd	Linux カーネルのイベント通知メッセージを管理します
klogd	Linux カーネル メッセージのインターセプションおよびロギングを管理します
kswapd	Linux カーネルのスワップ メモリを管理します
kupdated	ディスクの同期を実行する、Linux カーネルの更新プロセスを管理します
mysqld	ASA FirePOWER モジュール データベース プロセスを管理します
ntpd	Network Time Protocol（NTP）プロセスを管理します
午後	すべてのシスコプロセスを管理し、必要なプロセスを始動し、予期せずに失敗したプロセスをすべて再始動します
reportd	レポートを管理します
safe_mysqld	データベースのセーフ モード運用を管理し、エラーが発生した場合にはデータベース デーモンを再始動し、ランタイム情報をファイルに記録します
sfmgr	アプライアンスへの sftunnel 接続を使用して、リモートでアプライアンスを管理および設定するための RPC サービスを提供します

表 47-3　システム デーモン(続き)

デーモン	説明
sftroughd	着信ソケットで接続をリッスンしてから、正しい実行可能ファイル(通常は、シスコ メッセージ ブローカ sfmb)を呼び出して要求を処理します
sftunnel	リモート アプライアンスとの通信を必要とするすべてのプロセスに対し、安全な通信チャネルを提供します。
sshd	セキュア シェル(SSH)プロセスを管理し、アプライアンスへの SSH アクセスを提供するためにバックグラウンドで実行します
syslogd	システム ロギング(syslog)プロセスを管理します

実行可能ファイルおよびシステム ユーティリティについて

ライセンス:任意(Any)

システム上には、他のプロセスまたはユーザ操作によって実行される実行可能ファイルが数多く存在します。次の表に、[プロセス ステータス(Process Status)] ページで表示される実行可能ファイルについて説明します。

表 47-4　システムの実行可能ファイルおよびユーティリティ

実行可能ファイル	説明
awk	awk プログラミング言語で作成されたプログラムを実行するユーティリティ
bash	GNU Bourne-Again シェル
cat	ファイルを読み取り、コンテンツを標準出力に書き込むユーティリティ
chown	ユーザおよびグループのファイル権限を変更するユーティリティ
chsh	デフォルトのログイン シェルを変更するユーティリティ
cp	ファイルをコピーするユーティリティ
df	アプライアンスの空き領域の量をリストするユーティリティ
エコー	コンテンツを標準出力に書き込むユーティリティ
egrep	指定された入力を、ファイルおよびフォルダで検索するユーティリティ。標準 grep でサポートされていない正規表現の拡張セットをサポートします
検索	指定された入力のディレクトリを再帰的に検索するユーティリティ
grep	指定された入力をファイルとディレクトリで検索するユーティリティ
halt	サーバを停止するユーティリティ
httpsdctl	セキュアな Apache Web プロセスを処理する
hwclock	ハードウェア クロックへのアクセスを許可するユーティリティ
ifconfig	ネットワーク構成実行可能ファイルを示します。MAC アドレスが常に一定になるようにします
iptables	[アクセス権の設定(Access Configuration)] ページに加えられた変更に基づいてアクセス制限を処理します。アクセス権の設定の詳細については、アプライアンスのアクセス リストの設定(43-4 ページ)を参照してください。

表 47-4　システムの実行可能ファイルおよびユーティリティ(続き)

実行可能ファイル	説明
iptables-restore	iptables ファイルの復元を処理します
iptables-save	iptables に対する保存済みの変更を処理します
kill	セッションおよびプロセスを終了するために使用できるユーティリティ
killall	すべてのセッションおよびプロセスを終了するために使用できるユーティリティ
ksh	Korn シェルのパブリック ドメイン バージョン
ロガー	コマンドラインから syslog デーモンにアクセスする方法を提供するユーティリティ
md5sum	指定したファイルのチェックサムとブロック数を印刷するユーティリティ
mv	ファイルを移動(名前変更)するユーティリティ
myisamchk	データベース テーブルの検査および修復を示します
mysql	データベース プロセスを示します。複数のインスタンスが表示されることがあります
openssl	認証証明書の作成を示します
perl	perl プロセスを示します
ps	標準出力にプロセス情報を書き込むユーティリティ
sed	1 つ以上のテキスト ファイルの編集に使用されるユーティリティ
sh	Korn シェルのパブリック ドメイン バージョン
shutdown	アプライアンスをシャットダウンするユーティリティ
sleep	指定された秒数のあいだプロセスを中断するユーティリティ
smtpclient	電子メール イベント通知機能が有効な場合に、電子メール送信を処理するメール クライアント
snmptrap	SNMP 通知機能が有効な場合に、指定された SNMP トラップ サーバに SNMP トラップ データを転送します
snort (Protection が必要)	Snort が動作していることを示します
ssh	アプライアンスへのセキュア シェル(SSH)接続を示します
sudo	sudo プロセスを示します。これにより、admin 以外のユーザが実行可能ファイルを実行できるようになります
top	上位の CPU プロセスに関する情報を表示するユーティリティ
touch	指定したファイルへのアクセス時刻や変更時刻を変更するために使用できるユーティリティ
vim	テキスト ファイルの編集に使用されるユーティリティ
wc	指定したファイルの行、ワード、バイトのカウントを実行するユーティリティ