



システムのモニタリング

FireSIGHT システムは、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 \(Host Statistics\)](#)] ページでは、基本的なホスト統計情報および侵入イベント情報に加え、当日の [[データ コリレータ \(Data Correlator\)](#)] やネットワーク検出プロセスを監視できます。また、防御センターまたは管理対象デバイスで現在実行されているすべてのプロセスの、概要と詳細情報のどちらもモニタできます。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 \(67-2 ページ\)](#) 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
- データ コリレータ統計
- システム プロセス
- 侵入イベント情報
- 防御センターで、ヘルス モニタを使用して、ディスク使用状況を監視し、ディスク容量不足の状態をアラートすることもできます。詳細については、[ヘルス モニタリングについて \(68-2 ページ\)](#) を参照してください。
- [システム ステータスとディスク領域使用率のモニタ \(67-4 ページ\)](#) 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 \(67-5 ページ\)](#) 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。
- [実行中のプロセスについて \(67-7 ページ\)](#) 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。

[[概要 \(Overview\)](#)] > [[サマリ \(Summary\)](#)] にあるオプションを使用して、侵入イベントおよび検出イベントの統計情報を表示およびグラフ化することができます。詳細については、以下を参照してください。

- [侵入イベントの統計の表示 \(41-2 ページ\)](#)
- [侵入イベント グラフの表示 \(41-10 ページ\)](#)
- [ディスカバリ イベントの統計情報の表示 \(50-2 ページ\)](#)
- [ディスカバリのパフォーマンス グラフの表示 \(50-6 ページ\)](#)

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
- データ コリレータの統計情報 (防御センターのみ FireSIGHT が必要)。詳細については [データ コリレータ プロセスの統計情報](#)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、[侵入イベント情報](#)の表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 67-1 ホスト統計情報

カテゴリ	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。
ディスク使用量 (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 (67-4 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 (67-5 ページ) を参照してください。

FireSIGHT システムの展開に FireSIGHT のライセンスを使用した防御センターが含まれる場合、当日のデータ コリレータやネットワーク検出プロセスも表示できます。管理対象デバイスがデータの取得、復号化、および分析を実行する際に、ネットワーク検出プロセスはデータをフィンガープリントおよび脆弱性データベースと関連付けてから、防御センターで実行中のデータ コリレータで処理されるバイナリ ファイルを生成します。データ コリレータはバイナリ ファイルの情報を分析し、イベントを生成し、検出ネットワーク マップを作成します。

ネットワーク検出とデータ コリレータに表示される統計情報は、デバイスごとに 0:00 から 23:59 までの間に収集された統計情報を使用した、当日の平均です。

次の表に、データ コリレータ プロセスに表示される統計情報を示します。

表 67-2 データ コリレータ プロセスの統計情報

カテゴリ	説明
Events/Sec	データ コリレータが受信し処理する検出イベントの 1 秒あたりの数
Connections/Sec	データ コリレータが受信し処理する接続の 1 秒あたりの数
CPU Usage — User (%)	当日のユーザ プロセスで使用される CPU 時間の平均パーセンテージ

表 67-2 データ コリレータ プロセスの統計情報(続き)

カテゴリ	説明
CPU Usage — System (%)	当日のシステム プロセスで使用される CPU 時間の平均パーセンテージ
VmSize(KB)	データ コリレータに割り当てられたメモリの当日の平均サイズ(キロバイト単位)
VmRSS(KB)	データ コリレータで使用されるメモリの当日の平均量(キロバイト単位)

管理対象デバイスおよびデバイスを管理する防御センターでは、前回の侵入イベントの日時、過去 1 時間および過去 1 日に発生したイベントの合計数、およびデータベース内のイベントの合計数を表示することもできます。



(注)

[統計(Statistics)] ページの [侵入イベント情報(Intrusion Event Information)] セクションにある情報は、防御センターに送信された侵入イベントではなく、管理対象デバイスに保存されている侵入イベントに基づいています。侵入イベントがローカルで保存されないようにデバイスを管理する場合、このページには侵入イベントの情報は表示されません。これは、イベントをローカルで保存できない管理対象デバイスについても同様です。

次の表に、[統計(Statistics)] ページの [侵入イベント情報(Intrusion Event Information)] セクションに表示される統計情報を示します。

表 67-3 侵入イベント情報

統計	説明
Last Alert Was	前回のイベントが発生した日時
Total Events Last Hour	過去 1 時間に発生したイベントの合計数
Total Events Last Day	過去 24 時間に発生したイベントの合計数
Total Events in Database	イベント データベース内のイベントの合計数

[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。

アクセス: Admin/Maint

-
- 手順 1** [システム(System)] > [モニタリング(Monitoring)] > [統計(Statistics)] を選択します。
[統計情報(Statistics)] ページが表示されます。
- 手順 2** 防御センターで、管理対象デバイスの統計情報をリストすることもできます。[デバイスの選択(Select Device(s))] ボックスから、[デバイスの選択(Select Devices)] をクリックします。Shift キーおよび Ctrl キーを使用して、複数のデバイスを同時に選択することができます。
[統計(Statistics)] ページは、選択したデバイスの統計情報で更新されます。
-

システム ステータスとディスク領域使用率のモニタ

ライセンス:任意 (Any)

[統計情報 (Statistics)] ページの [ディスク使用量 (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。



ヒント

防御センターで、ヘルス モニタを使用して、ディスク使用状況を監視し、ディスク容量不足の状態をアラートすることもできます。詳細については、[ヘルス モニタリングについて \(68-2 ページ\)](#) を参照してください。

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。

アクセス:Admin/Maint

手順 1 [システム (System)] > [モニタリング (Monitoring)] > [統計 (Statistics)] を選択します。

[統計情報 (Statistics)] ページが表示されます。

手順 2 [カテゴリ別 (By Category)] 積み上げ棒グラフで、ディスク使用率カテゴリの上にポインタを移動すると、以下が (順番に) 表示されます。

- そのカテゴリが使用する使用可能なディスク領域の割合
- ディスク上の実際のストレージ領域
- そのカテゴリで使用可能なディスク領域の合計

ディスク使用量カテゴリの詳細については、[Disk Usage ウィジェットについて \(55-31 ページ\)](#) を参照してください。

手順 3 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。

[ディスク使用量 (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。

複数の管理対象デバイスが展開に含まれる場合、特定のデバイスによってディスク使用量のデータを制約することもできます。

防御センターで、特定のデバイスのディスク使用状況の情報を表示するには、次の手順に従います。

アクセス:Admin/Maint

手順 1 [デバイスの選択 (Select Device(s))] ボックスからデバイス名を選択し、[デバイスの選択 (Select Devices)] をクリックします。

ページがリロードされ、選択した各デバイスのホスト統計情報が表示されます。

手順 2 展開するには、[ディスク使用状況 (Disk Usage)] の横にある下矢印をクリックします。

[ディスク使用状況 (Disk Usage)] セクションが展開されます。

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。防御センターでデバイスを管理している場合、防御センターの Web インターフェイスを使用して、管理対象デバイスのプロセス ステータスを表示することができます。

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 67-4 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	<i>nice</i> 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)
状態(State)	プロセスの状態: <ul style="list-style-type: none"> • 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 <i>nice</i> 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 <i>nice</i> 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。

アクセス:Admin/Maint

-
- 手順 1 [システム(System)] > [モニタリング(Monitoring)] > [統計(Statistics)] を選択します。
[統計情報(Statistics)] ページが表示されます。
- 手順 2 防御センターで、プロセス統計を表示するデバイスを [デバイスの選択(Select Device(s))] ボックスから選択し、[デバイスの選択(Select Devices)] をクリックします。
- 手順 3 [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、[実行中のプロセスについて \(67-7 ページ\)](#) 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。

アクセス:Admin/Maint

-
- 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。
-

実行中のプロセスについて

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\(67-7 ページ\)](#)
- [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\(67-8 ページ\)](#)

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 67-5 システム デーモン

デーモン	説明
crond	スケジューラされたコマンド(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
fpcollect	クライアントとサーバのフィンガープリントの収集を管理します
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	FireSIGHT システムデータベース 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
pm	すべての Cisco 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
SFDataCorrelator	データ転送を管理します

表 67-5 システム デーモン(続き)

デーモン	説明
sfstreamer (防御センターのみ)	Event Streamer を使用するサードパーティ製クライアントアプリケーションへの接続を管理します。
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
SFRemediateD (防御センターのみ、 FireSIGHT が必要)	修復応答を管理します
sftimeserviced (防御センターのみ)	時刻同期メッセージを管理対象デバイスに転送します
sfmbservice (Protection が必要)	アプライアンスへの sftunnel 接続を使用して、リモート アプライアンスで実行されている sfmb メッセージブローカ プロセスへのアクセスを提供します。現在ヘルスモニタリングによってのみ使用されており、管理対象デバイスから防御センターに、または高可用性環境では防御センター間でヘルスイベントおよびアラートを送信します
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、Cisco 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、安全な通信チャンネルを提供します。
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 67-6 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
SFDataCorrelator (防御センターのみ、 FireSIGHT が必要)	FireSIGHT で作成されるバイナリ ファイルを分析し、イベント、接続データ、およびネットワーク マップを生成します。
cp	ファイルをコピーするユーティリティ

表 67-6 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
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
echo	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 <code>grep</code> 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
find	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 (63-9 ページ) を参照してください。
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
logger	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
sfheartbeat	アプライアンスがアクティブであることを示す、ハートビート ブロードキャストを識別します。ハートビートはデバイスと防御センターの間の接続を維持するのに使用されます

表 67-6 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
sfmb	メッセージブローカ プロセスを示します。防御センターとデバイスとの間の通信を処理します。
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、バイトのカウンタを実行するユーティリティ