Cisco Secure Firewall Management Center ヘルスモニターバージョン 7.4.0 によって収集される Cisco Secure Firewall Threat Defense デバイスメトリック

初版：2023 年 9 月 7 日

最終更新：2023 年 9 月 7 日

Secure Firewall Management Center ヘルスモニターによって収集される Secure Firewall Threat Defense デバイスメトリック

デバイス正常性モニターには、システムイベントを予測して対応するのに役立つ、一連の主要 Threat Defense デバイスメトリックが含まれています。Threat Defense デバイスの正常性は、これらの報告されたメトリックによって判断できます。このドキュメントには、すべてのヘルスモニター ダッシュボードと、報告されたメトリックのリストが記載されています。

CPU グループのメトリック

正常性モニターは、CPU 使用率（プロセス別および物理コア別の CPU 使用率を含む）に関連する統計情報を追跡します。

表 *1 : CPU* グループのメトリック

メトリック	説明	書式
コントロール委任プレーン（Control Delegate Plane）	コントロール委任プレーンによる平均 CPU 使用率。	percentage
コントロール プレーン	過去 1 分間のコントロールプレーンの平均 CPU 使用率。	percentage
データ プレーン	過去 1 分間のデータプレーンの平均 CPU 使用率。	percentage
Snort	過去 1 分間の Snort プロセスの平均 CPU 使用率。	percentage

メトリック	説明	書式
システム	過去 1 分間のシステムプロセスの平均 CPU 使用率。	percentage
Physical cores	過去 1 分間のすべてのコアの平均 CPU 使用率。	percent

メモリグループのメトリック

ヘルスモニターは、データプレーンや Snort のメモリ使用率などの、デバイスのメモリ使用率に関連する統計を追跡します。

表 *2:* メモリグループのメトリック

メトリック	説明	書式
バッファ キャッシュ	バッファキャッシュ。	bytes
未使用	空きメモリの合計。	bytes
最大データプレーン（Maximum Data Plane）	データプレーンによって使用されている最大メモリ。	bytes
最大 Snort（Maximum Snort）	Snort プロセスによって使用されている最大メモリ。	bytes
Snort の最大スワップ（Maximum Swap for Snort）	Snort プロセスによって使用されている最大スワップメモリ。	bytes
残りのメモリブロック（1550）（Remaining Memory Block (1550)）	1550 バイトブロックの空きメモリ。	number
残りのメモリブロック（256）（Remaining Memory Block (256)）	256 バイトブロックの空きメモリ。	number
使用システム（System Used）	システムによって使用されている合計メモリ。	bytes
総量	使用可能な合計メモリ。	bytes
Total Swap	スワップに使用可能な合計メモリ。	bytes
データ プレーン	データプレーンによって使用されている合計メモリ。	bytes

メトリック	説明	書式
データプレーンによる使用済み割合（Percent Used by Data Plane）	データプレーンによって使用されているメモリの割合。	percent
Snort による使用済み割合（Percent Used by Snort）	Snort プロセスによって使用されているメモリの割合。	percent
スワップの使用済み割合（Percent Used for Swap）	スワップに使用されているメモリの割合。	percent
システムによる使用済み割合（Percent Used by System）	システムによって使用されているメモリの割合。	percent
システムおよびスワップによる使用済み割合（Percent Used by System and Swap）	システムとスワップの合計によって使用されているメモリの割合。	percent
Snort	Snort プロセスによって使用されている合計メモリ。	bytes
Used Swap	スワップに使用されている合計メモリ。	bytes
Snort によって使用されているスワップ（Used Swap by Snort）	Snort プロセスによって使用されている合計スワップメモリ。	bytes

インターフェイスグループのメトリック

ヘルスモニターは、インターフェイスステータスや集約トラフィック統計情報など、デバイスインターフェイスに関連する統計情報を追跡します。

表 *3:* インターフェイスグループのメトリック

メトリック	説明	書式
廃棄パケット数	ドロップしたパケットの数。	number
Average Input Packet Size	着信パケットの平均サイズ。	bytes
Input Rate	合計着信バイト。	bytes
入力パケット	合計着信パケット数。	number
Average Output Packet Size	発信パケットの平均サイズ。	bytes
Output Rate	合計発信バイト数。	bytes

メトリック	説明	書式
出力パケット	合計発信パケット数。	number
Status（ステータス）	インターフェイスのステータス。アップの場合は 1、ダウンの場合は 0。	1 または 0
CRC Errors	CRC（Cyclic Redundancy Check）エラーで受信されたパケットの合計数。	number
入力エラー（Input Error）	入力エラーの数。	number
出力エラー（Output Error）	出力エラーの数。	number
オーバーランエラー（Overrun Errors）	入力レートが受信データを処理するレシーバの能力を超えたためにドロップされたパケットの数。	number
アンダーランエラー（Underrun Errors）	ルータの処理能力を超えた速度でトランスミッタが動作したためにドロップされたパケットの数。	number
L2デコードドロップ（L2 Decode Drops）	名前が設定されていないため（nameif コマンド）、または無効な VLAN ID を持つフレームが受信されたためにドロップされたパケットの数。	number
ジッタ	パケットフローの遅延の変動。	microseconds
平均オピニオン評点（MOS）	接続の品質の尺度は、0 ー 5 の範囲で、5 が最適です。	0 ～ 5
パケット損失	送信されたパケットのうち接続先に到達しない割合。	percentage
ラウンドトリップ時間	ICMP エコーの要求と応答間の平均継続時間。	マイクロ秒

接続グループのメトリック

正常性モニターは、接続と NAT 変換カウントに関連する統計情報を追跡します。

表 *4*: 接続グループのメトリック

メトリック	説明	書式
アクティブなエレファントフロー（Active Elephant Flows）	アクティブなエレファントフローの数を表示します。 エレファントフローは、システム全体のパフォーマンスに影響を与えるほど大規模な接続です。デフォルトでは、エレファントフローとは 1GB/10 秒を超えるフローです。**system support elephant-flow-detection** コマンドを使用して、Threat Defense CLI でエレファントフローを識別するためのバイトしきい値と時間しきい値を調整できます。 （注） フローは、バイトと時間の両方のしきい値を超えた場合にのみ、エレファントフローと見なされます。	number
アクティブな接続数（Active connections）	アクティブな接続数を表示します。	number
Peak Connections	同時接続の最大数を示します。	number
Total Connections per second	すべての接続タイプの1秒あたりの接続数。	number
TCP Connections per second	TCP 接続タイプの 1 秒あたりの接続数。	number
UDP Connections per second	UDP 接続タイプの 1 秒あたりの接続数。	number
Preserve Connections Enabled	Snort プロセスがダウンした場合に、ルーテッドインターフェイスとトランスペアレントインターフェイスで既存の TCP/UDP 接続を維持します。	number
Connections Preserved	現在 preserve-connection が有効になっている接続数。	number
Preserve Connections Most Enabled	保持された接続の最大数。	number
Peak Connections Preserved	保持されたピーク接続の最大数。	number
NAT Translations	変換数を表示します。	number
Peak NAT Translations	同時変換の最大数の履歴を一度に表示します。	number

Snort グループのメトリック

正常性モニターは、Snort プロセスに関連する統計情報を追跡します。

表 *5 : Snort* グループのメトリック

メトリック	説明	書式
Blocked list flows	Snort によってドロップされた、ポリシー設定からのフローの数。	number
Blocked Packets	ブロックされたパケットの数。	number
拒否されたフロー	拒否されたフローイベントの数。データプレーンは、Snort に送信する前にフローをドロップすることを決定すると、拒否されたフローイベントを Snort に送信します。	number
End of flows	高速パスフローが終了すると、データプレーンはフロー終了イベントを Snort に送信します。	number
Fast forwarded flows	ポリシーによって高速転送されたため、検査されなかったフローの数。	number
Dropped frames forwarded from the data plane	データプレーンから転送された、ドロップされたフレームの数。	number
Injected packets dropped	Snort がトラフィックストリームに追加したパケットのうち、ドロップされたパケット数。	number
Injected packets	Snort が作成し、トラフィックストリームに追加したパケットの数。たとえば、リセットアクションを伴うブロックを設定すると、Snort は接続をリセットするためのパケットを生成します。	number
Instances	Snort インスタンス（プロセス）の数。	number
Packet receiving queue utilization percentage	データプレーン受信キューのキュー使用率。	percent
Packets bypassed due to Snort busy	Snort がビジー状態でパケットを処理できない場合に、インスペクションをバイパスしたパケットの数。	number
Packets bypassed due to Snort down	Snort がダウンしたときにインスペクションをバイパスしたパケットの数。	number

メトリック	説明	書式
Packets bypassed due to RX queue full	受信キューがいっぱいのためバイパスされたパケットの数。	number
Packets bypassed due to TX queue full	送信キューがいっぱいのためバイパスされたパケットの数。	number
Passed packets	データプレーンから Snort に送信されたパケットの数。	number
Start of flows	フロー開始イベントの数。これらのイベントは、Snort が接続を追跡し、接続イベントを報告するのに役立ちます。	number

ASP ドロップメトリック

正常性モニターは、高速セキュリティパス（ASP）でドロップされたパケットまたは接続に関連する統計を追跡します。

次の表に、一般的な ASP ドロップ ダッシュボード メトリックのリストを示します。すべての ASP ドロップ ダッシュボードメトリックのリストの詳細については、『Show ASP Drop Command Usage』ドキュメントを参照してください。

表 *6 : ASP* ドロップメトリック

メトリック	説明	書式
Connection limit exceeded	接続制限を超えたときに閉じられたフローの数をカウントします。	number
Connection limit reached	接続制限またはホストの接続制限を超えたときにドロップされたパケットの数をカウントします。	number
アクセスルールによって拒否されたフロー	アクセスルールによって拒否された接続の数。	number
設定済みのルールによって拒否されたフロー	設定済みのルールによって拒否された接続の数。	number
L2 ルールドロップ	レイヤ 2 ACL により拒否されたパケットの数をカウントします。	number
L2 ルール VXLAN ドロップ	レイヤ 2 ACL チェックの適用時に VXLAN out_tag の検索に失敗したために拒否されたパケットの数をカウントします。	number

メトリック	説明	書式
NAT reverse path failed	変換されたホストへの、そのホストの実際のアドレスを使用した接続が拒否された回数をカウントします。	number
NAT failed	IP またはトランスポートヘッダーを変換するための xlate の作成が失敗した回数をカウントします。	number
有効な v4 隣接関係がありません	セキュリティアプライアンスが隣接関係の取得を試み、次のホップ（IPv4）の MAC アドレスを取得できなかったときにドロップされたパケットの数をカウントします。	number
有効な v6 隣接関係がありません	セキュリティアプライアンスが隣接関係の取得を試み、次のホップ（IPv6）の MAC アドレスを取得できなかったときにドロップされたパケットの数をカウントします。	number
Snort によってブロックリストに登録されたパケット。Snort によってブロックされたパケット	Snort モジュールの要求に従ってドロップされたパケットの数をカウントします。	number
フレームドロップ： Snort ビジー。フレームドロップ：Snort ダウン。フレームドロップ：Snort ドロップ	Snort モジュールがビジーでフレームを処理できないためにドロップされたフレームの数をカウントします。 Snort モジュールがダウン。Snort モジュールがドロップを要求。	number
Dispatch queue limit reached	デバイスのロードバランス ASP ディスパッチャがキュー制限に達した回数をカウントします。 When more packets are attempted, tail drop occurs and this counter is incremented.	number
宛先 MAC L2 ルックアップに失敗しました	失敗したレイヤ 2 宛先 MAC アドレスルックアップの数をカウントします。 Upon the lookup failure, the appliance will begin the destination MAC discovery process and attempt to find the location of the host via ARP and/or ICMP messages.	number

メトリック	説明	書式
Inspection failure	接続のためにネットワークプロセッサによって実行されるプロトコルインスペクションをアプライアンスが有効にできなかった回数をカウントします。The cause could be memory allocation failure, or for ICMP error message, the appliance not being able to find any established connection related to the frame embedded in the ICMP error message.	number
NAT no xlate to PAT pool	PAT プール内のマッピングアドレスと一致する宛先との接続で、既存の xlate が検出されなかった場合にカウントします。	number
ホストへのルートがありません	セキュリティアプライアンスがパケットをインターフェイスから送信しようとし、そのルートがルーティングテーブルで見つからなかった回数。	number
PDTS パント制限を超過しました	データパスがパケットをインスペクタにパントし、snort にキューイングされたパケットの数が上限を超えた場合に、ドロップされたパケットの数。	number
パント制限	検査のためにキューイングされたパケットが制限に達したためにドロップされたパケットの数。	number
Snortによるサイレントドロップ	Snort モジュールの要求に従って、パケットがサイレントにドロップされた回数。	number
SYN にない最初の TCP パケット	非傍受かつ非固定接続の最初のパケットとして非 SYN パケットを受信した回数。	number

ハードウェア/環境のステータスメトリック

ハードウェア/環境ヘルスモニターは、統計情報をトラッキングし、脅威防御ハードウェアエンティティに関連するメトリック値を収集します。

表 7: ハードウェア/環境のステータスメトリック

メトリック	説明	書式
ファンの速度	シャーシファンの速度。	RPM
吸気温度。	吸気センサーの温度。	摂氏

メトリック	説明	書式
Internal Temperature	内部センサーの温度。	摂氏
排気温度。	排気センサーの温度。	摂氏
電源ユニット温度（Power Supply Unit Temperature）	電源ユニットの温度。	摂氏
電源ユニットファン速度（Power Supply Unit Fan Speed）	電源ユニットファンの速度。	RPM
電源ユニット入力電流（Power Supply Unit Input Current）	電源ユニットの入力電流。	アンペア
電源ユニット入力電圧（Power Supply Unit Input Voltage）	電源ユニットの入力電圧。	ボルト
電源ユニット入力電力（Power Supply Unit Input Power）	電源ユニットの入力電力。	ワット
電源ユニット入力ステータス（Power Supply Unit Input Status）	電源ユニットの入力ステータス。	ブール値
電源ユニット出力電力（Power Supply Unit Output Power）	電源ユニットの出力電力。	ワット
電源ユニット温度（Power Supply Unit Temperature）	電源ユニットの温度。	摂氏
電源ユニットファン速度（Power Supply Unit Fan Speed）	電源ユニットファンの速度。	RPM
電源ユニットファンステータス（Power Supply Unit Fan Status）	電源ユニットファンのステータス。	ブール値
SSD1	SSD1 のステータス。	number
システム稼動時間	システムがアクティブな期間。	seconds
温度ステータス	デバイスの電源ステータス。1 は稼働状態を表し、0 は停止状態を表します。	1 または 0

ハードウェア/環境ステータスメトリックが使用可能かどうかは、Threat Defense デバイスのモデルによって異なる場合があります。次の表では、各デバイスモデルで使用可能なメトリックについて説明します。

表 *8*：デバイスモデル別のハードウェア/環境ステータスメトリック

メトリック	1000 シリーズ	2100 シリーズ	3100 シリーズ	4100 シリーズ	4200 シリーズ	9300 シリーズ	SSP
システム稼動時間	対応	対応	対応	対応	対応	対応	対応
ファンの速度	対応	対応	対応	×	対応	×	×
電源ユニット温度（Power Supply Unit Temperature）	×	×	対応	×	対応	×	×
電源ユニットファン速度（Power Supply Unit Fan Speed）	×	×	対応	×	対応	×	×
電源ユニットファンステータス（Power Supply Unit Fan Status）	対応	×	対応	×	対応	×	×
電源ユニット入力電流（Power Supply Unit Input Current）	×	×	対応	×	対応	×	×
電源ユニット入力電圧（Power Supply Unit Input Voltage）	×	×	対応	×	対応	×	×
電源ユニット入力電力（Power Supply Unit Input Power）	×	×	対応	×	対応	×	×
電源ユニット入力ステータス（Power Supply Unit Input Status）	対応	対応	対応	×	対応	×	×
電源ユニット出力電力（Power Supply Unit Output Power）	×	×	対応	×	対応	×	×
Internal Temperature	対応	対応	対応	×	対応	×	×
吸気温度。	×	×	×	×	×	×	×
排気温度。	×	×	×	×	×	×	×

メトリック	1000 シリーズ	2100 シリーズ	3100 シリーズ	4100 シリーズ	4200 シリーズ	9300 シリーズ	SSP
SSD1 ステータス（SSD1 Status）	対応	対応	対応	×	対応	×	×
温度ステータス	×	×	×	対応	×	対応	対応

展開された設定グループのメトリック

正常性モニターは、IPSルールの数やACEの数など、展開された設定に関連する統計情報を追跡します。

表 *9*：展開された設定グループのメトリック

メトリック	説明	書式
Number of ACEs	アクセスコントロールエントリ（ACE）またはルールの数。アクセスコントロールリスト（ACL）は1つ以上のACEで構成されます。	number
Number of rules	侵入ポリシー内のルールの数。	number

ディスクグループのメトリック

正常性モニターは、パーティションごとのディスクサイズやディスク使用率など、デバイスのディスク使用率に関連する統計情報を追跡します。

表 *10*：ディスクグループのメトリック

メトリック	説明	書式
Total	デバイスディスクの合計サイズ。	bytes
Used	デバイスディスクで使用されている合計領域。	bytes
/ngfwによる使用率（Used Percentage by /ngfw）	/ngfwパーティションが使用しているディスク領域の割合。	percentage
/ngfw/Volumeによる使用率（Used Percentage by /ngfw/Volume）	/ngfw/Volumeパーティションが使用しているディスク領域の割合。	percentage
/dev/cgroupsによる使用率（Used Percentage by /dev/cgroups）	/dev/cgroupsパーティションが使用しているディスク領域の割合。	percentage

メトリック	説明	書式
/mnt/disk0による使用率（Used Percentage by /mnt/disk0）	/mnt/disk0パーティションが使用しているディスク領域の割合。	percentage
/var/volatileによる使用率（Used Percentage by /var/volatile）	/var/volatileパーティションが使用しているディスク領域の割合。	percentage

クリティカル プロセス グループのメトリック

正常性モニターは、管理対象プロセスのプロセス再起動に関連する統計情報を追跡します。また、ヘルスモニターは重要なプロセスごとに、CPU使用率、メモリ使用率、稼働時間、およびステータスをトラッキングします。

表 *11 :* クリティカル プロセス グループのメトリック

メトリック	説明	書式
CPU 使用率	プロセスの開始以降のプロセスの CPU 使用率。	percent
Restart count	Threat Defense デバイスが起動してからプロセスが再起動した回数。 プロセスの再起動頻度が高すぎる場合、再起動カウントメトリックは毎分実行されるため、正確な数を反映しない可能性があることに注意してください。	number
予期しない再起動の回数（Unexpected Restart Count）	Threat Defense デバイスが起動してからプロセスが予期せず再起動した回数。	number

メトリック	説明	書式
Status（ステータス）	プロセスのステータス。	次のいずれかが必要です。 • Started • 実行中（Running） • ダウン • Waiting • ロック（Locked） • Disabled ユーザーが無効（User Disabled）
Uptime	プロセスが実行されている期間。	seconds
Memory used	プロセスによって使用された RSS メモリ。	bytes

クラスタメトリック

クラスタのヘルスモニターは、クラスタとそのノードに関連する統計情報と、負荷分散、パフォーマンス、および CCL トラフィックの統計データの集約結果を追跡します。

表 *12:* クラスタメトリック

メトリック	説明	書式
CPU	クラスタノード上の CPU メトリックの平均（データプレーンと snort についてそれぞれ表示）。	percentage
メモリ	クラスタノード上のメモリメトリックの平均（データプレーンと snort についてそれぞれ表示）。	percentage
データスループット	クラスタの着信および発信データトラフィックの統計。	bytes

メトリック	説明	書式
CCL スループット	クラスタの着信および発信 CCL トラフィックの統計。	bytes
接続（Connections）	クラスタ内のアクティブな接続数。	number
NAT Translations	クラスタの NAT 変換数。	number
Distribution	1 秒ごとのクラスタ内の接続分布数。	number
パケット	クラスタ内の1秒ごとのパケット配信の件数。	number

NTP サーバーグループのメトリック

ヘルスモニターは、管理対象デバイスの NTP クロック同期ステータス関連の統計をトラッキングします。

表 *13 : NTP* サーバーグループのメトリック

メトリック	説明	書式
遅延	NTP サーバーへの到達の遅延。	milliseconds
ジッタ	デバイスと NTP サーバー間のネットワーク遅延。	milliseconds
最終ポーリング（Last polled）	NTP サーバーに対するデバイスの最終ポーリング以降の時間。	seconds
Offset	ローカルクロックと NTP サーバーのクロックの差。	seconds
Reach	最新の 8 つの NTP 更新（8 進数）。たとえば、8 回の試行が成功した場合は 377 で表されます。	number

フローオフロード統計グループのメトリック

ヘルスモニタリングは、Threat Defense 9300 および 4100 プラットフォームのハードウェア フロー オフロード統計をトラッキングします。

表 *14 :* フローオフロード統計グループのメトリック

メトリック	説明	書式
使用中（In Use）	現在オフロードされているフローの数。	number

メトリック	説明	書式
最も使用されている（Most Used）	これまでに確認されたオフロードフローの最大数。	number
コリジョンフローの数（Number of Collision Flows）	同じハードウェアオフロードの場所を同時に照合する複数のフローの数。	number
オフロード率（Offload Percentage）	現時点でハードウェアにオフロードされている合計フロー数の割合。	percentage

ルート統計グループのメトリック

ヘルスモニターは、Threat Defense デバイスからの IPv4 と IPv6 の両方のルート情報をトラッキングします。

表 *15 :* ルート統計グループのメトリック

メトリック	説明	書式
現在のIPv4およびIPv6ルート数（Current IPv4 and IPv6 routes）	現在の IPv4 および IPv6 のルート数。	number
グローバルIPv4ルート数（Global IPv4 routes）	グローバル IPv4 ルート数。	number
グローバルIPv6ルート数（Global IPv6 routes）	グローバル IPv6 ルート数。	number
ピークIPv4およびIPv6ルート数（Peak IPv4 and IPv6 routes）	IPv4 および IPv6 のピークルート数。	number
VRFあたりの合計IPv4ルート数（Per VRF Total IPv4 routes）	VRF あたりの IPv4 ルートの総数。	number
VRFあたりの合計IPv6ルート数（Per VRF Total IPv6 routes）	VRF あたりの IPv6 ルートの総数。	number

VPN グループのメトリック

ヘルスモニタリングは、サイト間およびリモートアクセスの VPN トンネル統計をトラッキングします。

表 *16 : VPN* グループのメトリック

メトリック	説明	書式
アクティブRA VPNトンネル数（Active RA VPN Tunnels）	アクティブなリモートアクセス VPN トンネルの数。	number
アクティブS2S VPNトンネル数（Active S2S VPN Tunnels）	アクティブなサイト間 VPN トンネルの数。	number
累積RA VPNセッション数（Cumulative RA VPN Sessions）	アクティブだったリモートアクセス VPN トンネルの現時点までの合計数。	number
累積S2S VPNセッション数（Cumulative S2S VPN Sessions）	アクティブだったサイト間 VPN トンネルの現時点までの合計数。	number
非アクティブRA VPNトンネル数（Inactive RA VPN Tunnels）	非アクティブなリモートアクセス VPN トンネルの数。	number
最大同時RA VPNトンネル数（Peak Concurrent RA VPN Tunnels）	同時にアクティブだったリモートアクセス VPN トンネルの現時点までの最大数。	number
最大同時S2S VPNトンネル数（Peak Concurrent S2S VPN Tunnels）	同時にアクティブだったサイト間 VPN トンネルの現時点までの最大数。	number

Cisco Advanced Malware Protection 接続グループのメトリック

ヘルスモニタリングは、Threat Defense デバイスからの Cisco Advanced Malware Protection クラウド接続ステータスをトラッキングします。

表 *17*:

メトリック	説明	書式
接続ステータス	Cisco Advanced Malware Protection クラウド接続のステータス。	0 ～ 5 の範囲の数値： • 0 は無効（Disabled）を示します。 • 1 は待機中（Waiting）を示します。 • 2 は実行中（Running）を示します。 • 3 は未設定（Not configured）を示します。 • 4 は、Cisco Advanced Malware Protection クラウド接続がオンであることを示します。 • 5 は、Cisco Advanced Malware Protection クラウド接続がオフであることを示します。

AMP Threat Grid 接続グループのメトリック

ヘルスモニタリングは、Threat Defense デバイスからの AMP Threat Grid クラウド接続ステータスをトラッキングします。

表 *18*:

メトリック	説明	書式
接続ステータス	AMP Threat Grid クラウド接続のステータス。	0 ～ 5 の範囲の数値： • 0 は無効（Disabled）を示します。 • 1 は待機中（Waiting）を示します。 • 2 は実行中（Running）を示します。 • 3 は未設定（Not configured）を示します。 • 4 は、AMP Threat Grid クラウド接続がオンであることを示します。 • 5 は、AMP Threat Grid クラウド接続がオフであることを示します。

Device Health メトリックの履歴

機能	バージョン	詳細
ASP ドロップの可視性の向上	7.4.0	ASP ドロップダッシュボードに新しい正常性メトリックが追加され、ASP ドロップの可視性が強化されました。新しいメトリックを使用すると、パケットと接続のドロップのさらなる理由をモニターできます。
新しいクラスタ ヘルス モニター ダッシュボード	7.3	クラスタ ヘルス モニター メトリックを表示するための新しいダッシュボードが、次のコンポーネントで導入されました。 • [概要（Overview）]：クラスタトポロジ、クラスタ統計、およびメトリックチャートに関する情報を表示します。 • [負荷分散（Load Distribution）]：クラスタノード間の負荷分散を表示します。 • [メンバーパフォーマンス（Member Performance）]：クラスタのすべてのメンバーノードの現在のメトリックを表示します。 • [CCL]：クラスタの制御リンクデータ、つまり入力レートと出力レートをグラフ形式で表示します。 （注） これらの機能は、クラスタでのみ使用できます。したがって、クラスタダッシュボードを表示して使用するには、[モニタリング（Monitoring）] ペインの [デバイス（Devices）] リストでクラスタを選択する必要があります。 新規/変更された画面：**[システム（System）]** > **[正常性（Health）]** > **[モニター（Monitor）]**。
ハードウェア電源ユニット（PSU）のファン速度と温度のモニター	7.3	カスタムメトリックグループの [ハードウェア/環境ステータス（Hardware/Environment Status）] に、電源ユニットをモニターするためのメトリックが新たに追加されました。新しいメトリックには、PSU ファン速度、PSU ファンステータス、PSU 温度、および PSU 入出力メトリックが含まれます。 （注） これらの機能は、脅威防御ハードウェアでのみ使用できます。したがって、[モニタリング（Monitoring）] ペインの [デバイス（Devices）] リストで適切なデバイスを選択する必要があります。 新規/変更された画面：**[システム（System）]** > **[正常性（Health）]** > **[モニター（Monitor）]**。
エレファントフローの検出	7.1	ヘルスモニターには、次の拡張機能が含まれます。 • 接続統計情報には、アクティブなエレファントフローが含まれます。 • 接続グループメトリックには、アクティブなエレファントフローの数が含まれます。

機能	バージョン	詳細
新しいヘルス モジュール	7.0	次の正常性モジュールが追加されました。 • [Cisco Advanced Malware Protection接続ステータス（AMP Connection Status）]：Threat Defense からの Cisco Advanced Malware Protection クラウド接続をモニターします。 • [AMP Threat Gridのステータス（AMP Threat Grid Status）]：Threat Defense からの AMP Threat Grid クラウド接続をモニターします。 • [ASPドロップ（ASP Drop）]：データプレーンの高速セキュリティパスによってドロップされた接続をモニターします。 • [高度なSnort統計情報（Advanced Snort Statistics）]：パケットパフォーマンス、フローカウンタ、およびフローイベントに関連する Snort 統計情報をモニターします。 • [ハードウェアと環境のステータス（Hardware and Environment Status）]：Threat Defense デバイスからデバイスのハードウェアと環境のメトリックをモニターします。 • [フローオフロード（Flow Offload）]：Threat Defense 9300 および 4100 プラットフォームのハードウェア フロー オフロード統計をモニターします。 • [NTPステータス（NTP Status）]：管理対象デバイスの NTP クロック同期ステータスをモニターします。 • [ルーティング統計情報（Routing Statistics）]：Threat Defense からの IPv4 と IPv6 の両方のルート情報をモニターします。 • [SSE接続ステータス（SSE Connection Status）]：Threat Defense からの SSE クラウド接続をモニターします。 • [VPN統計（VPN Statistics）]：サイト間およびリモートアクセスの VPN トンネルの統計をモニターします。 • [TLSカウンタ（TLS Counters）]：xTLS/SSL フロー、メモリ、およびキャッシュの有効性をモニターします。

機能	バージョン	詳細
新しいヘルス モジュール	6.7	CPU 使用率をトラッキングするために、次のメトリックが追加されました。 • CPU 使用率（コアごと）：すべてのコアの CPU 使用率をモニターします。 • CPU使用率データプレーン：デバイス上のすべてのデータプレーンプロセスの平均 CPU 使用率をモニターします。 • CPU 使用率 Snort：デバイス上の Snort プロセスの平均 CPU 使用率をモニターします。 • CPU 使用率システム：デバイス上のすべてのシステムプロセスの平均 CPU 使用率をモニターします。 デバイスの正常性の統計情報をトラッキングするために、次のメトリックグループが追加されました。 • [接続統計情報（Connection Statistics）]：接続統計情報と NAT 変換カウントをモニターします。 • クリティカルプロセス統計情報：クリティカルプロセスの状態、リソース消費量、再起動回数をモニターします。 • 展開された設定の統計情報：展開された設定に関する統計情報（ACE の数や IPS ルールなど）をモニターします。 • [Snort統計情報（Snort Statistics）]：イベント、フロー、およびパケットの Snort 統計情報をモニターします。 メモリ使用率をトラッキングするために、次のメトリックが追加されました。 • [メモリ使用率データプレーン（Memory Usage Data Plane）]：データプレーンプロセスで使用される割り当て済みメモリの割合をモニターします。 • メモリ使用率 Snort：Snort プロセスによって使用される割り当て済みメモリの割合をモニターします。

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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。