ヘルス モニタリングの使用

ヘルス モニタは、防御センターからアプライアンスの正常性を確認するためのさまざまなテストを提供します。ヘルス モニタを使用すれば、*正常性ポリシー*とも呼ばれるテストのコレクションを作成し、正常性ポリシーを 1 つ以上のアプライアンスに適用できます。システム内のすべてのアプライアンスに共通の正常性ポリシーを作成することも、適用を予定している特定のアプライアンス用に正常性ポリシーをカスタマイズすることも、デフォルトの正常性ポリシーを使用することもできます。別の防御センターからエクスポートした正常性ポリシーをインポートすることもできます。

*ヘルス モジュール*とも呼ばれるテストは、指定された基準に照らしてテストするスクリプトです。テストを有効または無効にするか、テスト設定を変更することによって、正常性ポリシーを変更したり、不要になった正常性ポリシーを削除したりできます。アプライアンスをブラックリストに登録することによって、選択したアプライアンスからのメッセージを抑制することもできます。

正常性ポリシー内のテストは設定された時間間隔で自動的に実行されます。すべてのテストを実行することも、オンデマンドで特定のテストを実行することもできます。ヘルス モニタは設定されたテスト条件に基づいてヘルス イベントを収集します。オプションで、ヘルス イベントに対応して警告する電子メール、SNMP、または syslog を設定することもできます。

防御センターでは、システム全体または特定のアプライアンスに関するヘルス ステータス情報を表示できます。完全にカスタマイズ可能なイベント ビューを使用すれば、ヘルス モニタによって収集されたヘルス ステータス イベントを迅速かつ容易に分析できます。このイベント ビューでは、イベント データを検索して表示したり、調査中のイベントに関係する他の情報にアクセスしたりできます。

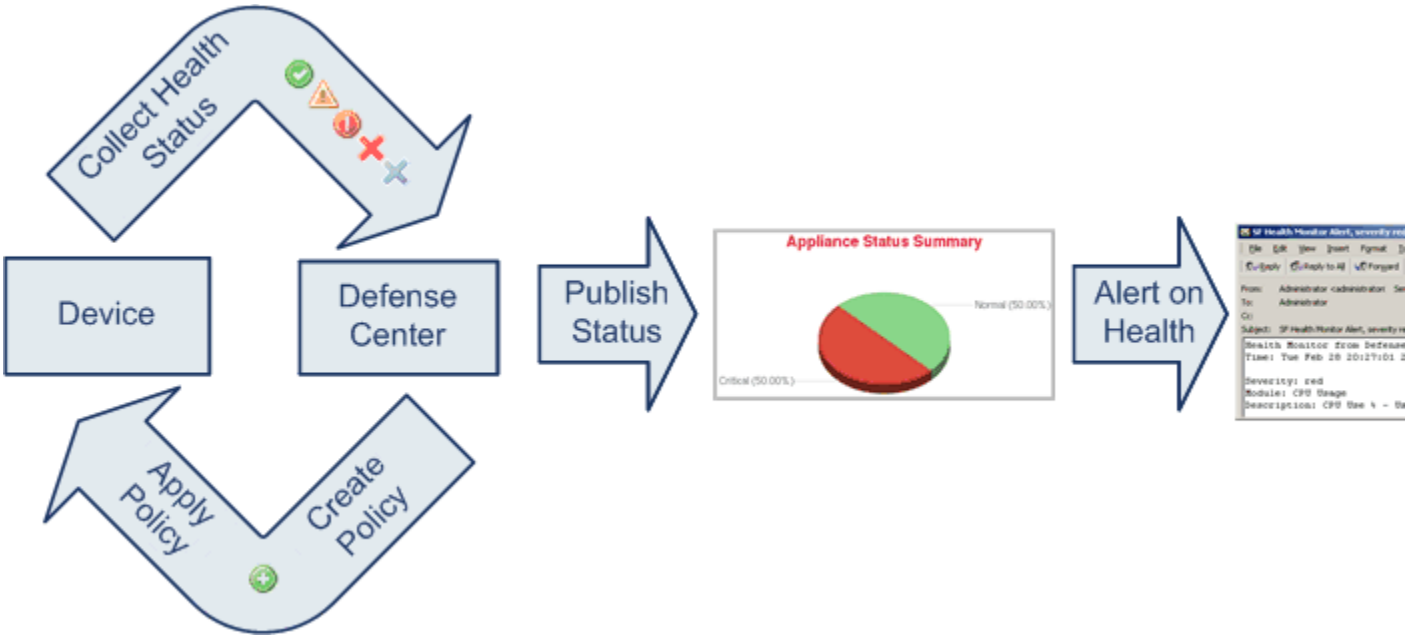
サポートから依頼された場合に、アプライアンスのトラブルシューティング ファイルを作成することもできます。

詳細については、次の項を参照してください。

ヘルス モニタリングについて

ライセンス：任意

ヘルス モニタを使用して、FireSIGHT システム展開全体の重要な機能のステータスを確認できます。防御センターを通して管理対象デバイスのそれぞれに正常性ポリシーを適用し、防御センターで結果のヘルス データを収集することによって、FireSIGHT システム全体の正常性を監視します。[Health Monitor] ページ上の円グラフとステータス テーブルは、監視対象のアプライアンスのヘルス ステータスを視覚的に表しているため、一目でステータスをチェックでき、必要に応じてステータス詳細にドリルダウンできます。



ヘルス モニタを使用して、システム全体または特定のアプライアンスのヘルス ステータス情報にアクセスできます。[Health Monitor] ページには、システム上のすべてのアプライアンスのステータスの概要が表示されます。個々のアプライアンスのヘルス モニタを使用すれば、特定のアプライアンスのヘルス詳細にドリルダウンできます。

標準の FireSIGHT システム テーブル ビューでヘルス イベントを表示することもできます。個々のアプライアンスのヘルス モニタから、特定のイベント発生のテーブル ビューを開いたり、そのアプライアンスのすべてのステータス イベントを取得したりできます。特定のヘルス イベントを検索することもできます。たとえば、特定のパーセンテージの CPU 使用率の全記録を表示する場合は、CPU 使用率モジュールを検索して、パーセンテージ値を入力できます。

ヘルス イベントに対応した電子メール、SNMP、または syslog アラートを設定することもできます。*ヘルス アラート*は、標準アラートとヘルス ステータス レベルを関連付けたものです。たとえば、アプライアンスでハードウェアの過負荷が原因で障害が発生することは絶対ないことを確認する必要がある場合は、電子メール アラートをセットアップできます。その後で、CPU、ディスク、またはメモリの使用率がそのアプライアンスに適用される正常性ポリシーで設定された警告レベルに達するたびにその電子メール アラートをトリガーとして使用するヘルス アラートを作成できます。アラートしきい値を、受け取る反復アラートの数が最小になるように設定できます。

ヘルス モニタリングは管理活動であるため、管理者ユーザー ロール特権を持っているユーザーのみがシステム ヘルス データにアクセスできます。ユーザ特権の割り当て方法については、「ユーザ特権とオプションの変更」（P.48-58）を参照してください。

注　防御センターを除いて、FireSIGHT システム デバイスにはデフォルトでヘルス モニタリング ポリシーが適用されません。管理対象デバイスはハードウェア アラーム ヘルス モジュール経由で自動的にハードウェア ステータスを報告します。他のモジュールを使用して管理対象デバイスを監視する場合は、正常性ポリシーをそのデバイスに適用する必要があります。シスコが提供するアプライアンス用のデフォルト正常性ポリシーの詳細については、「デフォルト正常性ポリシーについて」（P.55-8）を参照してください。カスタマイズした正常性ポリシーの作成方法については、「正常性ポリシーの作成」（P.55-9）を参照してください。ポリシーの適用について詳しくは、「正常性ポリシーの適用」（P.55-32）を参照してください。

正常性ポリシーと、システム ヘルスをテストするために実行可能なヘルス モジュールの詳細については、次のトピックを参照してください。

- 「正常性ポリシーについて」（P.55-3）
- 「ヘルス モジュールについて」（P.55-3）
- 「ヘルス モニタリング設定について」（P.55-6）

正常性ポリシーについて

ライセンス：任意

*正常性ポリシー*は、防御センターがアプライアンスの正常性をチェックするときに使用する基準を定義するためにアプライアンスに適用するヘルス モジュール設定のコレクションです。ヘルス モニタは、FireSIGHT システムのハードウェアとソフトウェアが正しく機能していることを確認するためのさまざまなヘルス インジケータを追跡します。

正常性ポリシーを作成するときに、アプライアンスの正常性を確認するために実行するテストを選択します。また、デフォルト正常性ポリシーをアプライアンスに適用することもできます。

ヘルス モジュールについて

ライセンス：任意

*ヘルス テスト*とも呼ばれる*ヘルス モジュール*は、正常性ポリシー内で指定された基準に照らしてテストするスクリプトです。使用可能なヘルス モジュールの説明を次の表に示します。

表 55-1　ヘルス モジュール

モジュール	説明
高度なマルウェア対策	このモジュールは、ファイル ポリシー設定に基づいて、ネットワーク トラフィックで検出されたファイルに関するファイル性質情報を取得するため、または動的分析用にファイルを送信するために防御センターが Collective Security Intelligence クラウドに接続できなかった場合、または、ネットワーク トラフィックで過剰なファイル数が検出された場合に警告します。 このモジュールは、高度なマルウェア対策をサポートしていない DC500 を除くすべての防御センター上で動作します。
アプライアンス ハートビート	このモジュールは、アプライアンス ハートビートがアプライアンスから届いているかどうかを確認し、アプライアンスのハートビート ステータスに基づいてアラートを出します。
自動アプリケーション バイパス ステータス	このモジュールは、アプライアンスがバイパスしきい値で設定された秒数以内に応答しなかったためにバイパスされたかどうかを確認し、バイパスが発生した場合にアラートを出します。
CPU 使用率	このモジュールは、アプライアンス上の CPU が過負荷になっていないことを確認し、CPU 使用率がモジュールに設定されたパーセンテージを超えた場合にアラートを出します。 このモジュールは、3D9900 デバイスに適用される正常性ポリシーでは使用できません。
カード リセット	このモジュールは、リセット時に、ハードウェア障害原因で再起動されたネットワーク カードをチェックし、アラートを出します。
ディスカバリ イベント ステータス	このモジュールは、指定された時間内にデバイスでディスカバリ イベントが検出されたかどうかを示します。
ディスク ステータス	このモジュールは、ハード ディスクと、アプライアンス上のマルウェア ストレージ パック（設置されている場合）のパフォーマンスを調査します。また、ハード ディスクと RAID コントローラ（設置されている場合）に障害が発生する恐れがある場合、あるいは、マルウェア ストレージ パックが設置後に検出されないまたは正規品でない場合にアラートを出します。
ディスク使用率	このモジュールは、アプライアンスのハード ドライブとマルウェア ストレージ パック上のディスク使用率をモジュールに設定された制限と比較し、その使用率がモジュールに設定されたパーセンテージを超えた時点でアラートを出します。また、モジュールしきい値に基づいて、システムが監視対象のディスク使用カテゴリ内のファイルを過剰に削除する場合、または、これらのカテゴリを除くディスク使用率が過剰なレベルに達した場合にもアラートを出します。
FireAMP ステータス モニタ	このモジュールは、防御センターが初期接続の成功後にシスコ クラウドに接続できない場合、または FireAMP ポータルを使用してクラウド接続を登録解除した場合、アラートを出します。 このモジュールは、防御センター上でのみ動作します。
FireSIGHTホスト ライセンス制限	このモジュールは、十分な FireSIGHT ホスト ライセンスが残っているかどうかを確認し、モジュールに設定された警告レベルに基づいてアラートを出します。 このモジュールは、防御センター上でのみ動作します。

表 55-1　　ヘルス モジュール（続き）

モジュール	説明
ハードウェア アラーム	このモジュールは、シリーズ 3 または 3D9900 デバイス上のハードウェアを交換する必要があるかどうかを確認し、ハードウェア ステータスに基づいてアラートを出します。また、ハードウェア関連デーモンのステータスとクラスタ化されたアプライアンスのステータスについて報告します。 これらのデバイスについて報告される詳細については、「3D9900 デバイスのハードウェア アラート詳細の解釈」（P.55-55）と「シリーズ 3 デバイスのハードウェア アラート詳細の解釈」（P.55-56）を参照してください。
ヘルス モニタ プロセス	このモジュールは、ヘルス モニタ自体のステータスを監視し、防御センターで受信された最後のステータス イベント以降の分数が警告制限または重大制限を超えた場合にアラートを出します。 このモジュールは、防御センター上でのみ動作します。
インライン リンク不一致アラーム	このモジュールは、インライン セットに関連付けられたポートを監視し、インライン ペアの 2 つのインターフェイスが別々の速度をネゴシエートした場合にアラートを出します。
侵入イベント レート	このモジュールは、1 秒あたりの侵入イベント数をこのモジュールに設定された制限と比較し、制限を超えた場合にアラートを出します。侵入イベント レートが 0 の場合は、侵入プロセスがダウンしているか、管理対象デバイスがイベントを送信していない可能性があります。イベントがデバイスから送られているかどうかをチェックするには、[Analysis] > [Intrusions] > [Events] の順に選択します。
ライセンス モニタ	このモジュールは、Control、Protection、URL Filtering、Malware、および VPN 用の十分なライセンスが残っているかどうかを確認します。また、スタック内のデバイスに適合しないライセンス セットが含まれている場合にアラートを出します。モジュールに自動的に設定された警告レベルに基づいてアラートを出します。このモジュールの設定は変更できません。 このモジュールは、防御センター上でのみ動作します。
リンクステート伝達	このモジュールは、ペア化されたインライン セット内のリンクで障害が発生した時点を特定して、リンクステート伝達モードをトリガーとして使用します。
メモリ使用率	このモジュールは、アプライアンス上のメモリ使用率をモジュールに設定された制限と比較し、使用率がモジュールに設定されたレベルを超えるとアラートを出します。
電源	このモジュールは、デバイスの電源が交換が必要かどうかを確認し、電源ステータスに基づいてアラートを出します。 このモジュールは、防御センター DC1500、DC3500 上で動作します。 このモジュールは、デバイス 3D3500、3D4500、3D6500、3D9900、および シリーズ 3 上で動作します。
プロセス ステータス	このモジュールは、アプライアンス上のプロセスがプロセス マネージャの外部で停止または終了したかを確認します。プロセスが故意にプロセス マネージャの外部で停止された場合は、モジュールが再開してプロセスが再起動するまで、モジュール ステータスが Warning に変更され、ヘルス イベント メッセージが停止されたプロセスを示します。プロセスがプロセス マネージャの外部で異常終了またはクラッシュした場合は、モジュールが再開してプロセスが再起動するまで、モジュール ステータスが Critical に変更され、ヘルス イベント メッセージが終了したプロセスを示します。
RRD サーバ プロセス	このモジュールは、時系列データを保存するラウンド ロビン データ サーバが正常に動作しているかどうかを確認し、最近の RRD サーバの再起動回数に基づいてアラートを出します。 このモジュールは、防御センター上でのみ動作します。

表 55-1　ヘルス モジュール（続き）

モジュール	説明
セキュリティ インテリジェンス	このモジュールは、フィード更新、フィード破損、メモリ問題などのセキュリティ インテリジェンス フィルタリングに関するさまざまな状況でアラートを出します。 このモジュールは、セキュリティ インテリジェンス フィルタリングをサポートしていない DC500 以外のすべての防御センター上で動作します。
時系列データ モニタ	このモジュールは、時系列データ（コンプライアンス イベント カウントなど）が保存されるディレクトリ内の破損ファイルの存在を追跡して、ファイルが破損としてフラグが付けられ、削除された段階でアラートを出します。 このモジュールは、防御センター上でのみ動作します。
時刻同期ステータス	このモジュールは、NTP を使用して時刻を取得するデバイス クロックと NTP サーバ上のクロックの同期を追跡して、クロックの差が 10 秒を超えた場合にアラートを出します。
トラフィック ステータス	このモジュールは、デバイスが現在トラフィックを収集しているかどうかを確認して、トラフィック ステータスに基づいてアラートを出します。
URL フィルタリング モニタ	このモジュールは、通常訪問される URL に関する URL フィルタリング（カテゴリとレピュテーション）データをシステムが取得する防御センターと シスコ クラウド間の通信を追跡します。防御センターがクラウドとの通信またはクラウドからの更新の取得に失敗した場合にアラートを出します。 このモジュールは、防御センターと、URL フィルタリングが有効になっている管理対象デバイス間の通信も追跡します。防御センターが URL フィルタリング データをそのようなデバイスにプッシュできない場合にアラートを出します。 このモジュールは、URL フィルタリングをサポートしていない DC500 以外のすべての防御センター上でのみ動作します。
ユーザ エージェント ステータス モニタ	このモジュールは、防御センターに接続されたユーザ エージェントでハートビートが検出されない場合にアラートを出します。 このモジュールは、防御センター上でのみ動作します。
VPN ステータス	このモジュールは、VPN 機能が動作していないことをシステムが検出するとアラートを出します。 このモジュールは、防御センター上でのみ動作します。

ヘルス モニタリング設定について

ライセンス：任意

次の手順に示すように、FireSIGHT システム上でヘルス モニタリングをセットアップするためのいくつかのステップがあります。

ステップ 1　アプライアンス用の正常性ポリシーを作成します。

FireSIGHT システムで使用しているアプライアンスの種類ごとに固有のポリシーをセットアップして、そのアプライアンスに適切なテストだけを有効にすることができます。

ヒント　モニタリング動作をカスタマイズすることなくすぐにヘルス モニタリングを有効にするには、そのために用意されたデフォルト ポリシーを適用できます。

正常性ポリシーのセットアップについては、「正常性ポリシーの設定」（P.55-7）を参照してください。

ステップ 2　ヘルス ステータスを追跡するアプライアンスごとに正常性ポリシーを適用します。すぐに適用できるデフォルト正常性ポリシーについては、「デフォルト正常性ポリシーについて」（P.55-8）を参照してください。

ステップ 3　オプションで、ヘルス モニタ アラートを設定します。

ヘルス ステータス レベルが特定のヘルス モジュールの特定の重大度レベルに達した段階でトリガーされる電子メール、Syslog、または SNMP アラートをセットアップできます。

ヘルス モニタ アラートのセットアップについては、「ヘルス モニタ アラートの設定」（P.55-41）を参照してください。

システム上でヘルス モニタリングをセットアップしたら、[Health Monitor] ページまたは [Health Events] テーブル ビューでいつでもヘルス ステータスを確認できます。システム正常性データの表示方法については、次のトピックを参照してください。

- 「ヘルス モニタの使用」（P.55-44）
- 「アプライアンス ヘルス モニタの使用」（P.55-46）
- 「ヘルス イベントの操作」（P.55-52）

正常性ポリシーの設定

ライセンス：任意

正常性ポリシーには、複数のモジュールに対して設定されたヘルス テスト基準が含まれます。アプライアンスごとにどのヘルス モジュールを実行するかを制御したり、モジュールごとに実行するテストで使用される特定の制限を設定したりできます。正常性ポリシーで設定可能なヘルス モジュールの詳細については、「ヘルス モニタリングについて」（P.55-2）を参照してください。

システム内のすべてのアプライアンスに適用可能な 1 つの正常性ポリシーを作成することも、適用を計画している特定のアプライアンス用に正常性ポリシーをカスタマイズすることも、付属のデフォルト正常性ポリシーを使用することもできます。別の防御センターからエクスポートした正常性ポリシーをインポートすることもできます。

正常性ポリシーを設定するときに、そのポリシーに対して各ヘルス モジュールを有効にするかどうかを決定します。また、有効にした各モジュールが、プロセスの正常性を評価するたびに報告するヘルス ステータスを制御するための基準を選択することもできます。

防御センター に自動的に適用されるデフォルト正常性ポリシーの詳細については、「デフォルト正常性ポリシーについて」（P.55-8）を参照してください。

詳細については、次のトピックを参照してください。

- 「デフォルト正常性ポリシーについて」（P.55-8）
- 「正常性ポリシーの作成」（P.55-9）
- 「正常性ポリシーの適用」（P.55-32）
- 「正常性ポリシーの編集」（P.55-33）
- 「正常性ポリシーの比較」（P.55-35）
- 「正常性ポリシーの削除」（P.55-38）

デフォルト正常性ポリシーについて

ライセンス：任意

防御センター ヘルス モニタには、アプライアンスのヘルス モニタリングの迅速な実装を容易にするデフォルト正常性ポリシーが付属しています。デフォルト正常性ポリシーは、自動的に防御センターに適用されます。デフォルト正常性ポリシーを編集することはできませんが、コピーしてその設定に基づくカスタム ポリシーを作成することができます。詳細については、「正常性ポリシーの作成」（P.55-9）を参照してください。

また、デバイスの正常性を監視するために、正常性ポリシーを管理対象デバイスにプッシュすることもできます。

注　正常性ポリシーを Sourcefire Software for X-Series に適用することはできません。

デフォルト正常性ポリシーでは、実行中のプラットフォーム上で使用可能なヘルス モジュールのほとんどが自動的に有効になります。次の表に、防御センターと管理対象デバイスのデフォルト ポリシーでアクティブにされているモジュールの詳細を示します。

表 55-2　デフォルト アクティブ ヘルス モジュール

モジュール	防御センター	管理対象デバイス
高度なマルウェア対策	Yes	No
アプライアンス ハートビート	Yes	No
自動アプリケーション バイパス	No	Yes
CPU 使用率	No	No
カード リセット	No	No
ディスカバリ イベント ステータス	No	No
ディスク ステータス	Yes	Yes
ディスク使用率	Yes	Yes
FireAMP ステータス モニタ	Yes	No
FireSIGHT ホスト ライセンス制限	Yes	No
ハードウェア アラーム	No	Yes
ヘルス モニタ プロセス	No	No
インライン リンク不一致アラーム	No	Yes
侵入イベント レート	No	Yes
ライセンス モニタ	Yes	No
リンクステート伝達	No	Yes
メモリ使用率	Yes	Yes
電源	No	Yes
プロセス ステータス	Yes	Yes
RRD サーバ プロセス	Yes	No
セキュリティ インテリジェンス	Yes	No
時系列データ モニタ	Yes	No

表 55-2　デフォルト アクティブ ヘルス モジュール（続き）

モジュール	防御センター	管理対象デバイス
時刻同期ステータス	Yes	Yes
トラフィック ステータス	No	Yes
URL フィルタリング モニタ	Yes	No
ユーザ エージェント ステータス モニタ	Yes	No
VPN ステータス	Yes	No

正常性ポリシーの作成

ライセンス：任意

アプライアンスで使用する正常性ポリシーをカスタマイズすることによって、新しいポリシーを作成できます。ポリシー内の設定は、最初に、新しいポリシーの基準として選択した正常性ポリシー内の設定を使用して生成されます。必要に応じて、ポリシー内のモジュールを有効または無効にし、各モジュールのアラート基準を変更できます。

ヒント　新しいポリシーを作成する代わりに、別の防御センターから正常性ポリシーをエクスポートして、それを対象の防御センターにインポートできます。その後で、インポートしたポリシーをニーズに合わせて編集してから、適用できます。詳細については、「設定のインポートおよびエクスポート」（P.A-1）を参照してください。

正常性ポリシーを作成する方法：

アクセス：Admin/Maint

ステップ 1　[Health] > [Health Policy] の順に選択します。

[Health Policy] ページが表示されます。

ステップ 2　[Create Policy] をクリックします。

[Create Health Policy] ページが表示されます。

ステップ 3　[Copy Policy] ドロップダウン リストから、新しいポリシーの基準として使用する既存のポリシーを選択します。

ステップ 4　ポリシーの名前を入力します。

ステップ 5　ポリシーの説明を入力します。

ステップ 6　[Save] を選択して、ポリシー情報を保存します。

[Health Policy Configuration] ページが開いて、モジュールのリストが表示されます。

ステップ 7　次の項の説明に従って、アプライアンスのヘルス ステータスをテストするために使用する各モジュールの設定を構成します。

- 「ポリシー実行時間間隔の設定」（P.55-11）
- 「高度なマルウェア対策モニタリングの設定」（P.55-11）
- 「アプライアンス ハートビート モニタリングの設定」（P.55-12）
- 「自動アプリケーション バイパス モニタリングの設定」（P.55-13）

- 「CPU 使用率モニタリングの設定」（P.55-13）
- 「カード リセット モニタリングの設定」（P.55-14）
- 「ディスカバリ イベント ステータス モニタリングの設定」（P.55-15）
- 「ディスク ステータス モニタリングの設定」（P.55-16）
- 「ディスク使用率モニタリングの設定」（P.55-16）
- 「ステータス モニタリングFireAMPの設定」（P.55-17）
- 「FireSIGHT ホスト使用量モニタリングの設定」（P.55-18）
- 「ハードウェア アラーム モニタリングの設定」（P.55-19）
- 「ヘルス ステータス モニタリングの設定」（P.55-20）
- 「インライン リンク不一致アラーム モニタリングの設定」（P.55-21）
- 「侵入イベント レート モニタリングの設定」（P.55-21）
- 「ライセンス モニタリングについて」（P.55-22）
- 「リンクステート伝達モニタリングの設定」（P.55-22）
- 「メモリ使用率モニタリングの設定」（P.55-23）
- 「電源モニタリングの設定」（P.55-24）
- 「プロセス ステータス モニタリングの設定」（P.55-25）
- 「RRD サーバ プロセス モニタリングの設定」（P.55-26）
- 「セキュリティ インテリジェンス モニタリングの設定」（P.55-27）
- 「時系列データ モニタリングの設定」（P.55-28）
- 「時刻同期モニタリングの設定」（P.55-28）
- 「トラフィック ステータス モニタリングの設定」（P.55-29）
- 「URL フィルタリングモニタリングの設定」（P.55-30）
- 「ユーザ エージェント ステータス モニタリングの設定」（P.55-30）
- 「VPN ステータス モニタリングの設定」（P.55-31）

注　設定を構成するときに、それぞれの [Health Policy Configuration] ページでヘルス ステータスをテストするために実行するモジュールが有効になっていることを確認します。無効になっているモジュールは、そのモジュールを含むポリシーがアプライアンスに適用されていても、ヘルス ステータス フィードバックを生成しません。

ステップ 8　[Save Policy and Exit] をクリックしてポリシーを保存します。

有効にするには、それぞれのアプライアンスにポリシーを適用する必要があります。正常性ポリシーの適用方法については、「正常性ポリシーの適用」（P.55-32）を参照してください。

ポリシー実行時間間隔の設定

ライセンス：任意

正常性ポリシーのポリシー実行時間間隔を変更することによって、正常性テストの実行頻度を制御できます。設定可能な最大実行時間間隔は 99999 分です。

注意　5 分未満の実行時間間隔を設定しないでください。

ポリシー実行時間間隔を設定する方法：

アクセス：Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Policy Run Time Interval] を選択します。

[Health Policy Configuration — Policy Run Time Interval] ページが表示されます。

ステップ 2　[Run Interval (mins)] フィールドに、テストの自動反復の時間間隔を分単位で入力します。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するアプライアンスに適用する必要があります。詳細については、「正常性ポリシーの適用」（P.55-32）を参照してください。

高度なマルウェア対策モニタリングの設定

ライセンス：Malware

このモジュールは、シスコ クラウドに問い合わせてネットワーク トラフィックでファイルを検出する防御センターの機能の状態と安定性を追跡します。システムで、クラウドとの接続が中断された、接続に使用されている暗号キーが無効である、または一定のタイム フレームで検出されたファイル数が多すぎることが検出された場合は、このモジュールのステータス分類が Warning に変更され、モジュールが正常性アラートを生成します。

高度なマルウェア対策ヘルス モジュールの設定を構成する方法：

アクセス：Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Advanced Malware Protection] を選択します。

[Health Policy Configuration — Advanced Malware Protection] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するアプライアンスに適用する必要があります。詳細については、「正常性ポリシーの適用」（P.55-32）を参照してください。

アプライアンス ハートビート モニタリングの設定

ライセンス：任意

防御センターは、デバイスが実行しており防御センターと正常に通信していることを示すものとして、その管理対象デバイスから、2 分ごとと 200 イベントごとのどちらか早い方でハートビートを受け取ります。アプライアンス ハートビート ヘルス ステータス モジュールは、防御センターが管理対象アプライアンスからハートビートを受信しているかどうかを追跡するために使用します。防御センターがデバイスからのハートビートを検出しない場合、このモジュールのステータス分類が Critical に変わります。このステータス データがヘルス モニタに反映されます。

アプライアンス ハートビート ヘルス モジュールの設定を構成する方法：

アクセス：Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Appliance Heartbeat] を選択します。

[Health Policy Configuration — Appliance Heartbeat] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するアプライアンスに適用する必要があります。詳細については、「正常性ポリシーの適用」（P.55-32）を参照してください。

自動アプリケーション バイパス モニタリングの設定

ライセンス：任意

このモジュールは、管理対象デバイスがバイパスしきい値として設定された秒数以内に応答しなかったためにバイパスされた時点を検出するために使用します。バイパスが発生すると、このモジュールがアラートを生成します。このステータス データがヘルス モニタに反映されます。

自動アプリケーション バイパスの詳細については、「Automatic Application Bypass」（P.6-52）を参照してください。

自動アプリケーション バイパス モニタリング ステータスを設定する方法：

アクセス：Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Automatic Application Bypass Status] を選択します。

[Health Policy Configuration — Automatic Application Bypass Status] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当する管理対象デバイスに適用する必要があります。詳細については、「正常性ポリシーの適用」（P.55-32）を参照してください。

CPU 使用率モニタリングの設定

ライセンス：任意

サポート対象デバイス：任意（3D9900 は除く）

サポート対象防御センター：任意

CPU 使用率が高すぎる場合、ハードウェアをアップグレードする必要がある、または、正しく機能していないプロセスが存在することを示している可能性があります。CPU 使用率ヘルス ステータス モジュールは、CPU 使用率の制限を設定するために使用します。

監視対象アプライアンスの CPU 使用率が警告制限を超えた場合、そのモジュールのステータス分類が Warning に変更されます。監視対象アプライアンスの CPU 使用率が重大制限を超えた場合、そのモジュールのステータス分類が Critical に変更されます。このステータス データがヘルス モニタに反映されます。

両方の制限に設定可能な最大パーセンテージは 100% であり、重大制限は警告制限より高くする必要があります。

CPU 使用率の制限を設定する方法：

アクセス：Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[CPU Usage] を選択します。

[Health Policy Configuration — CPU Usage] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　[Critical Threshold %] フィールドに、重大ヘルス ステータスをトリガーとして使用する CPU 使用率のパーセンテージを入力します。

ステップ 4　[Warning Threshold %] フィールドに、警告ヘルス ステータスをトリガーとして使用する CPU 使用率のパーセンテージを入力します。

ステップ 5　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するアプライアンスに適用する必要があります。詳細については、「正常性ポリシーの適用」（P.55-32）を参照してください。

カード リセット モニタリングの設定

ライセンス：任意

カード リセット モニタリング ヘルス ステータス モジュールは、ハードウェア障害が原因でネットワーク カードが再起動された時点を追跡するために使用します。リセットが発生すると、このモジュールがアラートを生成します。このステータス データがヘルス モニタに反映されます。

カード リセット モニタリングを設定する方法：

アクセス：Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Card Reset] を選択します。

[Health Policy Configuration — Card Reset Monitoring] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。

- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、該当する防御センターに正常性ポリシーを適用する必要があります。詳細については、「正常性ポリシーの適用」（P.55-32）を参照してください。

ディスカバリ イベント ステータス モニタリングの設定

ライセンス：FireSIGHT

ディスカバリ イベント ステータス モジュールは、防御センターが受信するディスカバリ イベントの時間間隔が長すぎる場合に警告することによって、防御センターからデバイス上のディスカバリ プロセスの正常性を監視するために使用します。アラートの生成を引き起こすイベントの時間間隔を秒単位で設定できます。最後のイベント制限以降の待ち時間が [Warning Seconds] に設定された秒数を超えると、そのモジュールのステータス分類が Warning に変更されます。最後のイベント制限以降の待ち時間が [Critical Seconds] を超えると、そのモジュールのステータス分類が Critical に変更されます。このステータス データがヘルス モニタに反映されます。

両方の制限に設定可能な最大秒数は 7200 であり、重大制限は警告制限より高くする必要があります。最小秒数は 3600 です。

ディスカバリ イベント ステータス モジュールの設定を構成する方法：

アクセス：Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Discovery Event Status] を選択します。

[Health Policy Configuration — Discovery Event Status] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　[Critical Seconds since last event] に、重大ヘルス ステータスをトリガーとして使用する前のイベント間で待機する最大秒数を入力します。

ステップ 4　[Warning Seconds since last event] に、警告ヘルス ステータスをトリガーとして使用する前のイベント間で待機する最大秒数を入力します。

ステップ 5　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするためには、正常性ポリシーを防御センターに適用する必要があります。詳細については、「正常性ポリシーの適用」（P.55-32）を参照してください。

ディスク ステータス モニタリングの設定

ライセンス：任意

ディスク ステータス ヘルス モジュールは、アプライアンスのハード ディスクとマルウェア ストレージ パック（設置されている場合）の現在のステータスを監視するために使用します。このモジュールは、ハード ディスクと RAID コントローラ（設置されている場合）で障害が発生する恐れがある場合、または、マルウェア ストレージ パックではない追加のハード ドライブが設置されている場合に、警告（黄色）ヘルス アラートを生成します。また、設置されているマルウェア ストレージ パックを検出できなかった場合はアラート（赤色）ヘルス アラートを生成します。

ディスク ステータス ヘルス モジュールの設定を構成する方法：

アクセス：Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Disk Status] をクリックします。

[Health Policy Configuration — Disk Status] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、「正常性ポリシーの適用」（P.55-32）を参照してください。

ディスク使用率モニタリングの設定

ライセンス：任意

十分なディスク スペースがないと、アプライアンスは動作できません。ヘルス モニタは、スペースが使い果たされる前に、アプライアンスのハード ドライブとマルウェア ストレージ パック上のディスク スペースが少ない状態を特定できます。また、ヘルス モニタは、ハード ドライブのファイル ドレインが頻繁に発生する場合にアラートを出せます。ディスク使用率ヘルス ステータス モジュールは、アプライアンス上の `/` パーティションと `/volume` パーティションのディスク使用率を監視して、ドレイン頻度を追跡するために使用します。

注　ディスク使用率モジュールは `/boot` パーティションを監視対象パーティションとして列挙しますが、そのパーティションのサイズが固定のため、このモジュールはブート パーティションに基づいてアラートを出すことはしません。

監視対象アプライアンスのディスク使用率が警告制限を超えた場合、そのモジュールのステータス分類が Warning に変更されます。監視対象アプライアンスのディスク使用率が重大制限を超えた場合、そのモジュールのステータス分類が Critical に変更されます。両方の制限に設定可能な最大パーセンテージは 100% であり、重大制限は警告制限より高くする必要があります。

システムが未処理のイベントを削除すると、そのモジュールのステータス分類が Warning に変更されます。システムがモジュールしきい値に基づいて、頻繁に、ディスク使用率カテゴリ内のファイルをドレインしている場合、または、監視対象ディスク使用率カテゴリに含まれないファイルのディスク使用率がモジュールしきい値に基づいて大きくなる場合、そのモジュールのステータス分類が Critical に変更されます。ディスク使用率カテゴリの詳細については、「Disk Usage ウィジェットについて」（P.3-29）を参照してください。

ディスク使用率ヘルス モジュールの設定を構成する方法：

アクセス：Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Disk Usage] を選択します。

[Health Policy Configuration — Disk Usage] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　[Critical Threshold %] フィールドに、重大ヘルス ステータスをトリガーとして使用するディスク使用率のパーセンテージを入力します。

ステップ 4　[Warning Threshold %] フィールドに、警告ヘルス ステータスをトリガーとして使用するディスク使用率のパーセンテージを入力します。

ステップ 5　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するアプライアンスに適用する必要があります。詳細については、「正常性ポリシーの適用」（P.55-32）を参照してください。

ステータス モニタリングFireAMPの設定

ライセンス：任意

FireAMP ステータス モニタ モジュールは、次の状況でアラートを出すために使用します。

- 防御センターが シスコ クラウドに最初は正しく接続できたのに、その後接続できない
- FireAMP ポータルを使用してクラウド接続を登録解除した

このようなケースでは、モジュール ステータスが Critical に変更され、失敗した接続に関連付けられたクラウド名が表示されます。クラウド接続の設定方法については、「FireAMP 用のクラウド接続の操作」（P.33-24）を参照してください。

FireAMP ステータス モニタ モジュールの設定を構成する方法：

アクセス：Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[FireAMP Status Monitor] を選択します。

[Health Policy Configuration — FireAMP Status Monitor] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、FireAMP ステータス モニタリングに対するモジュールの使用を有効にします。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを防御センターに適用する必要があります。詳細については、「正常性ポリシーの適用」（P.55-32）を参照してください。

FireSIGHT ホスト使用量モニタリングの設定

ライセンス：FireSIGHT

FireSIGHT ホスト ライセンス制限ヘルス ステータス モジュールは、FireSIGHT ホスト使用量警告制限を設定するために使用します。監視対象デバイス上の残りの FireSIGHT ホスト数が警告ホスト数制限を下回った場合は、そのモジュールのステータス分類が Warning に変更されます。監視対象デバイス上の残りの FireSIGHT ホスト数が重大ホスト数制限を下回った場合は、そのモジュールのステータス分類が Critical に変更されます。このステータス データがヘルス モニタに反映されます。

両方の制限に設定可能な最大ホスト数は 1000 で、重大ホスト制限数は警告制限より小さくする必要があります。

FireSIGHT ホスト ライセンス制限ヘルス モジュールの設定を構成する方法：

アクセス：Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[**FireSIGHT** Host License Limit] を選択します。

[Health Policy Configuration — FireSIGHT Host License Limit] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　[Critical number Hosts] フィールドに、重大ヘルス ステータスをトリガーとして使用する使用可能なホストの残数を入力します。

ステップ 4　[Warning number Hosts] フィールドに、警告ヘルス ステータスをトリガーとして使用する使用可能なホストの残数を入力します。

ステップ 5　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、「正常性ポリシーの適用」（P.55-32）を参照してください。

ハードウェア アラーム モニタリングの設定

ライセンス：任意

サポート対象デバイス：シリーズ 3、3D9900

ハードウェア アラーム ヘルス ステータス モジュールは、シリーズ 3 または 3D9900 デバイス上でハードウェア障害を検出するために使用します。ハードウェア アラーム モジュールが、障害が発生したハードウェア コンポーネントまたは相互に通信していないクラスタ化されたデバイスを検出すると、そのモジュールのステータス分類が Critical に変更されます。このステータス データがヘルス モニタに反映されます。

3D9900 デバイス上のハードウェア アラートの原因となるハードウェア ステータス状態の詳細については、「3D9900 デバイスのハードウェア アラート詳細の解釈」（P.55-55）を参照してください。

ハードウェア アラーム ヘルス モジュールの設定を構成する方法：

アクセス：Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Hardware Alarms] を選択します。

[Health Policy Configuration — Hardware Alarm Monitor] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、「正常性ポリシーの適用」（P.55-32）を参照してください。

ヘルス ステータス モニタリングの設定

ライセンス：任意

ヘルス モニタ プロセス モジュールは、監視対象アプライアンスから受け取るヘルス イベントの時間間隔が長すぎる場合にアラートを生成することによって、防御センター上でのヘルス モニタの正常性を監視するために使用します。

たとえば、防御センター（myrtle.example.com）がデバイス（dogwood.example.com）を監視する場合は、ヘルス モニタ プロセス モジュールが有効になっている正常性ポリシーを myrtle.example.com に適用します。その後で、ヘルス モニタ プロセス モジュールが、dogwood.example.com から最後のイベントが受信されてから経過した分数を示すイベントを報告します。

アラートの生成を引き起こすイベントの時間間隔を分単位で設定できます。最後のイベント制限以降の待ち時間が [Warning Minutes] に設定された分数を超えると、そのモジュールのステータス分類が Warning に変更されます。最後のイベント制限以降の待ち時間が [Critical Minutes] を超えると、そのモジュールのステータス分類が Critical に変更されます。このステータス データがヘルス モニタに反映されます。

両方の制限に設定可能な最大分数は 144 であり、重大制限は警告制限より高くする必要があります。最小分数は 5 です。

ヘルス モニタ プロセス モジュールの設定を構成する方法：

アクセス：Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Health Monitor Process] を選択します。

[Health Policy Configuration — Health Monitor Process] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　[Critical Minutes since last event] に、重大ヘルス ステータスをトリガーとして使用する前にイベント間で待機する最大分数を入力します。

ステップ 4　[Warning Minutes since last event] に、警告ヘルス ステータスをトリガーとして使用する前にイベント間で待機する最大分数を入力します。

ステップ 5　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするためには、正常性ポリシーを防御センターに適用する必要があります。詳細については、「正常性ポリシーの適用」（P.55-32）を参照してください。

インライン リンク不一致アラーム モニタリングの設定

ライセンス：任意

インライン リンク不一致アラーム ヘルス ステータス モジュールは、インライン セットの両側のインターフェイスが別々の接続速度をネゴシエートした時点を追跡するために使用します。別々にネゴシエートされた速度が検出された場合は、このモジュールがアラートを生成します。

インライン リンク不一致モニタリングを設定する方法：

アクセス：Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Inline Link Mismatch Alarms] を選択します。

[Health Policy Configuration — Inline Link Mismatch Alarms] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、該当する防御センターに正常性ポリシーを適用する必要があります。詳細については、「正常性ポリシーの適用」（P.55-32）を参照してください。

侵入イベント レート モニタリングの設定

ライセンス：Protection

侵入イベント レート ヘルス ステータス モジュールは、ヘルス ステータスの変化をトリガーとして使用する 1 秒あたりのパケット数の制限を設定するために使用します。監視対象デバイス上のイベント レートが [Events per second (Warning)] 制限で設定された 1 秒あたりのイベント数を超えると、そのモジュールのステータス分類が Warning に変更されます。監視対象デバイス上のイベント レートが [Events per second (Critical)] 制限で設定された 1 秒あたりのイベント数を超えると、そのモジュールのステータス分類が Critical に変更されます。このステータス データがヘルス モニタに反映されます。

一般に、ネットワーク セグメントのイベント レートは平均で 1 秒あたり 20 イベントです。この平均レートのネットワーク セグメントでは、[Events per second (Critical)] を 50 に設定し、[Events per second (Warning)] を 30 に設定する必要があります。システムの制限を決定するには、デバイスの [Statistics] ページ（[System] > [Monitoring] > [Statistics]）で [Events/Sec] 値を探してから、次の式を使用して制限を計算します。

- Events per second (Critical) = Events/Sec * 2.5
- Events per second (Warning) = Events/Sec * 1.5

両方の制限に設定可能な最大イベント数は 999 であり、重大制限は警告制限より大きくする必要があります。

侵入イベント レート モニタ ヘルス モジュールの設定を構成する方法：

アクセス：Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Intrusion Event Rate] を選択します。

[Health Policy Configuration — Intrusion Event Rate] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　[Events per second (Critical)] フィールドに、重大ヘルス ステータスをトリガーとして使用する 1 秒あたりのイベント数を入力します。

ステップ 4　[Events per second (Warning)] フィールドに、警告ヘルス ステータスをトリガーとして使用する 1 秒あたりのイベント数を入力します。

ステップ 5　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、「正常性ポリシーの適用」（P.55-32）を参照してください。

ライセンス モニタリングについて

ライセンス：任意

ライセンス モニタリング ヘルス ステータス モジュールは、Control、Protection、URL Filtering、Malware、および VPN の十分なライセンスが残っているかどうかを確認するために使用します。このモジュールは、残りのライセンスの数が少ないまたは不十分な場合にアラートを出します。

また、スタック設定内のデバイスのライセンス セットが一致しないことをシステムが検出した場合にもアラートを出します（スタックされたデバイスのライセンス セットは同じでなければなりません）。

ライセンス モニタリング モジュールは自動的に設定されます。このモジュールは変更または無効にすることができないため、[Health Policy Configuration] ページに表示されません。

リンクステート伝達モニタリングの設定

ライセンス：任意

リンクステート伝達ヘルス ステータス モジュールは、インライン ペア上のリンク ステートの伝達を検出するために使用します。リンクステートがペアに伝達した場合は、そのモジュールのステータス分類が Critical に変更され、状態が次のように表示されます。

```
Module Link State Propagation: ethx_ethy is Triggered
```

ここで、*x* と *y* はペア化されたインターフェイス番号です。

リンクステート伝達ヘルス モジュールの設定を構成する方法：

アクセス：Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Link State Propagation] を選択します。

[Health Policy Configuration — Link State Propagation monitor] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、「正常性ポリシーの適用」（P.55-32）を参照してください。

メモリ使用率モニタリングの設定

ライセンス：任意

メモリ使用率ヘルス ステータス モジュールは、メモリ使用率の制限を設定するために使用します。このモジュールは、空きメモリ、キャッシュされたメモリ、およびスワップ メモリを考慮して空きメモリを計算します。監視対象アプライアンスのメモリ使用率が警告制限を超えた場合は、そのモジュールのステータス分類が Warning に変更されます。監視対象アプライアンスのメモリ使用率が重大制限を超えた場合は、そのモジュールのステータス分類が Critical に変更されます。このステータス データがヘルス モニタに反映されます。

メモリが 4 GB を超えるアプライアンスの場合、プリセットされたアラートしきい値は、システム問題を引き起こす可能性のあるメモリ空き容量の割合を求める式に基づいています。

注　4 GB を超えるアプライアンスでは、警告しきい値と重大しきい値の時間間隔が非常に狭いため、シスコは、[Warning Threshold %] の値を手動で 50 に設定することを推奨します。これにより、時間内にアプライアンスのメモリ アラートを受け取って問題を解決できる可能性がさらに高まります。

両方の制限に設定可能な最大パーセンテージは 100% であり、重大制限は警告制限より高くする必要があります。

注　多数の FireSIGHT 機能（セキュリティ インテリジェンス、ファイル キャプチャ、複数のルールを使用した侵入ポリシー、URL フィルタリングなど）を有効にして、アクセス コントロール ポリシーを適用した場合、より安価な ASA FirePOWER デバイスによっては、メモリ割り当てを最大限拡張して使用したために、断続的なメモリ使用率警告が生成される可能性があります。

メモリ使用率ヘルス モジュールの設定を構成する方法：

アクセス：Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Memory Usage] を選択します。

[Health Policy Configuration — Memory Usage] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　[Critical Threshold %] フィールドに、重大ヘルス ステータスをトリガーとして使用するメモリ使用率のパーセンテージを入力します。

ステップ 4　[Warning Threshold %] フィールドに、警告ヘルス ステータスをトリガーとして使用するメモリ使用率のパーセンテージを入力します。

ステップ 5　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するアプライアンスに適用する必要があります。詳細については、「正常性ポリシーの適用」（P.55-32）を参照してください。

電源モニタリングの設定

ライセンス：任意

サポート対象デバイス：3D3500、3D4500、3D6500、3D9900、シリーズ 3

サポート対象防御センター：DC1500、DC3500

電源ヘルス ステータス モジュールは、サポートされているプラットフォームのいずれかで電源障害を検出するために使用します。モジュールが電力を消失した電源を検出すると、そのモジュールのステータス分類は No Power に変わります。モジュールが電源の存在を検出できない場合、ステータスは Critical Error に変わります。このステータス データがヘルス モニタに反映されます。ヘルス モニタの [Alert Detail] リストで [Power Supply] 項目を展開して、電源ごとの特定のステータス項目を表示できます。

電源ヘルス モジュールの設定を構成する方法：

アクセス：Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Power Supply] を選択します。

[Health Policy Configuration — Power Supply] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、「正常性ポリシーの適用」（P.55-32）を参照してください。

プロセス ステータス モニタリングの設定

ライセンス：任意

プロセス ステータス ヘルス モジュールは、プロセス マネージャの外部で停止または終了したアプライアンス上で実行中のプロセスを監視するために使用します。プロセス ステータス モジュールのプロセス終了に対する応答はプロセスの終了方法によって異なります。

- プロセスがマネージャ プロセスの内部で終了した場合、モジュールはヘルス イベントを報告しません。
- プロセスが故意にプロセス マネージャの外部で停止された場合は、モジュールが再開してプロセスが再起動するまで、モジュール ステータスが Warning に変更され、ヘルス イベント メッセージが停止されたプロセスを示します。
- プロセスがプロセス マネージャの外部で異常終了またはクラッシュした場合は、モジュールが再開してプロセスが再起動するまで、モジュール ステータスが Critical に変わり、ヘルス イベント メッセージが終了したプロセスを示します。

プロセス ステータス ヘルス モジュールの設定を構成する方法：

アクセス：Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Process Status] を選択します。

[Health Policy Configuration — Process Status] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するアプライアンスに適用する必要があります。詳細については、「正常性ポリシーの適用」（P.55-32）を参照してください。

RRD サーバ プロセス モニタリングの設定

ライセンス：任意

RRD サーバ プロセス モジュールは、時系列データを保存する RRD サーバが正常に動作しているかどうかを確認するために使用します。このモジュールは、RRD サーバが前回の更新以降に再起動した場合にアラートを出します。また、RRD サーバの再起動を伴う連続更新回数がモジュール設定で指定された数値に達した場合に Critical または Warning ステータスに遷移します。

RRD サーバ プロセス モニタリングの設定を構成する方法：

アクセス：Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[RRD Server Process] を選択します。

[Health Policy Configuration — RRD Server Process] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　[Critical Number of restarts] フィールドに、重大ヘルス ステータスをトリガーとして使用する連続検出される RRD サーバ リセットの回数を入力します。

ステップ 4　[Warning Number of restarts] フィールドに、警告ヘルス ステータスをトリガーとして使用する連続検出される RRD サーバ リセットの回数を入力します。

ステップ 5　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、「正常性ポリシーの適用」（P.55-32）を参照してください。

セキュリティ インテリジェンス モニタリングの設定

ライセンス：Protection

サポート対象防御センター：任意（DC500 を除く）

セキュリティ インテリジェンス モジュールは、セキュリティ インテリジェンス フィルタリングを伴うさまざまな状況で警告するために使用します。このモジュールは、セキュリティ インテリジェンスが使用中で次の場合にアラートを出します。

- 防御センターがフィードを更新できないか、フィード データが破損している、または認識可能な IP アドレスが含まれていない
- 管理対象デバイスが防御センターから更新されたセキュリティ インテリジェンス データを受信できない
- 管理対象デバイスが、メモリ問題のために、防御センターから提供されたすべてのセキュリティ インテリジェンス データをロードできない

ヒント　セキュリティ インテリジェンス メモリ警告がヘルス モニタに表示された場合は、影響を受けるデバイスのアクセス コントロール ポリシーを再適用して、セキュリティ インテリジェンスに割り当てるメモリを増やすことができます。詳細については、「アクセス コントロール ポリシーの適用」（P.13-39）を参照してください。

セキュリティ インテリジェンス フィルタリングの詳細については、「セキュリティ インテリジェンス データに基づくトラフィックのフィルタリング」（P.13-13）と「セキュリティ インテリジェンス リストとフィードの操作」（P.5-4）を参照してください。

セキュリティ インテリジェンス モジュールの設定を構成する方法：

アクセス：Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Security Intelligence] を選択します。

[Health Policy Configuration — Security Intelligence] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、セキュリティ インテリジェンス モニタリングに対するモジュールの使用を有効にします。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、「正常性ポリシーの適用」（P.55-32）を参照してください。

時系列データ モニタリングの設定

ライセンス：任意

時系列データ モニタ モジュールは、システムが保存した時系列データ（コンプライアンス イベントのリストなど）のステータスを監視するために使用します。このモジュールは、時系列データ ストレージ ディレクトリで破損ファイルをスキャンします。モジュールが破損したデータを検出すると、Warning ステータスに遷移し、影響を受けるすべてのファイルの名前を報告します。

時系列データ モニタリングの設定を構成する方法：

アクセス：Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Time Series Data Monitor] を選択します。

[Health Policy Configuration — Time Series Data Monitor] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、「正常性ポリシーの適用」（P.55-32）を参照してください。

時刻同期モニタリングの設定

ライセンス：任意

時刻同期ステータス モジュールは、NTP を使用して NTP サーバから時刻を取得する管理対象デバイス上の時刻がサーバ上の時刻と 10 秒以上異なる時点を検出するために使用します。

時刻同期モニタリングの設定を構成する方法：

アクセス：Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Time Synchronization Status] を選択します。

[Health Policy Configuration — Time Synchronization Status] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、「正常性ポリシーの適用」（P.55-32）を参照してください。

トラフィック ステータス モニタリングの設定

FireSIGHT

トラフィック ステータス ヘルス ステータス モジュールは、デバイスがトラフィックを受信しているかどうかを検出するために使用します。トラフィック ステータス モジュールは、デバイスがトラフィックを受信していないことを確認すると、そのモジュールのステータス分類が Critical に変わります。このステータス データがヘルス モニタに反映されます。

注　`DataPlaneInterfacex` というラベルの付いたインターフェイス（ここで、`x` は数値）は、内部 ASA インターフェイス（ユーザ定義ではない）で、システム内部のパケット フローに関与します。

トラフィック ステータス ヘルス モジュールの設定を構成する方法：

アクセス：Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[Traffic Status] を選択します。

[Health Policy Configuration — Traffic Status] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、「正常性ポリシーの適用」（P.55-32）を参照してください。

URL フィルタリングモニタリングの設定

ライセンス：URL Filtering

サポート対象防御センター：任意（DC500 を除く）

URL フィルタリング モニタ モジュールは、防御センター と シスコ クラウド間の通信を追跡するために使用します。システムは、頻繁に訪問される URL に関する URL フィルタリング（カテゴリとレピュテーション）データを取得します。防御センターがクラウドと正常に通信できない、または、クラウドから更新を取得できない場合、そのモジュールのステータス分類は Critical に変わります。

ハイ アベイラビリティ設定では、プライマリ防御センターだけが URL フィルタリング クラウドと通信します。このモジュールからのすべてのデータはそのプライマリ アプライアンスのみを参照します。

URL フィルタリング モニタ モジュールは、防御センターと URL フィルタリングが有効になっている管理対象デバイス間の通信も追跡します。防御センターがクラウドと正常に通信している状態で、防御センターが新しい URL フィルタリング データをその管理対象デバイスにプッシュできない場合、モジュール ステータスは Warning に変わります。

URL フィルタリング モニタ ヘルス モジュールの設定を構成する方法：

アクセス：Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[URL Filtering Monitor] を選択します。

[Health Policy Configuration — URL Filtering Monitor] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを防御センターに適用する必要があります。詳細については、「正常性ポリシーの適用」（P.55-32）を参照してください。

ユーザ エージェント ステータス モニタリングの設定

ライセンス：FireSIGHT

ユーザ エージェント ステータス モニタ ヘルス モジュールは、防御センターに接続されているエージェントのハートビートを監視するために使用できます。適用した正常性ポリシー内のモジュールを有効にすると、防御センターが防御センター上で設定されているエージェントのハートビートを検出しない場合に、モジュールはヘルス アラートを生成します。

防御センターへの報告に従来のユーザ エージェントを使用している場合、このヘルス モジュールは、エージェントがハートビートを発行していないというアラートを出します。

ユーザ エージェント ステータス モニタ ヘルス モジュールの設定を構成する方法：

アクセス：Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[User Agent Status Monitor] を選択します。

[Health Policy Configuration — User Agent Status Monitor] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを防御センターに適用する必要があります。詳細については、「正常性ポリシーの適用」（P.55-32）を参照してください。

VPN ステータス モニタリングの設定

ライセンス：VPN

サポート対象防御センター：任意 （シリーズ 2 以外）

VPN ステータス ヘルス モジュールは、設定したゲートウェイ VPN トンネルの現在のステータスを監視するために使用します。個別のトンネルに関する情報が表示されます。このモジュールは、VPN トンネルのいずれかが動作していないときに、重大（赤色）ヘルス アラートを生成します。

VPN ステータス ヘルス モジュールの設定を構成する方法：

アクセス：Admin/Maint

ステップ 1　[Health Policy Configuration] ページで、[VPN Status] をクリックします。

[Health Policy Configuration — VPN Status] ページが表示されます。

ステップ 2　[Enabled] オプションに対して [On] を選択して、ヘルス ステータス テストに対するモジュールの使用を有効にします。

ステップ 3　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。

- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

設定を有効にするには、正常性ポリシーを該当するデバイスに適用する必要があります。詳細については、「正常性ポリシーの適用」（P.55-32）を参照してください。

正常性ポリシーの適用

ライセンス：任意

正常性ポリシーをアプライアンスに適用すると、ポリシー内で有効にしたすべてのモジュールのヘルス テストが、アプライアンス上のプロセスとハードウェアの正常性を自動的に監視します。その後、ヘルス テストは、ポリシー内で設定された時間間隔で実行を続け、アプライアンスのヘルス データを収集し、そのデータを防御センターに転送します。

正常性ポリシーでモジュールを有効にしてから、ヘルス テストが必要ないアプライアンスにポリシーを適用した場合、ヘルス モニタはそのヘルス モジュールのステータスを無効として報告します。

すべてのモジュールが無効になっているポリシーをアプライアンスに適用すると、適用されたすべての正常性ポリシーがアプライアンスから削除されるため、どの正常性ポリシーも適用されません。

すでにポリシーが適用されているアプライアンスに別のポリシーを適用した場合は、新しく適用されたテストに基づく新しいデータの表示が少し遅れる可能性があります。

注　ハイ アベイラビリティ ペア内の防御センター上で作成されたカスタム 正常性ポリシーは両方のアプライアンス間で複製されます。ただし、デフォルト正常性ポリシーに対する変更は複製されません。各アプライアンスは、それ用に設定されたローカルのデフォルト正常性ポリシーを使用します。

正常性ポリシーを適用する方法：

アクセス：Admin/Maint

ステップ 1　[Health] > [Health Policy] の順に選択します。

[Health Policy] ページが表示されます。

ステップ 2　適用するポリシーの横にある適用アイコン（  ）をクリックします。

[Health Policy Apply] ページが表示されます。

ヒント　[Health Policy] 列の横にあるステータス アイコン（  ）は、アプライアンスの現在のヘルス ステータスを示します。[System Policy] 列の横にあるステータス アイコン（  ）は、防御センターとデバイス間の通信ステータスを示します。削除アイコン（  ）をクリックすることによって、現在適用されているポリシーを削除できることに注意してください。

ステップ 3　正常性ポリシーを適用するアプライアンスを選択します。

ステップ 4　[Apply] をクリックして、選択したアプライアンスにポリシーを適用します。

[Health Policy] ページが開いて、ポリシーの適用が成功したかどうかを示すメッセージが表示されます。アプライアンスのモニタリングは、ポリシーが正常に適用された直後に開始されます。

正常性ポリシーの編集

ライセンス：任意

モジュールを有効または無効にするか、モジュール設定を変更することによって、正常性ポリシーを変更できます。すでにアプライアンスに適用されているポリシーを変更すると、その変更はポリシーを再適用するまで有効になりません。

さまざまなアプライアンスに適用可能なヘルス モデルを次の表に列挙します。

表 55-3　　アプライアンスに適用可能なヘルス モジュール

モジュール	適用可能なアプライアンス
高度なマルウェア対策	防御センター、DC500 以外
アプライアンス ハートビート	防御センター
自動アプリケーション バイパス ステータス	すべての管理対象デバイス
CPU 使用率	任意（3D9900 は除く）
カード リセット	すべての管理対象デバイス
ディスカバリ イベント ステータス	防御センター
ディスク ステータス	任意
ディスク使用率	任意
FireAMP ステータス モニタ	防御センター
FireSIGHT ホスト ライセンス制限	防御センター
ハードウェア アラーム	シリーズ 3、3D9900
ヘルス モニタ プロセス	防御センター
インライン リンク不一致アラーム	すべての管理対象デバイス
侵入イベント レート	Protection 付きの管理対象デバイス
ライセンス モニタ	防御センター
リンクステート伝達	Protection 付きの管理対象デバイス
メモリ使用率	任意
電源	防御センター：DC1500、DC3500 デバイス：3D3500、3D4500、3D6500、3D9900、シリーズ 3
プロセス ステータス	任意
RRD サーバ プロセス	防御センター
セキュリティ インテリジェンス	防御センター、DC500 以外
時系列データ モニタ	防御センター

表 55-3　アプライアンスに適用可能なヘルス モジュール（続き）

モジュール	適用可能なアプライアンス
時刻同期ステータス	任意
トラフィック ステータス	すべての管理対象デバイス
URL フィルタリング モニタ	防御センター、DC500 以外
ユーザ エージェント ステータス モニタ	防御センター
VPN ステータス	防御センター

正常性ポリシーを編集する方法：

アクセス：Admin/Maint

ステップ 1　[Health] > [Health Policy] の順に選択します。

[Health Policy] ページが表示されます。

ステップ 2　変更するポリシーの横にある編集アイコン（  ）をクリックします。

[Policy Run Time Interval] 設定が選択された状態で [Health Policy Configuration] ページが表示されます。

ステップ 3　必要に応じて、次の項の説明に従って、設定を変更します。

- 「ポリシー実行時間間隔の設定」（P.55-11）
- 「高度なマルウェア対策モニタリングの設定」（P.55-11）
- 「アプライアンス ハートビート モニタリングの設定」（P.55-12）
- 「自動アプリケーション バイパス モニタリングの設定」（P.55-13）
- 「CPU 使用率モニタリングの設定」（P.55-13）
- 「カード リセット モニタリングの設定」（P.55-14）
- 「ディスカバリ イベント ステータス モニタリングの設定」（P.55-15）
- 「ディスク ステータス モニタリングの設定」（P.55-16）
- 「ディスク使用率モニタリングの設定」（P.55-16）
- 「ステータス モニタリングFireAMPの設定」（P.55-17）
- 「FireSIGHT ホスト使用量モニタリングの設定」（P.55-18）
- 「ハードウェア アラーム モニタリングの設定」（P.55-19）
- 「ヘルス ステータス モニタリングの設定」（P.55-20）
- 「インライン リンク不一致アラーム モニタリングの設定」（P.55-21）
- 「侵入イベント レート モニタリングの設定」（P.55-21）
- 「ライセンス モニタリングについて」（P.55-22）
- 「リンクステート伝達モニタリングの設定」（P.55-22）
- 「メモリ使用率モニタリングの設定」（P.55-23）
- 「電源モニタリングの設定」（P.55-24）
- 「プロセス ステータス モニタリングの設定」（P.55-25）
- 「RRD サーバ プロセス モニタリングの設定」（P.55-26）

- 「セキュリティ インテリジェンス モニタリングの設定」（P.55-27）
- 「時系列データ モニタリングの設定」（P.55-28）
- 「時刻同期モニタリングの設定」（P.55-28）
- 「トラフィック ステータス モニタリングの設定」（P.55-29）
- 「URL フィルタリングモニタリングの設定」（P.55-30）
- 「ユーザ エージェント ステータス モニタリングの設定」（P.55-30）
- 「VPN ステータス モニタリングの設定」（P.55-31）

ステップ 4　次の 3 つのオプションがあります。

- このモジュールに対する変更を保存して、[Health Policy] ページに戻るには、[Save Policy and Exit] をクリックします。
- このモジュールの設定を保存せずに、[Health Policy] ページに戻るには、[Cancel] をクリックします。
- このモジュールに対する変更を一時的に保存して、変更する他のモジュールの設定に切り替えるには、ページの左側にあるリストから他のモジュールを選択します。設定が終わって [Save Policy and Exit] をクリックすると、加えたすべての変更が保存されます。[Cancel] をクリックすると、すべての変更が破棄されます。

ステップ 5　「正常性ポリシーの適用」（P.55-32）の説明に従って、該当するアプライアンスにポリシーを再適用します。

正常性ポリシーの比較

ライセンス：任意

ポリシーの変更が組織の標準に準拠していることを確認する、または、ヘルス モニタリングのパフォーマンスを最適化するため、2 つの正常性ポリシー間の違いを調査することができます。アクセス可能な正常性ポリシーの場合、2 つの正常性ポリシーまたは同じ正常性ポリシーの 2 つのリビジョンを比較できます。アクティブな正常性ポリシーを他の正常性ポリシーとすばやく比較するには、[Running Configuration] オプションを選択できます。オプションで、比較後に、2 つのポリシーまたはポリシー リビジョン間の違いを記録した PDF レポートを生成できます。

正常性ポリシーまたは正常性ポリシー リビジョンを比較するための 2 つのツールが用意されています。

- 比較ビューには、2 つ正常性ポリシーまたは正常性ポリシー リビジョン間の違いだけが並べて表示されます。各ポリシーまたはポリシー リビジョンの名前が比較ビューの左右のタイトル バーに表示されます。

  これを使用して、Web インターフェイスで相違点を強調表示したまま、両方のポリシーのリビジョンを表示し移動することができます。

- 比較レポートは、正常性ポリシー レポートに類似した PDF 形式で 2 つの正常性ポリシーまたは正常性ポリシー リビジョン間の違いのみのレコードを作成します。

  これは、ポリシー比較を保存、コピー、印刷、および共有して詳しく調査するために使用できます。

正常性ポリシー比較ツールの知識と使い方の詳細については、以下を参照してください。

- 「正常性ポリシー比較ビューの使用」（P.55-36）
- 「正常性ポリシー比較レポートの使用」（P.55-36）

正常性ポリシー比較ビューの使用

ライセンス：任意

比較ビューには、両方の正常性ポリシーまたはポリシー リビジョンが並べて表示されます。それぞれのポリシーまたはポリシー リビジョンは、比較ビューの左右のタイトル バーに表示された名前で識別されます。最終変更時刻と最終変更ユーザがポリシー名の右側に表示されます。[Health Policy] ページにはポリシーが最後に変更された時刻が現地時間で表示されますが、正常性ポリシー レポートでは変更時刻が UTC で表示されることに注意してください。

2 つの正常性ポリシーまたはポリシー リビジョン間の違いが強調表示されます。

- 青色は強調表示された設定が 2 つのポリシーまたはポリシー リビジョンで違うことを意味します。違いは赤色のテキストで表示されます。
- 緑色は強調表示された設定が一方のポリシーまたはポリシー リビジョンだけにあるが、他方にないことを意味します。

次の表に、実行できる操作を記載します。

表 55-4　正常性ポリシー比較ビューの操作

目的	操作
変更を 1 つずつ移動する	タイトル バーの上にある [Previous] または [Next] をクリックします。 左側と右側の中間にある二重矢印アイコン（）が移動し、[Difference] 番号が表示する違いを反映して更新されます。
新しい正常性ポリシー比較ビューを生成する	[New Comparison] をクリックします。 [Select Comparison] ウィンドウが表示されます。詳細については、正常性ポリシー比較レポートの使用を参照してください。
正常性ポリシー比較レポートを生成する	[Comparison Report] をクリックします。 正常性ポリシー比較レポートは比較ビューと同じ情報を含む PDF を作成します。

正常性ポリシー比較レポートの使用

ライセンス：任意

正常性ポリシー比較レポートは、正常性ポリシー比較ビューで特定された 2 つ正常性ポリシー間または同じ正常性ポリシーの 2 つのリビジョン間のすべての違いの記録を、PDF として提供するものです。このレポートは、2 つの正常性ポリシー設定間の違いをさらに調査し、その結果を保存して共有するために使用できます。

正常性ポリシー比較レポートは、アクセス可能な任意の正常性ポリシーの比較ビューから生成できます。正常性ポリシー レポートを生成する前に、未確定の変更をコミットするのを忘れないでください。コミットされた変更だけがレポートに表示されます。

設定に応じて、正常性ポリシー比較レポートに 1 つ以上のセクションを含めることができます。次のサンプル グラフィックは、正常性ポリシー比較レポートの [Policy Information] セクションと [Modules] セクションを示しており、両方の正常性ポリシー設定のルールごとの設定がリストされています。それぞれのセクションで、同じ形式が使用され、同じレベルの詳細が提供されます。[Value A] 列と [Value B] 列は、比較ビューで設定されたポリシーまたはポリシー リビジョンを表していることに注意してください。

FireSIGHT システム上で同様の手順を使用して他のポリシー タイプを比較します。詳細については、以下を参照してください。

- 「2 つのアクセス コントロール ポリシーの比較」（P.13-37）
- 「2 つの侵入ポリシーの比較」（P.20-13）
- 「システム ポリシーの比較」（P.50-5）

2 つの正常性ポリシーまたは同じポリシーの 2 つのリビジョンを比較する方法：

アクセス：Admin/Maint

ステップ 1　[Health] > [Health Policy] の順に選択します。

[Health Policy] ページが表示されます。

ステップ 2　[Compare Policies] をクリックします。

[Select Comparison] ウィンドウが表示されます。

ステップ 3　[Compare Against] ドロップダウン リストから、比較するタイプを次のように選択します。

- 異なる 2 つのポリシーを比較するには、[Other Policy] を選択します。
- 同じポリシーの 2 つのリビジョンを比較するには、[Other Revision] を選択します。
- 現在のアクティブ ポリシーを他のポリシーに対して比較するには、[Running Configuration] を選択します。

正常性ポリシー レポートを生成する前に、変更をコミットするのを忘れないでください。コミットされた変更だけがレポートに表示されます。

ステップ 4　選択した比較タイプに応じて、次のような選択肢があります。

- 2 つの別々のポリシーを比較する場合は、[Policy A] ドロップダウン リストと [Policy B] ドロップダウン リストから比較するポリシーを選択します。
- 同じポリシーの 2 つのリビジョンを比較する場合は、[Policy] ドロップダウン リストからポリシーを選択してから、[Revision A] ドロップダウン リストと [Revision B] ドロップダウン リストから比較するリビジョンを選択します。
- 実行中の設定を他のポリシーと比較する場合は、[Policy B] ドロップダウン リストから 2 つ目のポリシーを選択します。

ステップ 5　正常性ポリシー比較ビューを表示するには、[OK] をクリックします。

比較ビューが表示されます。

ステップ 6　正常性ポリシー比較レポートを生成するには、[Comparison Report] をクリックします。

正常性ポリシー レポートが表示されます。ブラウザの設定に応じて、レポートがポップアップ ウィンドウに表示される場合とレポートをコンピュータに保存するようプロンプトが表示される場合があります。

正常性ポリシーの削除

ライセンス：任意

不要になった正常性ポリシーを削除できます。アプライアンスに適用されているポリシーを削除した場合は、別のポリシーを適用するまでそのポリシー設定が有効のままになります。加えて、デバイスに適用されている正常性ポリシーを削除した場合、元となる関連アラート応答を無効にするまでは、そのデバイスに対して有効になっているヘルス モニタリング アラートがアクティブなままになります。「アラート応答の有効化と無効化」（P.15-8）を参照してください。

ヒント　アプライアンスのヘルス モニタリングを停止するには、すべてのモジュールが無効になっている正常性ポリシーを作成し、それをアプライアンスに適用します。正常性ポリシーの作成方法については、「正常性ポリシーの作成」（P.55-9）を参照してください。正常性ポリシーの適用方法については、「正常性ポリシーの適用」（P.55-32）を参照してください。

正常性ポリシーを削除する方法：

アクセス：Admin/Maint

ステップ 1　[Health] > [Health Policy] の順に選択します。

[Health Policy] ページが表示されます。

ステップ 2　削除するポリシーの横にある削除アイコン（ ）をクリックします。

削除が成功したかどうかを示すメッセージが表示されます。

ヘルス モニタ ブラックリストの使用

ライセンス：任意

通常のネットワーク メンテナンスの一環として、アプライアンスを無効にしたり、一時的に使用不能にしたりすることがあります。このような機能停止は意図したものであり、アプライアンスからのヘルス ステータスに 防御センター 上のサマリー ヘルス ステータスを反映させる必要がありません。

ヘルス モニタ ブラックリスト機能を使用して、アプライアンスまたはモジュールに関するヘルス モニタリング ステータス レポートを無効にすることができます。たとえば、ネットワークのあるセグメントが使用できなくなることがわかっている場合は、そのセグメント上の管理対象デバイスのヘルス モニタリングを一時的に無効にして、防御センター上のヘルス ステータスにデバイスへの接続がダウンしたことによる警告状態または重大状態が表示されないようにできます。

ヘルス モニタリング ステータスを無効にしても、ヘルス イベントは生成されますが、そのステータスが無効になっているため、ヘルス モニタのヘルス ステータスには影響しません。ブラックリストからアプライアンスまたはモジュールを削除しても、ブラックリストに登録中に生成されたイベントのステータスは Disabled のままです。

アプライアンスからのヘルス イベントを一時的に無効にするには、ブラックリスト設定ページに移動して、アプライアンスをブラックリストに追加します。設定が有効になると、システムは全体のヘルス ステータスを計算するときにブラックリストに登録されているアプライアンスを含めません。[Health Monitor Appliance Status Summary] にはこのアプライアンスが Disabled としてリストされます。

アプライアンス上の個別のヘルス モニタリング モジュールをブラックリストに登録する方が実用的な場合があります。たとえば、アプライアンス上の FireSIGHT ホスト ライセンスを使い果たした場合は、FireSIGHT ホスト ライセンス制限ステータス メッセージをブラックリストに登録できます。

メインの [Health Monitor] ページで、ステータス行内の矢印をクリックして特定のステータスを持つアプライアンスのリストを展開表示すれば、ブラックリストに登録されたアプライアンスを区別できることに注意してください。このビューの展開方法については、「ヘルス モニタの使用」（P.55-44）を参照してください。

ブラックリストに登録されたアプライアンスまたは部分的にブラックリストに登録されたアプライアンスのビューを展開すると、ブラックリスト アイコン（ ）と注記が表示されます。

注　防御センターでは、ヘルス モニタのブラックリスト設定はローカル コンフィギュレーション設定です。そのため、防御センター上でデバイスをブラックリストに登録してから削除しても、後で再登録すれば、ブラックリスト設定は元どおりになります。新たに再登録したデバイスはブラックリストに登録されたままです。

詳細については、以下を参照してください。

- 「正常性ポリシーまたはアプライアンスのブラックリストへの登録」（P.55-39）
- 「個別のアプライアンスのブラックリストへの登録」（P.55-40）
- 「個別の正常性ポリシー モジュールのブラックリストへの登録」（P.55-41）

正常性ポリシーまたはアプライアンスのブラックリストへの登録

ライセンス：任意

特定の正常性ポリシーが適用されたすべてのアプライアンスに対するヘルス イベントを無効に設定する場合、そのポリシーをブラックリストに登録できます。アプライアンス グループのヘルス モニタリングの結果を無効にする必要がある場合、そのアプライアンス グループをブラックリストに登録できます。ブラックリスト設定が有効になると、[Health Monitor Appliance Module Summary] と [Device Management] ページでアプライアンスが Disabled として表示されます。アプライアンスのヘルス イベントのステータスは Disabled です。

防御センターがハイ アベイラビリティ設定の場合は、一方のハイ アベイラビリティ ピア上の管理対象デバイスだけをブラックリストに登録できることに注意してください。ハイ アベイラビリティ ピアをブラックリストに登録することによって、それが生成したイベントとそれがヘルス イベントを受け取ったデバイスを Disabled としてマークすることもできます。ハイ アベイラビリティ ペア内の 防御センターには、ピアを完全にまたは部分的にブラックリストに登録するためのオプションがあります。

正常性ポリシー全体またはアプライアンスのグループをブラックリストに登録する方法：

アクセス：Admin/Maint

ステップ 1　[Health] > [Blacklist] の順に選択します。

[Blacklist] ページが表示されます。

ステップ 2　右側にあるドロップダウン リストを使用して、リストをグループ、ポリシー、またはモデルでソートします （防御センター上のグループは管理対象デバイスです。）。

全部ではなく一部のヘルス モジュールがブラックリストに登録されたアプライアンスは [(Partially Blacklisted)] として表示されることに注意してください。メインのブラックリスト ページでブラックリスト ステータスを編集する場合、アプライアンス上のすべてのモジュールをブラックリストに登録するか、すべてのブラックリスト登録を削除するかのいずれかを行えます。アプライアンス上の個別のヘルス モジュールをブラックリストに登録する方法については、「個別の正常性ポリシー モジュールのブラックリストへの登録」（P.55-41）を参照してください。

ヒント　[Health Policy] 列の横にあるステータス アイコン（）は、アプライアンスの現在のヘルス ステータスを示します。[System Policy] 列の横にあるステータス アイコン（）は、防御センターとデバイス間の通信ステータスを示します。

ステップ 3　次の 2 つのオプションから選択できます。

- グループ、モデル、またはポリシー カテゴリ内のすべてのアプライアンスをブラックリストに登録するには、カテゴリを選択してから、[Blacklist Selected Devices] をクリックします。
- グループ、モデル、またはポリシー カテゴリ内のすべてのアプライアンスからブラックリスト登録を消去するには、カテゴリを選択してから、[Clear Blacklist on Selected Devices] をクリックします。

ページが更新して、アプライアンスの新しいブラックリスト状態が表示されます。

個別のアプライアンスのブラックリストへの登録

ライセンス：任意

個別のアプライアンスのイベントとヘルス ステータスを Disabled に設定する必要がある場合、アプライアンスをブラックリストに登録できます。ブラックリスト設定が有効になると、アプライアンスが [Health Monitor Appliance Module Summary] に Disabled として表示され、アプライアンスのヘルス イベントのステータスが Disabled になります。

個別のアプライアンスをブラックリストに登録する方法：

アクセス：Admin/Maint

ステップ 1　[Health] > [Blacklist] の順に選択します。

[Blacklist] ページが表示されます。

ステップ 2　アプライアンス グループ、モデル、またはポリシーでリストをソートするには、右側にあるドロップダウン リストを使用します

ステップ 3　次の 2 つのオプションから選択できます。

- グループ、モデル、またはポリシー カテゴリ内のすべてのアプライアンスをブラックリストに登録するには、カテゴリを選択してから、[Blacklist Selected Devices] をクリックします。
- グループ、モデル、またはポリシー カテゴリ内のすべてのアプライアンスからブラックリスト登録を消去するには、カテゴリを選択してから、[Clear Blacklist on Selected Devices] をクリックします。

ページが更新されて、アプライアンスの新しいブラックリスト状態が表示されます。個別の正常性ポリシー モジュールをブラックリストに登録するには、[Edit] をクリックして、「個別の正常性ポリシー モジュールのブラックリストへの登録」（P.55-41）を参照してください。

個別の正常性ポリシー モジュールのブラックリストへの登録

ライセンス：任意

アプライアンス上の個別の正常性ポリシー モジュールをブラックリストに登録できます。この操作により、モジュールからのイベントによってアプライアンスのステータスが Warning または Critical に変更されないようにすることができます。

モジュールの一部がブラックリストに登録されている場合、そのモジュールの行は 防御センター Web インターフェイスにボールド体で表示されます。

ヒント　ブラックリスト設定が有効になると、アプライアンスが [Blacklist] ページと [Appliance Health Monitor Module Status Summary] で [Partially Blacklisted] または [All Modules Blacklisted] として表示されますが、メインの [Appliance Status Summary] ページでは展開されたビューにだけ表示されます。個別にブラックリストに登録したモジュールを追跡して、必要に応じてそれらを再アクティブ化できるようにしてください。誤ってモジュールを無効にすると、必要な警告または重大メッセージを見逃す可能性があります。

個別の正常性ポリシー モジュールをブラックリストに登録する方法：

アクセス：Admin/Maint

ステップ 1　[Health] > [Blacklist] の順に選択します。

[Blacklist] ページが表示されます。

ステップ 2　グループ、ポリシー、またはモデルでソートしてから、[Edit] をクリックして、アプライアンスの正常性ポリシー モジュールのリストを表示します。

正常性ポリシー モジュールが表示されます。

ステップ 3　ブラックリストに登録するモジュールを選択します。

ステップ 4　**[Save]** をクリックします。

ヘルス モニタ アラートの設定

ライセンス：任意

正常性ポリシー内のモジュールのステータスが変更された場合に電子メール、SNMP、またはシステム ログ経由で通知するアラートをセットアップできます。特定のレベルのヘルス イベントが発生したときにトリガーとして使用して警告するヘルス イベント レベルと既存のアラート応答を関連付けることができます。

たとえば、アプライアンスがハード ディスク スペースを使い果たす可能性を懸念している場合は、残りのディスク スペースが警告レベルに達したときに自動的に電子メールをシステム管理者に送信できます。ハード ドライブがさらにいっぱいになる場合、ハード ドライブが重大レベルに達したときに 2 つ目の電子メールを送信できます。

詳細については、次のトピックを参照してください。

- 「ヘルス モニタ アラートの作成」（P.55-42）
- 「ヘルス モニタ アラートの解釈」（P.55-43）
- 「ヘルス モニタ アラートの編集」（P.55-43）
- 「ヘルス モニタ アラートの削除」（P.55-44）

ヘルス モニタ アラートの作成

ライセンス：任意

ヘルス モニタ アラートを作成するときに、重大度レベル、ヘルス モジュール、およびアラート応答の関連付けを作成します。既存のアラートを使用することも、新しいアラートをシステム ヘルスの報告専用に設定することもできます。選択したモジュールが重大度レベルに達すると、アラートがトリガーされます。

既存のしきい値と重複するようにしきい値を作成または更新すると、競合が通知されることに注意してください。重複したしきい値が存在する場合、ヘルス モニタは最も少ないアラートを生成するしきい値を使用し、その他のしきい値を無視します。しきい値のタイムアウト値は、5 ～ 4,294,967,295 分の間にする必要があります。

ヘルス モニタ アラートを作成する方法：

アクセス：Admin

ステップ 1　[Health] > [Health Monitor Alerts] の順に選択します。

[Health Monitor Alerts] ページが表示されます。

ステップ 2　[Health Alert Name] フィールドに、ヘルス アラートの名前を入力します。

ステップ 3　[Severity] リストから、アラートをトリガーとして使用する重大度レベルを選択します。

ステップ 4　[Module] リストから、アラートを適用するモジュールを選択します。

ヒント　複数のモジュールを選択するには、Ctrl + Shift キーを押しながら、モジュール名をクリックします。

ステップ 5　[Alert] リストから、選択した重大度レベルに達したときにトリガーとして使用するアラート応答を選択します。

ヒント　[Alerts] をクリックして、[Alerts] ページを開きます。アラートの作成方法については、「アラート応答の使用」（P.15-2）を参照してください。

ステップ 6　オプションで、[Threshold Timeout] フィールドに、それぞれのしきい値期間が終了してしきい値がリセットされるまでの分数を入力します。デフォルト値は 5 分です。

ポリシー実行時間間隔値がしきい値タイムアウト値より小さい場合でも、特定のモジュールから報告される 2 つのステータス イベントの時間間隔の方が常に大きくなります。しきい値タイムアウトが 8 分で、ポリシー実行時間間隔が 5 分の場合、報告されるイベントの時間間隔は 10（5 x 2）分です。

ステップ 7　[Save] をクリックして、ヘルス アラートを保存します。

アラート設定が正常に保存されたかどうかを示すメッセージが表示されます。これで、[Active Health Alerts] リストに作成したアラートが表示されます。

ヘルス モニタ アラートの解釈

ライセンス：任意

ヘルス モニタによって生成されるアラートには次の情報が含まれます。

- アラートの重大度レベルを示す Severity。
- テスト結果がアラートをトリガーとして使用したヘルス モジュールを示す Module。
- アラートをトリガーとして使用したヘルス テスト結果を含む Description。

ヘルス アラートの重大度レベルの詳細については、次の表を参照してください。

表 55-5　　アラートの重大度

重大度	説明
Critical	ヘルス テスト結果が Critical アラート ステータスをトリガーとして使用する基準を満たしました。
Warning	ヘルス テスト結果が Warning アラート ステータスをトリガーとして使用する基準を満たしました。
Normal	ヘルス テスト結果が Normal アラート ステータスをトリガーとして使用する基準を満たしました。
Error	ヘルス テストが実行されませんでした。
Recovered	ヘルス テスト結果が Critical または Warning アラート ステータスから Normal アラート ステータスに戻るための基準を満たしました。

ヘルス モジュールの詳細については、「ヘルス モジュールについて」（P.55-3）を参照してください。

ヘルス モニタ アラートの編集

ライセンス：任意

既存のヘルス モニタ アラートを編集して、ヘルス モニタ アラートに関連付けられた重大度レベル、ヘルス モジュール、またはアラート応答を変更できます。

ヘルス モニタ アラートを編集する方法：

アクセス：Admin

ステップ 1　[Health] > [Health Monitor Alerts] の順に選択します。

[Health Monitor Alerts] ページが表示されます。

ステップ 2　[Active Health Alerts] リストで、変更するアラートを選択します。

ステップ 3　[Load] をクリックして、選択したアラートの構成済みの設定をロードします。

ステップ 4　必要に応じて設定を変更します。詳細については、「ヘルス モニタ アラートの作成」（P.55-42）を参照してください。

ステップ 5　[Save] をクリックして、変更したヘルス アラートを保存します。

アラート設定が正常に保存されたかどうかを示すメッセージが表示されます。

ヘルス モニタ アラートの削除

ライセンス：任意

既存のヘルス モニタ アラートを削除できます。

注　ヘルス モニタ アラートを削除しても、関連するアラート応答は削除されません。アラートが継続しないようにするには、元になるアラート応答を無効にするまたは削除する必要があります。詳細については、「アラート応答の有効化と無効化」（P.15-8）および「アラート応答の削除」（P.15-8）を参照してください。

ヘルス モニタ アラートを削除する方法：

アクセス：Admin

ステップ 1　[Health] > [Health Monitor Alerts] の順に選択します。

[Health Monitor Alerts] ページが表示されます。

ステップ 2　[Active Health Alerts] リストで、削除するアラートを選択します。

ステップ 3　[Delete] をクリックします。

アラート設定が正常に削除されたかどうかを示すメッセージが表示されます。

ヘルス モニタの使用

ライセンス：任意

[Health Monitor] ページには、防御センターによって管理されているすべてのデバイスに加えて、防御センターに関して収集されたヘルス ステータスが表示されます。[Status] テーブルには、この防御センターの管理対象アプライアンスの台数が全体のヘルス ステータス別に表示されます。円グラフは、各ヘルス ステータス カテゴリに含まれているアプライアンスのパーセンテージを示すヘルス ステータス内訳の別のビューを提供します。

ヘルス モニタを使用する方法：

アクセス：Admin/Maint/Any Security Analyst

ステップ 1　[Health] > [Health Monitor] の順にクリックします。

[Health Monitor] ページが表示されます。

ステップ 2　テーブルの [Status] 列内の該当するステータスまたは円グラフの該当する部分を選択して、そのステータスを持つアプライアンスをリストします。

ヒント　ステータス レベルに関する行内の矢印が下を向いている場合は、そのステータスのアプライアンス リストが下側のテーブルに表示されます。矢印が右を向いている場合、アプライアンス リストは非表示です。

次のトピックで、[Health Monitor] ページから実行可能な作業について詳しく説明します。

- 「ヘルス モニタ ステータスの解釈」（P.55-45）
- 「アプライアンス ヘルス モニタの使用」（P.55-46）
- 「正常性ポリシーの設定」（P.55-7）
- 「ヘルス モニタ アラートの設定」（P.55-41）

ヘルス モニタ ステータスの解釈

ライセンス：任意

次の表に示すように、重大度別に使用可能なステータス カテゴリには、Error、Critical、Warning、Normal、Recovered、および Disabled が含まれます。

表 55-6　ヘルス ステータス インジケータ

ステータス レベル	ステータス アイコン	ステータス色	説明
Error		白色	アプライアンス上の 1 つ以上のヘルス モニタリング モジュールで障害が発生し、それ以降、正常に再実行していないことを示します。テクニカル サポート担当者に連絡して、ヘルス モニタリング モジュールの更新プログラムを入手してください。
Critical		赤	アプライアンス上の 1 つ以上のヘルス モジュールが重大制限を超え、問題が解決されていないことを示します。
Warning		黄色	アプライアンス上の 1 つ以上のヘルス モジュールが警告制限を超え、問題が解決されていないことを示します。
Normal		緑	アプライアンス上のすべてのヘルス モジュールがアプライアンスに適用された正常性ポリシーで設定された制限内で動作していることを示します。
Recovered		緑	アプライアンス上のすべてのヘルス モジュールがアプライアンスに適用された正常性ポリシーで設定された制限内で動作していることを示します。これには、前に Critical または Warning 状態だったモジュールも含まれます。
Disabled		青	アプライアンスが無効またはブラックリストに登録されている、アプライアンスに正常性ポリシーが適用されていない、またはアプライアンスが現在到達不能になっていることを示します。

アプライアンス ヘルス モニタの使用

ライセンス：任意

アプライアンス ヘルス モニタは、アプライアンスのヘルス ステータスの詳細ビューを提供します。

注　通常は、非活動状態が 1 時間（または設定された他の時間間隔）続くと、ユーザはセッションからログアウトされます。ヘルス モニタを長期間受動的に監視する予定の場合は、一部のユーザのセッション タイムアウトの免除、またはシステム タイムアウト設定の変更を検討してください。詳細については、「ユーザ ログイン設定の管理」（P.48-50）および「ユーザ インターフェイスの設定」（P.50-29）を参照してください。

特定のアプライアンスのステータス サマリーを表示する方法：

アクセス：Admin/Maint/Any Security Analyst

ステップ 1　[Health] > [Health Monitor] の順に選択します。

[Health Monitor] ページが表示されます。

ステップ 2　特定のステータスを持つアプライアンスのリストを表示するには、そのステータス行内の矢印をクリックします。

ヒント　ステータス レベルに関する行内の矢印が下を向いている場合は、そのステータスのアプライアンス リストが下側のテーブルに表示されます。矢印が右を向いている場合、アプライアンス リストは非表示です。

ステップ 3　アプライアンス リストの [Appliance] 列で、ヘルス モニタ ツールバーで詳細を表示するアプライアンスの名前をクリックします。

[Health Monitor Appliance] ページが表示されます。

ステップ 4　オプションで、[Module Status Summary] グラフで、表示するイベント ステータス カテゴリの色をクリックします。[Alert Detail] リストは表示を切り替えてイベントを表示または非表示にします。

詳細については、次の項を参照してください。

- 「ヘルス モジュールについて」（P.55-3）
- 「ヘルス モニタ ステータスの解釈」（P.55-45）
- 「ステータス別のアラートの表示」（P.55-47）
- 「アプライアンスのすべてのモジュールの実行」（P.55-47）
- 「特定のヘルス モジュールの実行」（P.55-48）
- 「ヘルス モジュール アラート グラフの生成」（P.55-49）
- 「ヘルス モニタを使用したトラブルシューティング」（P.55-50）

ステータス別のアラートの表示

ライセンス：任意

ステータス別にアラートのカテゴリを表示または非表示にできます。

ステータス別にアラートを表示する方法：

アクセス：Admin/Maint/Any Security Analyst

ステップ 1　表示するアラートのヘルス ステータスに対応するステータス アイコンまたは円グラフの色セグメントをクリックします。そのカテゴリのアラートが [Alert Detail] リストに表示されます。

ステータス別にアラートを非表示にする方法：

アクセス：Admin/Maint/Any Security Analyst

ステップ 1　表示するアラートのヘルス ステータスに対応するステータス アイコンまたは円グラフの色セグメントをクリックします。そのカテゴリの [Alert Detail] リスト内のアラートが非表示になります。

アプライアンスのすべてのモジュールの実行

ライセンス：任意

ヘルス モジュール テストは、正常性ポリシー作成時に設定されたポリシー実行時間間隔で自動的に実行されます。ただし、アプライアンスの最新の正常性情報を収集するためにすべてのヘルス モジュール テストをオンデマンドで実行することもできます。

アプライアンスのすべてのヘルス モジュールを実行する方法：

アクセス：Admin/Maint/Any Security Analyst

ステップ 1　[Health] > [Health Monitor] の順に選択します。

[Health Monitor] ページが表示されます。

ステップ 2　アプライアンス リストを展開して特定のステータスを持つアプライアンスを表示するには、そのステータス行内の矢印をクリックします。

ヒント　ステータス レベルに関する行内の矢印が下を向いている場合は、そのステータスのアプライアンス リストが下側のテーブルに表示されます。矢印が右を向いている場合、アプライアンス リストは非表示です。

ステップ 3　アプライアンス リストの [Appliance] 列で、詳細を表示するアプライアンスの名前をクリックします。

[Health Monitor Appliance] ページが表示されます。

ステップ 4　[Run All Modules] をクリックします。

ステータス バーにテストの進捗状況が表示されてから、[Health Monitor Appliance] ページが更新されます。

注　ヘルス モジュールを手動で実行した場合は、自動的に発生する最初の更新に、手動で実行されたテストの結果が反映されない可能性があります。手動で実行したばかりのモジュールの値が変更されていない場合は、数秒待ってから、デバイス名をクリックしてページを更新します。ページが再び自動的に更新するのを待つこともできます。

特定のヘルス モジュールの実行

ライセンス：任意

ヘルス モジュール テストは、正常性ポリシー作成時に設定されたポリシー実行時間間隔で自動的に実行されます。ただし、そのモジュールの最新のヘルス情報を収集するためにヘルス モジュール テストをオンデマンドで実行することもできます。

特定のヘルス モジュールを実行する方法：

アクセス：Admin/Maint/Any Security Analyst

ステップ 1　[Health] > [Health Monitor] の順に選択します。

[Health Monitor] ページが表示されます。

ステップ 2　アプライアンス リストを展開して特定のステータスを持つアプライアンスを表示するには、そのステータス行内の矢印をクリックします。

ヒント　ステータス レベルに関する行内の矢印が下を向いている場合は、そのステータスのアプライアンス リストが下側のテーブルに表示されます。矢印が右を向いている場合、アプライアンス リストは非表示です。

ステップ 3　アプライアンス リストの [Appliance] 列で、詳細を表示するアプライアンスの名前をクリックします。

[Health Monitor Appliance] ページが表示されます。

ステップ 4　[Health Monitor Appliance] ページの [Module Status Summary] グラフで、表示するヘルス アラート ステータス カテゴリの色をクリックします。

[Alert Detail] リストが展開して、そのステータス カテゴリの選択されたアプライアンスのヘルス アラートがリストされます。

ステップ 5　イベントのリストを表示するアラートの [Alert Detail] 行で、[Run] をクリックします。

ステータス バーにテストの進捗状況が表示されてから、[Health Monitor Appliance] ページが更新されます。

注　ヘルス モジュールを手動で実行した場合は、自動的に発生する最初の更新に、手動で実行されたテストの結果が反映されない可能性があります。手動で実行したばかりのモジュールの値が変更されていない場合は、数秒待ってから、デバイス名をクリックしてページを更新します。ページが再び自動的に更新するのを待つこともできます。

ヘルス モジュール アラート グラフの生成

ライセンス：任意

特定のアプライアンスの特定のヘルス テストの一定期間に及ぶ結果をグラフ化できます。

ヘルス アラート モジュール グラフを生成する方法：

アクセス：Admin/Maint/Any Security Analyst

ステップ 1　[Health] > [Health Monitor] の順に選択します。

[Health Monitor] ページが表示されます。

ステップ 2　アプライアンス リストを展開して特定のステータスを持つアプライアンスを表示するには、そのステータス行内の矢印をクリックします。

ヒント　ステータス レベルに関する行内の矢印が下を向いている場合は、そのステータスのアプライアンス リストが下側のテーブルに表示されます。矢印が右を向いている場合、アプライアンス リストは非表示です。

ステップ 3　アプライアンス リストの [Appliance] 列で、詳細を表示するアプライアンスの名前をクリックします。

[Health Monitor Appliance] ページが表示されます。

ステップ 4　[Health Monitor Appliance] ページの [Module Status Summary] グラフで、表示するヘルス アラート ステータス カテゴリの色をクリックします。

[Alert Detail] リストが展開して、そのステータス カテゴリの選択されたアプライアンスのヘルス アラートがリストされます。

ステップ 5　イベントのリストを表示するアラートの [Alert Detail] 行で、[Graph] をクリックします。

一定期間のイベントのステータスを示すグラフが表示されます。グラフの下の [Alert Detail] セクションに、選択したアプライアンスのすべてのヘルス アラートがリストされます。

ヒント　イベントが表示されない場合は、時間範囲を調整する必要があります。詳細については、「イベント時間の制約の設定」（P.47-27）を参照してください。

ヘルス モニタを使用したトラブルシューティング

ライセンス：任意

アプリケーションで問題が発生したときに、サポートから問題の診断を容易にするためにトラブルシューティング ファイルの作成を依頼されることがあります。次の表に示すオプションのいずれかを選択して、ヘルス モニタから報告されるトラブルシューティング データをカスタマイズすることができます。

表 55-7　選択可能なトラブルシュート オプション

オプション	報告内容
Snort Performance and Configuration	アプライアンス上の Snort に関連するデータとコンフィギュレーション設定
Hardware Performance and Logs	アプライアンス ハードウェアのパフォーマンスに関連するデータとログ
System Configuration, Policy, and Logs	アプライアンスの現在のシステム設定に関連するコンフィギュレーション設定、データ、およびログ
Detection Configuration, Policy, and Logs	アプライアンス上の検出に関連するコンフィギュレーション設定、データ、およびログ
Interface and Network Related Data	アプライアンスのインライン セットとネットワーク設定に関連するコンフィギュレーション設定、データ、およびログ
Discovery, Awareness, VDB Data, and Logs	アプライアンス上の現在の検出設定と認識設定に関連するコンフィギュレーション設定、データ、およびログ
Upgrade Data and Logs	アプライアンスの以前のアップグレードに関連するデータとログ
All Database Data	トラブルシュート レポートに含まれるすべてのデータベース関連データ
All Log Data	アプライアンス データベースによって収集されたすべてのログ
Network Map Information	現在のネットワーク トポロジ データ

一部のオプションは報告するデータの観点で重複していますが、どのオプションが選択されたかに関係なく、トラブルシューティング ファイルには冗長なコピーは含まれません。

詳細については、次の項を参照してください。

- 「アプライアンス トラブルシューティング ファイルの生成」（P.55-50）
- 「トラブルシューティング ファイルのダウンロード」（P.55-51）

アプライアンス トラブルシューティング ファイルの生成

ライセンス：任意

次の手順を使用して、サポートに送信可能なカスタマイズされたトラブルシューティング ファイルを生成できます。

トラブルシューティング ファイルを生成する方法：

アクセス：Admin/Maint/Any Security Analyst

ステップ 1　[Health] > [Health Monitor] の順に選択します。

[Health Monitor] ページが表示されます。

ステップ 2　アプライアンス リストを展開して特定のステータスを持つアプライアンスを表示するには、そのステータス行内の矢印をクリックします。

ヒント　ステータス レベルに関する行内の矢印が下を向いている場合は、そのステータスのアプライアンス リストが下側のテーブルに表示されます。矢印が右を向いている場合、アプライアンス リストは非表示です。

ステップ 3　アプライアンス リストの [Appliance] 列で、詳細を表示するアプライアンスの名前をクリックします。

[Health Monitor Appliance] ページが表示されます。

ステップ 4　[Generate Troubleshooting Files] をクリックします。

[Troubleshooting Options] ポップアップ ウィンドウが表示されます。

ステップ 5　[All Data] を選択して可能性のあるすべてのトラブルシューティング データを生成することも、個別のチェック ボックスをオンにしてレポートをカスタマイズすることもできます。詳細については、「選択可能なトラブルシュート オプション」の表を参照してください。

ステップ 6　**[OK]** をクリックします。

防御センターがトラブルシューティング ファイルを生成します。タスク キュー（[System] > [Monitoring] > [Task Status]）でファイル生成プロセスを監視できます。

ステップ 7　次の項（トラブルシューティング ファイルのダウンロード）の手順に進みます。

トラブルシューティング ファイルのダウンロード

ライセンス：任意

次の手順を使用して、生成されたトラブルシューティング ファイルのコピーをダウンロードします。

トラブルシューティング ファイルをダウンロードする方法：

アクセス：Admin/Maint/Any Security Analyst

ステップ 1　[System] > [Monitoring] > [Task Status] の順にクリックします。

[Task Status] ページが表示されます。

ステップ 2　生成されたトラブルシューティング ファイルに対応するタスクを探します。

ステップ 3　アプライアンスがトラブルシューティング ファイルを生成し、タスク ステータスが [Completed] に変ったら、[Click to retrieve generated files] をクリックします。

ステップ 4　ブラウザのプロンプトに従ってファイルをダウンロードします。

ファイルは単一の `.tar.gz` ファイルとしてダウンロードされます。

ステップ 5　サポートの指示に従って、トラブルシューティング ファイルをシスコに送信してください。

ヘルス イベントの操作

ライセンス：任意

防御センターには、ヘルス モニタによって収集されたヘルス ステータス イベントを迅速かつ容易に分析するための完全にカスタマイズ可能なイベント ビューがあります。このイベント ビューでは、イベント データを検索して表示したり、調査中のイベントに関係する他の情報に簡単にアクセスしたりできます。

ヘルス イベント ビュー ページで実行可能なさまざまな機能がすべてのイベント ビュー ページで一貫しています。これらの一般的な手順の詳細については、「ヘルス イベント ビューについて」（P.55-52）を参照してください。

[Health] > [Health Events] メニュー オプションで、ヘルス イベントを表示したり、特定のイベントを検索したりできます。

イベントの表示について詳しくは、次の項を参照してください。

- 「ヘルス イベント ビューについて」（P.55-52）では、FireSIGHT が生成するイベントの種類について説明します。
- 「ヘルス イベントの表示」（P.55-52）では、[Event View] ページへのアクセス方法と使用方法について説明します。
- 「ヘルス イベントの検索」（P.55-59）では、[Event Search] ページを使用して特定のイベントを検索する方法について説明します。

ヘルス イベント ビューについて

ライセンス：任意

防御センター ヘルス モニタはヘルス イベントを記録し、記録されたヘルス イベントは [Health Event View] ページで表示できます。ヘルス モジュールごとにテストされる条件を理解していれば、ヘルス イベントに対するアラートをより効率的に設定できます。ヘルス イベントを生成するヘルス モジュールのタイプの詳細については、「ヘルス モジュールについて」（P.55-3）を参照してください。

ヘルス イベントの表示方法と検索方法については、次の項を参照してください。

- 「ヘルス イベントの表示」（P.55-52）
- 「ヘルス イベント テーブルについて」（P.55-58）
- 「ヘルス イベントの検索」（P.55-59）

ヘルス イベントの表示

ライセンス：任意

ヘルス モニタによって収集されたアプライアンス ヘルス データはさまざまな方法で表示できます。

詳細については、次のトピックを参照してください。

- 「すべてのステータス イベントの表示」（P.55-53）
- 「モジュールとアプライアンス別のヘルス イベントの表示」（P.55-53）
- 「ヘルス イベント テーブル ビューの操作」（P.55-54）

- 「3D9900 デバイスのハードウェア アラート詳細の解釈」（P.55-55）
- 「シリーズ 3 デバイスのハードウェア アラート詳細の解釈」（P.55-56）

すべてのステータス イベントの表示

ライセンス：任意

[Table View of Health Events] ページには、選択したアプライアンス上のすべてのヘルス イベントのリストが表示されます。このページに表示されるイベントを生成したヘルス モジュールについては、「ヘルス モジュールについて」（P.55-3）を参照してください。

防御センター上の [Health Monitor] ページからヘルス イベントにアクセスした場合は、すべての管理対象アプライアンスのすべてのヘルス イベントが表示されます。

すべての管理対象アプライアンス上のすべてのステータス イベントを表示する方法：

アクセス：Admin/Maint/Any Security Analyst

ステップ 1　[Health] > [Health Events] の順に選択します。

[Events] ページが開いて、すべてのヘルス イベントが表示されます。

注　イベントが表示されない場合は、時間範囲を調整する必要があります。詳細については、「イベント時間の制約の設定」（P.47-27）を参照してください。

ヒント　このビューをブックマークすれば、イベントの [Health Events] テーブルを含むヘルス イベント ワークフロー内のページに戻ることができます。ブックマークしたビューには、現在見ている時間範囲内のイベントが表示されますが、必要に応じて時間範囲を変更してテーブルを最新情報で更新することができます。詳細については、「イベント時間の制約の設定」（P.47-27）を参照してください。

モジュールとアプライアンス別のヘルス イベントの表示

ライセンス：任意

特定のアプライアンス上の特定のヘルス モジュールによって生成されたイベントを問い合わせることができます。

特定のモジュールのヘルス イベントを表示する方法：

アクセス：Admin/Maint/Any Security Analyst

ステップ 1　[Health] > [Health Monitor] の順に選択します。

[Health Monitor] ページが表示されます。

ステップ 2　アプライアンス リストを展開して特定のステータスを持つアプライアンスを表示するには、そのステータス行内の矢印をクリックします。

ヒント　ステータス レベルに関する行内の矢印が下を向いている場合は、そのステータスのアプライアンス リストが下側のテーブルに表示されます。矢印が右を向いている場合、アプライアンス リストは非表示です。

ステップ 3　アプライアンス リストの [Appliance] 列で、詳細を表示するアプライアンスの名前をクリックします。

[Health Monitor Appliance] ページが表示されます。

ステップ 4　[Health Monitor Appliance] ページの [Module Status Summary] グラフで、表示するヘルス アラート ステータス カテゴリの色をクリックします。

[Alert Detail] リストが展開して、そのステータス カテゴリの選択されたアプライアンスのヘルス アラートがリストされます。

ステップ 5　イベントのリストを表示するアラートの [Alert Detail] 行で、[Events] をクリックします。

[Health Events] ページが開いて、制限としてアプライアンスの名前と選択したヘルス アラート モジュールの名前を含むクエリーのクエリー結果が表示されます。

イベントが表示されない場合は、時間範囲を調整する必要があります。詳細については、「イベント時間の制約の設定」（P.47-27）を参照してください。

ステップ 6　選択したアプライアンスのすべてのステータス イベントを表示する場合は、[Search Constraints] を展開し、[Module Name] 制限をクリックして削除します。

ヘルス イベント テーブル ビューの操作

ライセンス：任意

次の表に、[Event View] ページから実行可能な各操作の説明を示します。

表 55-8　ヘルス イベント ビューの機能

目的	操作
ヘルス イベント ビューに表示される列の内容を確認する	「ヘルス イベント テーブルについて」（P.55-58）で詳細を確認してください。
ヘルス テーブル ビューに表示されるイベントの時刻と日付範囲を変更する	「イベント時間の制約の設定」（P.47-27）で詳細を確認してください。 イベント ビューを時間で制限すると、アプライアンスの設定された時間範囲（グローバルか、イベント固有か）外で生成されたイベントがイベント ビューに表示される場合があります。この現象は、アプライアンスの変動時間範囲を設定している場合でも発生する可能性があります。
表示されたイベントをソートする、イベント テーブルに表示する列を変更する、または表示するイベントを制限する	「ドリルダウン ワークフロー ページのソート」（P.47-39）で詳細を確認してください。
ヘルス イベントを削除する	削除するイベントの横にあるチェック ボックスをオンにして、[Delete] をクリックします。現在制限されているビューですべてのイベントを削除するには、[Delete All] をクリックしてから、すべてのイベントを削除することを確認します。

表 55-8　ヘルス イベント ビューの機能 （続き）

目的	操作
イベント ビュー ページ間を移動する	「ワークフロー内の他のページへのナビゲート」（P.47-40）で詳細を確認してください。
他のイベント テーブルに移動して関連イベントを表示する	「ワークフロー間のナビゲート」（P.47-41）で詳細を確認してください。
現在のページをブックマークしてすばやくそこに戻れるようにする	[Bookmark This Page] をクリックして、ブックマークの名前を指定し、[Save] をクリックします。詳細については、「ブックマークの使用」（P.47-42）を参照してください。
ブックマーク管理ページに移動する	イベント ビューで [View Bookmarks] をクリックします。詳細については、「ブックマークの使用」（P.47-42）を参照してください。
テーブル ビュー内のデータに基づいてレポートを生成する	[Report Designer] をクリックします。詳細については、「イベント ビューからのレポート テンプレートの作成」（P.44-2）を参照してください。
別のヘルス イベント ワークフローを選択する	[(switch workflow)] をクリックします。詳細については、「ワークフローの選択」（P.47-19）を参照してください。
1 つのヘルス イベントに関連付けられた詳細を表示する	イベントの左側にある下矢印リンクをクリックします。
複数のヘルス イベントのイベント詳細を表示する	詳細を表示するイベントに対応する行の横にあるチェックボックスをオンにしてから、[View] をクリックします。
ビュー内のすべてのイベントのイベント詳細を表示する	[View All] をクリックします。
特定のステータスのすべてのイベントを表示する	そのステータスを持つイベントの [Status] 列内のステータス アイコンをクリックします。

3D9900 デバイスのハードウェア アラート詳細の解釈

ライセンス：任意

3D9900 デバイス モデルでは、次の表に示すイベントに応答してハードウェア アラームが生成されます。トリガー条件はアラートのメッセージ詳細で見つけることができます。

表 55-9　3D9900 デバイスの監視対象条件

監視対象条件	黄色または赤色エラー状態の原因
NFE カードの存在	アプライアンスに対して無効な NFE ハードウェアが検出されると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細に NFE カードの存在への参照が追加されます。
NFE 温度	• NFE 温度が 95 ℃を超えると、ハードウェア アラーム モジュールのヘルス ステータスが黄色に変化し、メッセージ詳細に NFE 温度への参照が追加されます。 • NFE 温度が 99 ℃を超えると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細に NFE 温度への参照が追加されます。

表 55-9　3D9900 デバイスの監視対象条件 （続き）

監視対象条件	黄色または赤色エラー状態の原因
NFE プラットフォーム デーモン	NFE プラットフォーム デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照が追加されます。
NFE メッセージ デーモン	NFE メッセージ デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照が追加されます。
NFE TCAM デーモン	NFE TCAM デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照が追加されます。
LBIM の存在	ロード バランシング インターフェイス モジュール（LBIM）スイッチ アセンブリが存在しないか、通信していない場合は、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細に LBIM の存在への参照が追加されます。
Scmd デーモン	Scmd デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照が追加されます。
Psls デーモン	Psls デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照が追加されます。
Ftwo デーモン	Ftwo デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照が追加されます。
Rulesd（ホスト ルール）デーモン	Rulesd デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが黄色に変化し、メッセージ詳細にデーモンへの参照が追加されます。
nfm_ipfragd（ホスト フラグ）デーモン	nfm_ipfragd デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照が追加されます。

シリーズ 3 デバイスのハードウェア アラート詳細の解釈

シリーズ 3 デバイスでは、次の表に示すイベントに応答してハードウェア アラームが生成されます。トリガー条件がアラートのメッセージ詳細に表示されます。

表 55-10　シリーズ 3 デバイスの監視対象条件

監視対象条件	黄色または赤色エラー状態の原因
クラスタ ステータス	クラスタ化されたデバイスが相互に通信していない（ケーブル配線の問題などで）場合は、ハードウェア アラーム モジュールが赤色に変化します。
ftwo デーモン ステータス	ftwo デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照が追加されます。

表 55-10　シリーズ 3 デバイスの監視対象条件（続き）

監視対象条件	黄色または赤色エラー状態の原因
検出された NFE カード	システム上で検出された NFE カードの枚数を示します。この値がアプライアンスの予想 NFE カウントと一致しない場合は、ハードウェア アラーム モジュールが赤色に変化します。
NFE ハードウェア ステータス	1 つ以上の NFE カードが通信していない場合は、ハードウェア アラーム モジュールが赤色に変化し、該当するカードがメッセージ詳細に表示されます。
NFE ハートビート	システムが NFE ハートビートを検出しなかった場合は、ハードウェア アラーム モジュールが赤色に変化し、メッセージ詳細に関連カードへの参照が追加されます。
NFE 内部リンク ステータス	NMSB カードと NFE カード間のリンクがダウンした場合は、ハードウェア アラーム モジュールが赤色に変化し、メッセージ詳細に関連ポートへの参照が追加されます。
NFE メッセージ デーモン	NFE メッセージ デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照（および該当する場合は NFE カード番号）が追加されます。
NFE 温度	• NFE 温度が 97 ℃を超えると、ハードウェア アラーム モジュールのヘルス ステータスが黄色に変化し、メッセージ詳細に NFE 温度への参照（および該当する場合は NFE カード番号）が追加されます。 • NFE 温度が 102 ℃を超えると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細に NFE 温度への参照 （および該当する場合は NFE カード番号）が追加されます。
NFE 温度ステータス	特定の NFE カードの現在の温度ステータスを示します。OK の場合ハードウェア アラーム モジュールは緑色を、Warning の場合は黄色を、Critical の場合は赤色（および該当する場合は NFE カード番号）を示します。
NFE TCAM デーモン	NFE TCAM デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照（および該当する場合は NFE カード番号）が追加されます。
nfm_ipfragd（ホスト フラグ）デーモン	nfm_ipfragd デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照（および該当する場合は NFE カード番号）が追加されます。
NFE プラットフォーム デーモン	NFE プラットフォーム デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照（および該当する場合は NFE カード番号）が追加されます。
NMSB コミュニケーション	メディア アセンブリが存在しないか、通信していない場合は、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細に NFE 温度への参照（および該当する場合は NFE カード番号）が追加されます。

表 55-10　シリーズ 3 デバイスの監視対象条件（続き）

監視対象条件	黄色または赤色エラー状態の原因
psls デーモン ステータス	psls デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照が追加されます。
Rulesd（ホスト ルール）デーモン	Rulesd デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが黄色に変化し、メッセージ詳細にデーモンへの参照（および該当する場合は NFE カード番号）が追加されます。
scmd デーモン ステータス	scmd デーモンがダウンすると、ハードウェア アラーム モジュールのヘルス ステータスが赤色に変化し、メッセージ詳細にデーモンへの参照が追加されます。

ヘルス イベント テーブルについて

ライセンス：任意

防御センターのヘルス モニタを使用して、FireSIGHT システム内の重要な機能のステータスを確認できます。ハードウェア ステータスやソフトウェア ステータスなどのさまざまな側面を監視するため正常性ポリシーを作成してアプライアンスに適用します。正常性ポリシー内で有効にされたヘルス モニタ モジュールが、さまざまなテストを実行してアプライアンスのヘルス ステータスを特定します。ヘルス ステータスが指定された基準を満たしている場合は、ヘルス イベントが生成されます。ヘルス モニタリングの詳細については、「システムのモニタリング」（P.54-1）を参照してください。

ヘルス イベント テーブル内のフィールドについて、次の表で説明します。

表 55-11　ヘルス イベント フィールド

フィールド	説明
Test Name	イベントを生成したヘルス モジュールの名前。ヘルス モジュールのリストについては、「ヘルス モジュール」を参照してください。
Time	ヘルス イベントのタイムスタンプ。
Description	イベントを生成したヘルス モジュールの説明。たとえば、プロセスが実行できない場合に生成されるヘルス イベントには [Unable to Execute] というラベルが付けられます。
Value	イベントが生成されたヘルス テストから得られた結果の値（単位数）。 たとえば、監視対象デバイスが 80% 以上の CPU リソースを使用しているときに生成されるヘルス イベントを防御センターが生成した場合の値は 80 ～ 100 です。
Units	結果の単位記述子。アスタリスク（*）を使用してワイルドカード検索を作成できます。 たとえば、監視対象デバイスが 80% 以上の CPU リソースを使用しているときに生成されるヘルス イベントを防御センターが生成した場合の単位記述子はパーセント記号（%）です。
Status	アプライアンスに報告されるステータス（Critical、Yellow、Green、または Disabled）。
Device	ヘルス イベントが報告されたアプライアンス。

ヘルス イベントのテーブル ビューを表示する方法：

アクセス：Admin/Maint/Any Security Analyst

ステップ 1　[Health] > [Health Events] の順に選択します。

テーブル ビューが表示されます。ヘルス イベントの操作方法については、「ヘルス イベントの操作」（P.55-52）を参照してください。

ヒント　ヘルス イベントのテーブル ビューが含まれていないカスタム ワークフローを使用している場合は、[(switch workflow)] をクリックします。[Select Workflow] ページで、[Health Events] をクリックします。

ヘルス イベントの検索

ライセンス：任意

特定のヘルス イベントを検索できます。ネットワーク環境に合わせてカスタマイズされた検索を作成して保存すれば、後で再利用できます。次の表に、使用可能な検索基準の説明を示します。

表 55-12　ヘルス イベントの検索基準

検索フィールド	説明
Module Name	表示するヘルス イベントを生成したモジュールの名前を指定します。たとえば、CPU パフォーマンスを測定するイベントを表示するには、「`CPU`」と入力します。検索によって、該当する CPU 使用率イベントと CPU 温度イベントが取得されるはずです。
Value	表示するイベントのヘルス テストから得られた結果の値（単位数）を指定します。 たとえば、値として 15 を指定し、[Units] フィールドに「`CPU`」と入力した場合は、テストの実行時点でアプライアンス CPU が 15% の使用率で動作していたイベントが取得されます。
Description	表示するイベントの説明を指定します。たとえば、プロセスが実行できなかったヘルス イベントを表示するには、「`Unable to Execute`」と入力します。このフィールドでアスタリスク（*）を使用してワイルドカード検索を作成できます。
Units	表示するイベントのヘルス テストから得られた結果の単位記述子を指定します。このフィールドでアスタリスク（*）を使用してワイルドカード検索を作成できます。 たとえば、[Units] フィールドに「`%`」と入力した場合は、ディスク使用率モジュールの [Units] フィールドに「%」というラベルが付けられる（そして追加のテキストがない）ため、ディスク使用率モジュールに関するすべてのイベントが取得されます。ただし、[Units] フィールドに「`*%`」と入力した場合は、[Units] フィールド内のテキストの最後に「%」記号が付いているモジュールに関するすべてのイベントが取得されます。
Status	表示するヘルス イベントのステータスを指定します。有効なステータス レベルは、Critical、Warning、Normal、Error、および Disabled です。 たとえば、Critical ステータスを示すすべてのヘルス イベントを取得するには、「`Critical`」と入力します。
Device	デバイスの名前を指定します。

特殊な検索構文や検索の保存とロードに関する情報を含む検索の詳細については、「検索設定の実行と保存」（P.45-1）を参照してください。

ヘルス イベント検索を実行して保存する方法：

アクセス：Admin/Maint/Any Security Analyst

ステップ 1　[Analysis] > [Search] の順に選択します。

[Search] ページが表示されます。

ステップ 2　[Table] ドロップダウン リストから、[Health Events] を選択します。

[Health Event Search] ページが表示されます。

ステップ 3　オプションで、検索を保存する場合は、[Name] フィールドに検索の名前を入力します。

名前を入力しなかった場合は、検索を保存するときに自動的に名前が付けられます。

ステップ 4　「ヘルス イベントの検索基準」の表内の説明に従って、該当するフィールドに検索基準を入力します。

複数の基準を入力した場合は、すべての基準を満たすレコードだけが検索で返されます。

ステップ 5　オプションで、他のユーザがアクセスできるように検索を保存する場合、[Save As Private] チェック ボックスをオフにします。そうではなく、検索をプライベートとして保存するには、このチェック ボックスをオンのままにします。

ヒント　カスタム ユーザ ロールに対するデータ制限として検索を使用する場合は、それをプライベート検索として保存する**必要があります**。

ステップ 6　次の選択肢があります。

- 検索を開始するには、[Search] ボタンをクリックします。

  現在の時刻範囲に制限された検索結果がデフォルト ヘルス イベント ワークフローに表示されます。カスタム ワークフローを含む別のワークフローを使用するには、[(switch workflow)] をクリックします。別のデフォルト ワークフローの指定方法については、「イベント ビュー設定の設定」（P.58-3）を参照してください。
- 既存の検索を変更して、その変更を保存する場合は、[Save] をクリックします。
- 検索基準を保存する場合は、[Save as New Search] をクリックします。検索が保存され（[Save As Private] が選択された場合はユーザ アカウントに関連付けられる）、後で実行できるようになります。

検索の詳細については、次の項を参照してください。

- 「保存済み検索設定のロード」（P.45-3）
- 「保存済み検索設定の削除」（P.45-4）