デバイスの管理

防御センター は、FireSIGHT システムのキー コンポーネントです。FireSIGHT システム を構成するさまざまなデバイスを管理したり、ネットワーク上で検出された脅威を集約し、分析して対処したりするために、防御センター を使用できます。

防御センター を使用してデバイスを管理すると、以下の利点があります。

- すべてのデバイスのポリシーを単一の場所から設定できるため、設定の変更が容易になります。
- さまざまなタイプのソフトウェア アップデートをデバイスにインストールできます。
- 正常性ポリシーを管理対象デバイスに適用して、防御センター からデバイスのヘルス ステータスをモニタできます。

防御センター は、侵入イベント、ネットワーク検出情報、およびデバイスのパフォーマンス データを集約して相互に関連付けます。そのため、ユーザはデバイスが相互の関連でレポートする情報をモニタして、ネットワーク上で行われている全体的なアクティビティを評価することができます。

詳細については、次の項を参照してください。

- 管理の概念（4-2 ページ）では、防御センター を使用したデバイスの管理に関連する機能および制約事項について説明しています。
- 管理インターフェイスについて（4-4 ページ）では、トラフィック チャネルと複数の管理インターフェイスを使用してパフォーマンスを向上させる方法、および異なるネットワーク上にあるデバイス間のトラフィックを分離する方法について説明しています。
- NAT 環境での作業（4-8 ページ）では、ネットワーク アドレス変換（NAT）環境でデバイスの管理をセットアップする際の原則について説明しています。
- ハイ アベイラビリティの設定（4-9 ページ）では、運用の継続性の確保に役立てるために 2 つの 防御センター をハイ アベイラビリティ ペアとしてセットアップする方法について説明しています。
- デバイスの操作（4-19 ページ）では、デバイスと 防御センター 間の接続を確立する方法と、無効にする方法について説明しています。また、管理対象デバイスを追加および削除する方法と、管理対象デバイスの状態を変更する方法についても説明しています。
- デバイス グループの管理（4-29 ページ）では、デバイス グループを作成する方法と、デバイス グループのデバイスを追加および削除する方法について説明しています。
- デバイスのクラスタリング（4-31 ページ）では、2 つの管理対象デバイス間でハイ アベイラビリティを確立および管理する方法について説明しています。
- デバイス設定の編集（4-54 ページ）では、ユーザが編集できるデバイス属性と、それらの属性を編集する方法について説明しています。

- スタック構成のデバイスの管理（4-47 ページ）では、管理対象デバイスのスタックを構成する方法と、スタックからデバイスを削除する方法について説明しています。
- センシング インターフェイスの設定（4-66 ページ）では、管理対象デバイスでインターフェイスを設定する方法について説明しています。

管理の概念

防御センター を使用することで、デバイス動作のほぼすべての側面を管理できます。デバイスを管理するために必要な 防御センター は 1 つだけですが、2 つ目の 防御センター をハイアベイラビリティ ペアの一方として使用することもできます。以下の項で、FireSIGHT システムの展開を計画する際に知っておくべき概念のいくつかを説明します。

- 防御センター で管理できるデバイス（4-2 ページ）
- ポリシーとイベント以外の機能（4-3 ページ）
- 冗長な 防御センター の使用（4-4 ページ）

防御センター で管理できるデバイス

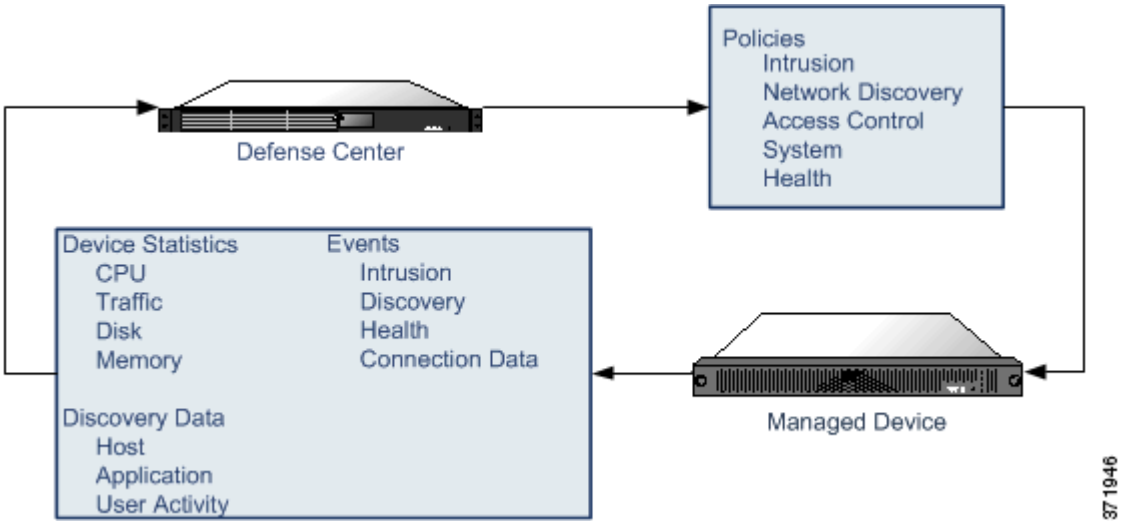
FireSIGHT システムの展開環境の集中管理ポイントとして 防御センター を使用することで、以下のデバイスを管理できます。

- FirePOWER 管理対象デバイス
- Cisco ASA with FirePOWER Services デバイス
- ソフトウェア ベースのデバイス（仮想デバイスや Blue Coat X-Series 向け Cisco NGIPS など）

（注）　シスコ では、DC500 モデルの 防御センター で管理するデバイスを最大 3 台（ソフトウェア ベースのデバイスを含む）に制限することを推奨しています。DC500 データベースに伴う制限事項の詳細については、データベース イベントの制限の表を参照してください。

デバイスを管理する際の情報は、SSL で暗号化されたセキュアな TCP トンネルを介して、防御センター とデバイスの間で送信されます。

以下の図に、防御センター と管理対象デバイスの間で送信される情報をリストします。アプライアンス間で送信されるポリシーとイベントのタイプは、デバイス タイプによって異なることに注意してください。



ポリシーとイベント以外の機能

ライセンス: 任意（Any）

防御センター では、ポリシーをデバイスに適用したり、デバイスからイベントを受信したりするだけでなく、以下のデバイス関連のタスクも実行できます。

デバイスのバックアップ

仮想の管理対象デバイス、Blue Coat X-Series 向け Cisco NGIPS、または Cisco ASA with FirePOWER Services のバックアップ ファイルを作成または復元することは**できません**。

物理管理対象デバイス自体からそのバックアップを実行する場合は、デバイス設定**のみ**をバックアップできます。設定データと統合ファイル（任意）をバックアップするには、管理 防御センター を使用してデバイスのバックアップを実行します。

イベント データをバックアップするには、管理用の 防御センター のバックアップを実行します。詳細については、バックアップ ファイルの作成（70-2 ページ）を参照してください。

デバイスの更新

シスコでは適宜、FireSIGHT システムのアップデートをリリースしています。これらのアップデートには以下が含まれます。

- 侵入ルールの更新（新しいルールや更新された侵入ルールが含まれる場合があります）
- 脆弱性データベースの更新
- 地理位置情報の更新
- ソフトウェア パッチおよびアップデート

防御センター を使用して、管理対象デバイスにアップデートをインストールできます。

冗長な 防御センター の使用

ライセンス: 任意（Any）

サポートされる防御センター: DC1000、DC1500、DC2000、DC3000、DC3500、DC4000

2 つの 防御センター をハイ アベイラビリティ ペアとしてセットアップできます。これにより、いずれか一方の 防御センター で障害が発生したとしても、冗長機能を確保できます。ポリシーやユーザ アカウントなどが 2 つの 防御センター 間で共有されます。イベントは両方の 防御センター に自動的に送信されます。詳細については、ハイ アベイラビリティの設定（4-9 ページ）を参照してください。

管理インターフェイスについて

管理インターフェイスは、防御センターが管理するすべてのデバイスと 防御センター の間の通信手段を提供します。アプライアンス間のトラフィック制御を正常に維持することが、展開の成功に不可欠です。

シリーズ 3 アプライアンスおよび仮想 防御センター では、デフォルト設定を変更して 防御センター またはデバイス（あるいは両方）の管理インターフェイスを有効にすることで、アプライアンス間のトラフィックを 2 つのトラフィック チャネルに分けることができます。*管理トラフィック チャネル*は、すべての内部トラフィック（アプライアンスおよびシステムの管理専用のデバイス間トラフィックなど）を伝送し、*イベント トラフィック チャネル*は、すべてのイベント トラフィック（Web イベントなど）を伝送します。トラフィックを 2 つのチャネルに分割することにより、アプライアンス間に 2 つの接続ポイントが作成され、スループットが増加してパフォーマンスが向上します。それぞれが固有の IP アドレス（IPv4 または IPv6）とホスト名を持つ*複数の管理インターフェイス*を使用することで、トラフィック チャネルを別々に管理し、スループットを増加させることができます。

また、複数の管理インターフェイスを使用する場合、1 つの 防御センター だけで、さまざまなネットワークからのトラフィックをそれぞれ分離して管理できます。特定のネットワークのトラフィックを他のネットワークのトラフィックから分離するには、管理インターフェイスを使用して特定の宛先ネットワークまでのスタティック ルートを追加し、個々の管理インターフェイスにデバイスを登録します。同じインターフェイスで両方のトラフィック チャネルを送信することもでき、また、追加の管理インターフェイスが十分にある場合は、ネットワーク トラフィックを切り分けて各管理インターフェイスが 1 つのトラフィック チャネルだけを伝送するように設定することもできます。

通常、管理インターフェイスは、アプライアンスの背面に配置されています。詳細については、『*FireSIGHT システム Installation Guide*』の「Identifying the Management Interfaces」を参照してください。管理インターフェイスの詳細については、以下の項を参照してください。

- 1 つの管理インターフェイスの使用（4-5 ページ）
- 複数の管理インターフェイスの使用（4-5 ページ）
- トラフィック チャネルの使用（4-6 ページ）
- ネットワーク ルートの使用（4-7 ページ）

1 つの管理インターフェイスの使用

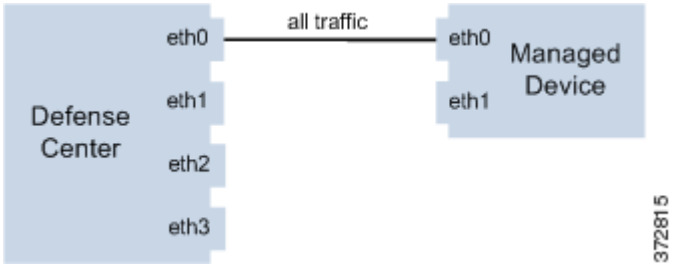
ライセンス: 任意（Any）

サポートされるデバイス: 任意（Any）

サポートされる防御センター: 任意（Any）

デバイスを 防御センター に登録すると、防御センター 上の管理インターフェイスとデバイス上の管理インターフェイスとの間のすべてのトラフィックを伝送する単一通信チャネルが確立されます。

以下の図に、デフォルトの単一通信チャネルを示します。1 つのインターフェイスにより、管理トラフィックとイベント トラフィックの両方が 1 つの通信チャネルで伝送されます。



複数の管理インターフェイスの使用

ライセンス: 任意（Any）

サポートされるデバイス: シリーズ 3

サポートされる防御センター: シリーズ 3、仮想

複数の管理インターフェイスを有効化および設定して、それぞれに固有の IP アドレス（IPv4 または IPv6）、および、必要に応じてホスト名を割り当て、各トラフィック チャネルを異なる管理インターフェイスに送信することによって、トラフィック スループットを著しく向上させることができます。負荷が軽い管理トラフィックの搬送用には小さなインターフェイスを構成し、負荷が大きいイベント トラフィックの搬送用には大きなインターフェイスを構成します。デバイスを別々の管理インターフェイスに登録し、同一のインターフェイスに対して両方のトラフィック チャネルを構成したり、防御センター によって管理されるすべてのデバイスのイベント トラフィック チャネルを専用の管理インターフェイスで伝送することができます。

防御センター 上の特定の管理インターフェイスから別のネットワーク上のデバイスまでのルートを作成することもできます。デフォルト以外の管理インターフェイスに他のネットワークのデバイスを登録すると、そのデバイスのトラフィックは、デフォルトの管理インターフェイス（`eth0`）に登録されているデバイスのトラフィックから分離されます。詳細については、ネットワーク ルートの使用（4-7 ページ）を参照してください。

デフォルト以外の管理インターフェイスは、デフォルトの管理インターフェイスと同じ機能を多数備えています（防御センター 間のハイ アベイラビリティの使用など）。ただし、次の例外があります。

- DHCP は、デフォルト（`eth0`）管理インターフェイスにのみ設定できます。追加のインターフェイス（`eth1` など）には、固有の静的 IP アドレスとホスト名が必要です。
- デフォルト以外の管理インターフェイスを使用して 防御センター と管理対象デバイスを接続する場合、それらのアプライアンスが NAT デバイスによって分離されているならば、同じ管理インタフェースを使用するよう両方のトラフィック チャネルを設定する必要があります。

- Lights-Out Management は、デフォルトの管理インターフェイスでのみ使用できます。
- 70xx ファミリ では、トラフィックを 2 つのチャネルに分離して、防御センター 上の 1 つ以上の管理インターフェイスにトラフィックを送信するようにそれらのチャネルを設定できます。ただし、70xx ファミリには 1 つの管理インターフェイスしかないため、デバイスは唯一の管理インターフェイス上で 防御センター から送信されたトラフィックを受信します。

トラフィック チャネルの使用

ライセンス: 任意（Any）

サポートされるデバイス: シリーズ 3

サポートされる防御センター: シリーズ 3、仮想

1 つの管理インターフェイス上で 2 つのトラフィック チャネルを使用する場合、防御センターと管理対象デバイスの間に 2 つの接続を作成します。同じインターフェイス上の 2 つのチャネルのうちの一方が管理トラフィックを伝送し、もう一方がイベント トラフィックを伝送します。

次の例は、同じインターフェイス上に 2 つの独立したトラフィック チャネルを持つ通信チャネルを示しています。

複数の管理インターフェイスを使用する場合、トラフィック チャネルを 2 つの管理インターフェイスに分割することによりパフォーマンスを向上できます。それによって両方のインターフェイス容量が増し、トラフィック フローが増加します。一方のインターフェイスで管理トラフィック チャネルを伝送し、もう一方のインターフェイスでイベント トラフィック チャネルを伝送します。いずれかのインターフェイスで障害が発生した場合は、すべてのトラフィックがアクティブ インターフェイスに再ルーティングされるため、接続が維持されます。

次の図は、2 つの管理インターフェイス上にある管理トラフィック チャネルとイベント トラフィック チャネルを示しています。

専用の管理インターフェイスを使用して、複数のデバイスからのイベント トラフィックのみを伝送することができます。この設定では、管理トラフィック チャネルを伝送する別の管理インターフェイスに各デバイスを登録し、すべてのデバイスからのすべてのイベント トラフィックを、防御センター 上の 1 つの管理インターフェイスで伝送します。インターフェイスで障害が発生した場合は、トラフィックがアクティブ インターフェイスに再ルーティングされるため、接続が維持されます。すべてのデバイスのイベント トラフィックが同じインターフェイスで伝送されることから、トラフィックはネットワーク間で分離されないことに注意してください。

以下の図では、2 台のデバイスが別々の管理チャネル トラフィック インターフェイスを使用し、イベント トラフィック チャネルに対しては同じ専用インターフェイスを共有しています。

1 つの管理インターフェイス上で 2 つのトラフィック チャネルを使用する場合、防御センターと管理対象デバイスの間に 2 つの接続を作成します。同じインターフェイス上の 2 つのチャネルのうちの一方が管理トラフィックを伝送し、もう一方がイベント トラフィックを伝送します。複数の管理インターフェイスを使用する場合は、トラフィック チャネルを 2 つの管理インターフェイスに分けることができます。それによって両方のインターフェイスの容量が増し、トラフィック フローが増えるため、さらにパフォーマンスが向上します。一方のインターフェイスで管理トラフィック チャネルを伝送し、もう一方のインターフェイスでイベント トラフィック チャネルを伝送します。いずれかのインターフェイスで障害が発生した場合は、すべてのトラフィックがアクティブ インターフェイスに再ルーティングされるため、接続が維持されます。

複数のデバイスからのイベント トラフィックだけを伝送する専用の管理インターフェイスを使用することもできます。この設定では、管理トラフィック チャネルを伝送する別の管理インターフェイスに各デバイスを登録し、すべてのデバイスからのすべてのイベント トラフィックを、防御センター 上の 1 つの管理インターフェイスで伝送します。インターフェイスで障害が発生した場合は、トラフィックがアクティブ インターフェイスに再ルーティングされるため、接続が維持されます。すべてのデバイスのイベント トラフィックが同じインターフェイスで伝送されることから、トラフィックはネットワーク間で分離されないことに注意してください。

ネットワーク ルートの使用

ライセンス: 任意（Any）

サポートされるデバイス: シリーズ 3

サポートされる防御センター: シリーズ 3、仮想

防御センター 上の特定の管理インターフェイスから別のネットワークまでのルートを作成できます。そのネットワークのデバイスを 防御センター 上の指定された管理インターフェイスに登録すると、別のネットワーク上のデバイスと 防御センター の間で独立した接続が実現されます。両方のトラフィック チャネルが同じ管理インターフェイスを使用するように設定することで、そのデバイスからのトラフィックが他のネットワーク上のデバイス トラフィックから確実に分離された状態を維持できます。ルーテッド インターフェイスは 防御センター 上の他のすべてのインターフェイスから分離されているため、ルーテッド管理インターフェイスに障害が発生した場合、接続が失われます。

ヒント　シスコでは、デフォルトの管理インターフェイス（eth0）以外の管理インターフェイスを使用して 防御センター とそのデバイスを登録する場合は、静的 IP アドレスを使用することを推奨しています。DHCP は、デフォルト管理インターフェイスだけでサポートされています。

防御センター をインストールした後に、Web インターフェイスを使用して、複数の管理インターフェイスを設定します。詳しくは、*FireSIGHT System ユーザ ガイド*の「Configuring Appliance Settings」を参照してください。

次の図では、2 台のデバイスですべてのトラフィックに対して別々の管理インターフェイスを使用することにより、ネットワーク トラフィックを分離しています。さらに管理インターフェイスを追加して、デバイスごとに独立した管理トラフィック チャネル インターフェイスとイベント トラフィック チャネル インターフェイスを構成できます。

NAT 環境での作業

ライセンス: 任意（Any）

ネットワーク アドレス変換（NAT）とは、ルータを介したネットワーク トラフィックの送受信方式であり、ルータ経由でトラフィックがパススルーされるときに送信元または宛先 IP アドレスの再割り当てが行われます。NAT を使用した標準的なアプリケーションでは、プライベート ネットワーク上の複数のホストが、単一のパブリック IP アドレスを使用してパブリック ネットワークにアクセスできます。

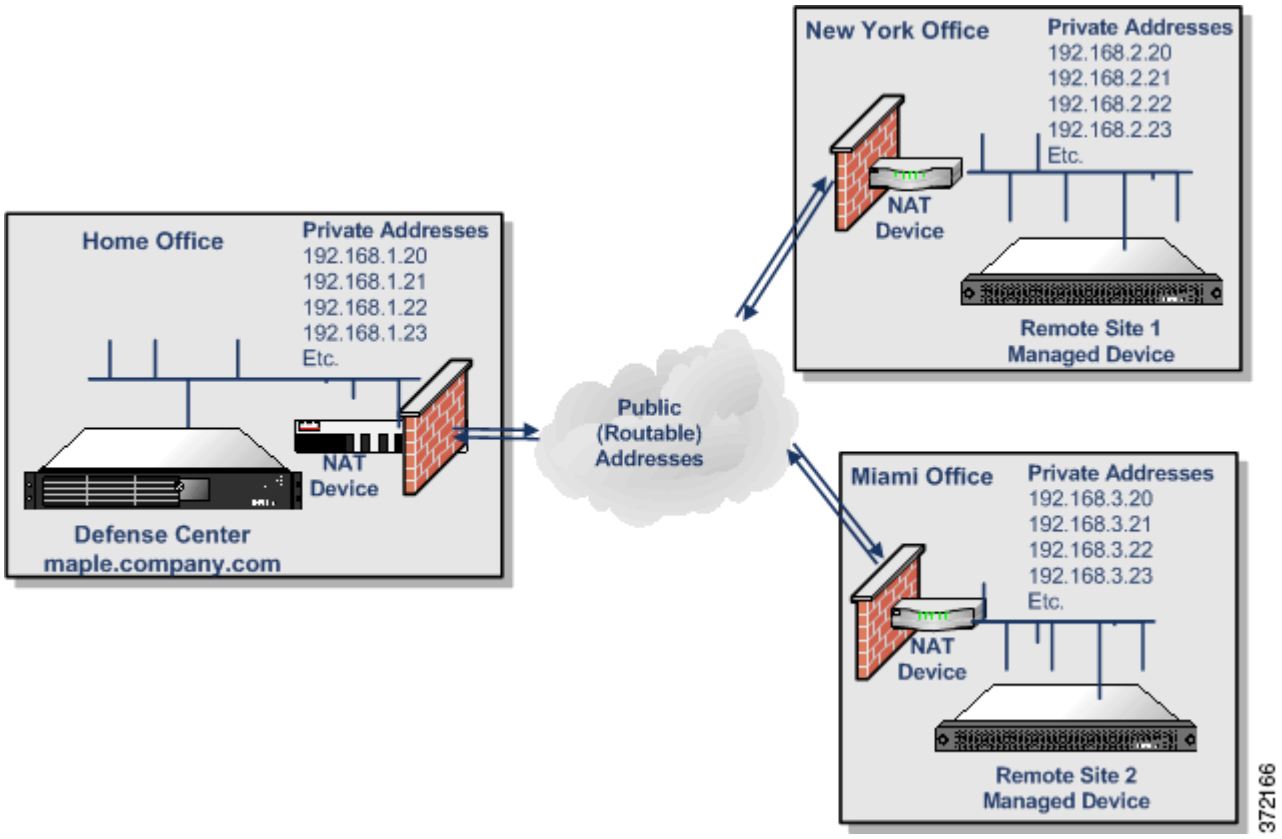
デバイスを 防御センター に追加するときには、アプライアンス間の通信を確立します。通信を確立するために必要な情報は、その環境が NAT を使用するかどうかによって異なります。

- NAT を使用していない環境では、登録キーと IP アドレス、または両方のアプライアンスの完全修飾ドメイン名が必要です。
- NAT を使用している環境では、登録キーと一意の NAT ID が必要です。

（注）　NAT ID は、デバイスを 防御センター に登録するために使用されているすべての NAT ID の間で**一意でなければなりません**。

デフォルト以外の管理インターフェイスを使用して 防御センター と管理対象デバイスを接続していて、これらのアプライアンスが NAT デバイスによって分離されている場合、両方のトラフィック チャネルが同じ管理インターフェイスを使用するように設定する必要があります。

以下の図は、NAT 環境で 2 つのデバイスを管理する 防御センター を示しています。登録キーは一意である必要はないため、同じ登録キーを使用して両方のデバイスを追加できます。ただし、デバイスを 防御センター に追加する際には、**一意の** NAT ID を使用する必要があります。



ハイ アベイラビリティの設定

ライセンス: 任意（Any）

サポートされる防御センター: DC1000、DC1500、DC2000、DC3000、DC3500、DC4000

運用の継続性を確保するために、ハイ アベイラビリティ機能を使用して、冗長 防御センター でデバイスを管理するように指定することができます。特定の設定要素と、管理対象デバイスから両方の 防御センター に送信されるイベント データ ストリームは、両方の 防御センター で保持されます。一方の 防御センター で障害が発生した場合は、もう一方の 防御センター を使用して、中断することなくネットワークをモニタできます。

注意　システムでは一部の機能をプライマリ 防御センター に制限しているため、そのアプライアンスで障害が発生した場合は、セカンダリ 防御センター をアクティブに昇格する必要があります。ハイ アベイラビリティ ステータスのモニタリングおよび変更（4-16 ページ）を参照してください。

ハイ アベイラビリティをセットアップする方法の詳細については、以下の項を参照してください。

- ハイ アベイラビリティの使用（4-10 ページ）では、ハイ アベイラビリティの実装時に共有される設定と共有されない設定をリストしています。
- ハイ アベイラビリティを実装する際のガイドライン（4-14 ページ）では、ハイ アベイラビリティを実装する場合に従わなければならないガイドラインを概説しています。
- ハイ アベイラビリティのセットアップ（4-15 ページ）では、プライマリおよびセカンダリ 防御センター を指定する方法を説明しています。
- ハイ アベイラビリティ ステータスのモニタリングおよび変更（4-16 ページ）では、リンクされた 防御センター のステータスを確認する方法、およびプライマリ 防御センター に障害が発生した場合に 防御センター のロールを変更する方法を説明しています。
- ハイ アベイラビリティの無効化とデバイスの登録解除（4-18 ページ）では、リンクされた 防御センター 間のリンクを完全に削除する方法を説明しています。
- ペアにされた 防御センター 間での通信の一時停止（4-19 ページ）では、リンクされた 防御センター 間の通信を一時停止する方法を説明しています。
- ペアにされた 防御センター 間での通信の再開（4-19 ページ）では、リンクされた 防御センター 間の通信を再開する方法を説明しています。

ハイ アベイラビリティの使用

ライセンス：任意（Any）

サポートされる防御センター：DC1000、DC1500、DC2000、DC3000、DC3500、DC4000

DC1500、DC2000、DC3500 および DC4000 はハイ アベイラビリティ設定をサポートしていますが、DC750 および仮想 防御センター はサポートしていません。シスコでは、ハイ アベイラビリティ ペアの両方の 防御センター に同じモデルを使用することを**強く**推奨しています。異なる 防御センター モデル間にハイ アベイラビリティをセットアップ**しないでください**。

ハイ アベイラビリティ モードでは、2 つの 防御センター がそれぞれ *プライマリ*、*セカンダリ* として指定されますが、どちらの 防御センター に対してもポリシーやその他の変更を行うことができます。ただし、シスコ では、設定の変更はプライマリ 防御センター に対して**のみ**行い、セカンダリ 防御センター はバックアップとして保持することを推奨しています。

防御センター は、互いの設定に対する変更を定期的に更新するため、ユーザが一方の 防御センター に対して行った変更は、もう一方の 防御センター に 10 分以内に適用されます。（各 防御センター には 5 分の同期サイクルが設定されていますが、このサイクル自体が最大 5 分間同期しないことがあるため、変更は 5 分のサイクル 2 回分の間に行われます。）この 10 分間では、それぞれの 防御センター の設定が異なっているように見える場合があります。

たとえば、プライマリ 防御センター でポリシーを作成し、セカンダリ 防御センター でも管理されるデバイスにそのポリシーを適用した場合、防御センター 間で通信が行われる前に、デバイスがセカンダリ 防御センター に接続する可能性があります。この場合、デバイスに適用されているポリシーは、セカンダリ 防御センター ではまだ認識していないため、防御センター が同期するまでは、セカンダリ 防御センター に「unknown」という名前の新しいポリシーが表示されます。

また、防御センター の同期が行われる前の同じ期間に両方の 防御センター に対してポリシーやその他の変更を行った場合は、防御センター がプライマリまたはセカンダリのどちらに指定されているかに関係なく、最後に行われた変更が優先されます。

ハイ アベイラビリティ ペアを設定する前に、以下の前提条件を確認してください。

- 両方の 防御センター に、管理者権限が割り当てられた admin という名前のユーザ アカウントがあること。これらのアカウントは同じパスワードを使用する必要があります。
- admin アカウントの他には、2 つの 防御センター に同じユーザ名を持つユーザ アカウントがないこと。重複するユーザ アカウントがある場合は、ハイ アベイラビリティを設定する前に、一方のユーザ アカウントを削除するか、名前を変更してください。

ハイ アベイラビリティ ペアとして設定する 2 つの 防御センター は、信頼された同じ管理ネットワーク上に存在する必要も、同じ地理的な場所に存在する必要もありません。

運用の継続性を確保するには、ハイ アベイラビリティ ペアの両方の 防御センター がインターネットにアクセス可能である必要があります。インターネット アクセス要件（E-2 ページ）を参照してください。特定の機能については、プライマリ 防御センター がインターネットにアクセスし、同期プロセスでセカンダリと情報を共有します。したがって、プライマリに障害が発生した場合は、ハイ アベイラビリティ ステータスのモニタリングおよび変更（4-16 ページ）の説明に従ってセカンダリをアクティブ ステータスにプロモートする必要があります。

ハイ アベイラビリティ ペアのメンバー間で共有される設定と共有されない設定の詳細については、以下の項を参照してください。

- 共有される設定（4-11 ページ）
- 正常性ポリシーとシステム ポリシー（4-12 ページ）
- 相関応答（4-12 ページ）
- ライセンス（4-13 ページ）
- URL フィルタリングおよびセキュリティ インテリジェンス（4-13 ページ）
- クラウド接続およびマルウェア情報（4-13 ページ）
- ユーザ エージェント（4-14 ページ）

共有される設定

ライセンス：任意（Any）

サポートされる防御センター：DC1000、DC1500、DC2000、DC3000、DC3500、DC4000

ハイ アベイラビリティ ペアの 防御センター は、以下の情報を共有します。

- ユーザ アカウントの属性、認証設定、カスタム ユーザ ロール
- ユーザ アカウントおよびユーザ認識のための認証オブジェクトと、アクセス コントロール ルールでユーザ条件に使用可能なユーザおよびグループ
- カスタム ダッシュボード
- カスタム ワークフローおよびテーブル
- デバイス属性（デバイスのホスト名など）、デバイスが生成するイベントの保存先、デバイスが属するグループ
- アクセス コントロール、SSL、ネットワーク分析、侵入、ファイル、およびネットワーク検出ポリシー
- ローカル侵入ルール
- カスタム侵入ルールの分類
- ネットワーク検出ポリシー

- ユーザ定義のアプリケーション プロトコル ディテクタと、それらのディテクタによって検出されるアプリケーション
- アクティブ化されたカスタム フィンガープリント
- ホスト属性
- ネットワーク検出ユーザ フィードバック（注意およびホスト重要度、ネットワーク マップからのホスト、アプリケーション、ネットワークの削除、脆弱性の非アクティブ化または変更など）
- 相関ポリシーおよびルール、コンプライアンス ホワイトリスト、トラフィック プロファイル
- 変更調整スナップショットおよびレポート設定
- 侵入ルール、地理位置情報データベース（GeoDB）、および脆弱性データベース（VDB）の更新
- 上記の設定のいずれかに関連付けられている再利用可能なオブジェクト（変数セットなど）

正常性ポリシーとシステム ポリシー

ライセンス：任意（Any）

サポートされる防御センター：DC1000、DC1500、DC2000、DC3000、DC3500、DC4000

防御センター および管理対象デバイスの正常性ポリシーとシステム ポリシーは、ハイ アベイラビリティ ペアで共有されます。新しくアクティブ化された 防御センター で、正常性ポリシー、モジュール、ブラックリストに関する情報が同期されるように十分な時間を設けてください。

（注） システム ポリシーは、ハイ アベイラビリティ ペアの 防御センター で共有されますが、自動的には適用されません。両方の 防御センター で同一のシステム ポリシーを使用するには、同期後にポリシーを適用します。

ハイ アベイラビリティ ペアの 防御センター は、以下のシステムおよび正常性ポリシー情報を共有します。

- システム ポリシー
- システム ポリシー設定（適用されるポリシーおよびその適用対象）
- 正常性ポリシー
- ヘルス モニタリング設定（適用されるポリシーおよびその適用対象）
- ヘルス モニタリングからブラックリスト化されるアプライアンス
- 個々のヘルス モニタリング ポリシーでブラックリスト化されるアプライアンス

相関応答

ライセンス：任意（Any）

サポートされる防御センター：DC1000、DC1500、DC2000、DC3000、DC3500、DC4000

相関ポリシー、ルール、および応答は、防御センター の間で共有されますが、相関ルールとその応答の間の *関連付け* は、防御センター の間で共有されません。これは、相関ポリシー違反が発生した場合に重複する応答が起動されないようにするためです。

修復を相関ポリシーに関連付けられるようにするには、その前に、セカンダリ 防御センター ですべてのカスタム修復モジュールをアップロードしてインストールし、修復インスタンスを設定する必要があります。運用の継続性を確保するために、プライマリ 防御センター で障害が発生した場合は、ただちにセカンダリ 防御センター で相関ポリシーを適切な応答と修復に関連付けるだけでなく、セカンダリ 防御センター の Web インターフェイスを使用してセカンダリをアクティブに昇格する必要があります。詳細については、ハイ アベイラビリティ ステータスのモニタリングおよび変更（4-16 ページ）を参照してください。相関応答の詳細については、相関ポリシーの作成（51-53 ページ）および修復の作成（54-1 ページ）を参照してください。

セカンダリ 防御センター でルールまたはホワイトリストとその応答および修復の間の関連付けを作成していた場合、障害発生後にプライマリ 防御センター を復元する際に、必ず関連付けを削除し、プライマリ 防御センター だけが応答と修復を生成するようにしてください。

ライセンス

ライセンス：任意（Any）

サポートされる防御センター：DC1000、DC1500、DC2000、DC3000、DC3500、DC4000

高可用性ペアの防御センターは、ライセンスを**共有しません**。ペアの各メンバーに同等のライセンスを追加する必要があります。詳細については、ライセンスについて（65-1 ページ）を参照してください。

URL フィルタリングおよびセキュリティ インテリジェンス

ライセンス：URL フィルタリング（URL Filtering）または Protection

サポートされるデバイス：シリーズ 3、仮想、X-シリーズ、ASA FirePOWER

サポートされる防御センター：DC1000、DC1500、DC2000、DC3000、DC3500、DC4000

URL フィルタリングとセキュリティ インテリジェンスの設定および情報は、ハイ アベイラビリティ展開の 防御センター 間で同期されます。ただし、プライマリ 防御センター だけが、URL カテゴリおよびレピュテーション データとセキュリティ インテリジェンスのフィード更新をダウンロードします。

プライマリ 防御センター に障害が発生した場合は、セカンダリ 防御センター が URL フィルタリング クラウドとその他すべての設定済みフィード サイトにアクセスできることを確認するだけでなく、セカンダリ 防御センター の Web インターフェイスを使用してセカンダリをアクティブに昇格する必要もあります。詳細については、ハイ アベイラビリティ ステータスのモニタリングおよび変更（4-16 ページ）を参照してください。

クラウド接続およびマルウェア情報

ライセンス：任意、または Malware

サポートされるデバイス：すべて（シリーズ 2 または X-シリーズ を除く）

サポートされる防御センター：DC1000、DC1500、DC2000、DC3000、DC3500、DC4000

ハイ アベイラビリティ ペアの 防御センター は、ファイル ポリシーおよび関連する設定を共有しますが、Collective Security Intelligence クラウド 接続とマルウェア性質はいずれも共有しません。運用の継続性を確保し、検出されたファイルのマルウェア性質が両方の防御センターで同じであるようにするためには、プライマリとセカンダリ両方の防御センターがクラウドにアクセスできなければなりません。詳細については、マルウェア防御とファイル制御について（37-2 ページ）を参照してください。

ユーザ エージェント

ライセンス：FireSIGHT

サポートされる防御センター：DC1000、DC1500、DC2000、DC3000、DC3500、DC4000

ユーザ エージェントは同時に最大 5 つの防御センターに接続できます。エージェントの接続先は、プライマリ 防御センター でなければなりません。プライマリ 防御センター に障害が発生した場合、すべてのエージェントがセカンダリ 防御センター と通信できることを確認する必要があります。詳細については、Active Directory のログインを報告するためのユーザ エージェントの使用（17-11 ページ）を参照してください。

ハイ アベイラビリティを実装する際のガイドライン

ライセンス：任意（Any）

サポートされる防御センター：DC1000、DC1500、DC2000、DC3000、DC3500、DC4000

ハイ アベイラビリティを利用するには、以下の項のガイドラインに従う必要があります。

プライマリおよびセカンダリ 防御センター の要件

一方の 防御センター をプライマリとして指定し、もう一方の 防御センター をセカンダリとして指定する必要があります。アプライアンスがアクティブから非アクティブ（またはその逆）に切り替わるときには、プライマリおよびセカンダリの指定はそのまま維持されます。

プライマリまたはセカンダリのどちらに指定するかに関わらず、ハイ アベイラビリティをセットアップする前に、両方の 防御センター にポリシー、ルール、管理対象デバイスなどを設定できます。

混乱を避けるために、セカンダリ 防御センター は元の状態から開始してください。つまり、ポリシーの作成や変更、新しいルールの作成、管理対象のデバイスの設定が行われていない状態から開始します。確実にセカンダリ 防御センター が元の状態であるようにするには、工場出荷時の初期状態に復元します。その場合、イベントと設定データも 防御センター から削除されることに注意してください。詳細については、『*FireSIGHT システム Installation Guide*』を参照してください。

バージョン要件

両方の 防御センター で実行しているソフトウェアとルールは、同じアップデート バージョンでなければなりません。また、このソフトウェア バージョンは、管理対象デバイスのソフトウェア バージョン以降でなければなりません。

通信要件

デフォルトでは、ペアとなっている 防御センター は、ポート 8305/tcp を使用して通信します。ポートを変更するには、管理ポートの変更（4-24 ページ）で説明している手順に従ってください。

2 つの 防御センター が同じネットワーク セグメント上に存在する必要はありませんが、防御センター が互いに通信可能であり、共有するデバイスとも通信可能でなければなりません。つまり、プライマリ 防御センター は、セカンダリ 防御センター の独自の管理インターフェイスの IP アドレスでセカンダリ 防御センター と通信できること、およびその逆も可能であることが必要です。さらに、それぞれの 防御センター が管理対象のデバイスと通信できること、あるいは管理対象デバイスが 防御センター と通信できることも必要です。

ハイ アベイラビリティのセットアップ

ライセンス:任意（Any）

サポートされる防御センター:DC1000、DC1500、DC2000、DC3000、DC3500、DC4000

ハイ アベイラビリティを使用するには、一方の 防御センター をプライマリとして指定し、同じモデルのもう一方の 防御センター をセカンダリとして指定する必要があります。2 つのアプライアンス間のリモート管理通信を編集する方法については、リモート管理の編集（4-23 ページ）を参照してください。

注意　シスコ では、設定の変更はプライマリ 防御センター に対して**のみ**行い、セカンダリ 防御センター はバックアップとして使用することを推奨しています。

必ず、ハイ アベイラビリティを設定する前に、リンクする 防御センター の間で時刻設定を同期してください。時刻を設定する方法の詳細については、時間の同期（63-28 ページ）を参照してください。

設定されているポリシーとカスタム標準テキスト ルールの数に応じて、すべてのルールとポリシーが両方の 防御センター に表示されるまでに 10 分程度かかることがあります。[ハイ アベイラビリティ（High Availability）] ページを表示して、2 つの 防御センター 間のリンクのステータスを確認できます。また、[タスクのステータス（Task Status）] をモニタして、プロセスが完了するタイミングを確認することもできます。ハイ アベイラビリティ ステータスのモニタリングおよび変更（4-16 ページ）を参照してください。

ハイ アベイラビリティ ペアのいずれかの 防御センター のイメージを再生成しなければならない場合は、最初にハイ アベイラビリティ リンクを無効にします。防御センター のイメージを再生成した後、ハイ アベイラビリティ ペアを再確立すると、既存の 防御センター のデータが新たに追加された 防御センター に同期されます。防御センター のイメージを再生成できない場合は（たとえば、アプライアンスに障害が発生した場合）、サポートに連絡してください。

2 つの 防御センター のハイ アベイラビリティをセットアップするには、以下を行います。

アクセス:管理

手順 1　セカンダリ 防御センター として指定する 防御センター にログインします。

手順 2　[システム（System）] > [ローカル（Local）] > [登録（Registration）] を選択します。

[登録（Registration）] ページが表示されます。

手順 3　[ハイ アベイラビリティ（High Availability）] をクリックします。

[ハイ アベイラビリティ（High Availability）] ページが表示されます。

手順 4　[セカンダリ 防御センター（secondary Defense Center）] オプションをクリックします。

[セカンダリ 防御センター 設定（Secondary Defense Center Setup）] ページが表示されます。

手順 5　[プライマリ DC ホスト（Primary DC Host）] テキスト ボックスに、プライマリ 防御センター のホスト名または IP アドレスを入力します。

注意　ネットワークで IP アドレスの割り当てに DHCP を使用している場合は、IP アドレスではなく、必ずホスト名を使用してください。

ルーティング可能アドレスが管理ホストにない場合は、[Primary DC Host] フィールドを空のままにして構いません。その場合は、[登録キー（Registration Key）] と [固有 NAT ID（Unique NAT ID）] の両方のフィールドを使用します。

手順 6　[登録キー(Registration Key)] テキスト ボックスに、1 回限り使用する登録キーを入力します。

手順 7　必要に応じて、[固有 NAT ID(Unique NAT ID)] フィールドに、プライマリ 防御センター を識別するために使用する、英数字による一意の登録 ID を入力します。スタック構成のデバイスの管理 (4-47 ページ) は参照しないでください。詳細については、4-8 ページの「NAT 環境での作業」を参照してください。

手順 8　[登録(Register)] をクリックします。

成功メッセージが表示され、[ピア マネージャ(Peer Manager)] ページに、セカンダリ 防御センター の現在の状態が示されます。

手順 9　管理者アクセス権限を持つアカウントを使用して、プライマリとして指定する 防御センター にログインします。

手順 10　[システム(System)] > [ローカル(Local)] > [登録(Registration)] を選択します。

[登録(Registration)] ページが表示されます。

手順 11　[ハイ アベイラビリティ(High Availability)] をクリックします。

[ハイ アベイラビリティ(High Availability)] ページが表示されます。

手順 12　[プライマリ 防御センター(primary Defense Center)] オプションをクリックします。

[プライマリ 防御センター 設定(Primary Defense Center Setup)] ページが表示されます。

手順 13　[セカンダリ DC ホスト(Secondary DC Host)] テキスト ボックスに、セカンダリ 防御センター のホスト名または IP アドレスを入力します。

注意　ネットワークで IP アドレスの割り当てに DHCP を使用している場合は、IP アドレスではなく、必ずホスト名を使用してください。

手順 14　[登録キー(Registration Key)] テキスト ボックスに、ステップ 6 で入力した 1 回限り使用する登録キーと同じものを入力します。

手順 15　セカンダリ 防御センター で一意の NAT ID を使用した場合は、ステップ 7 で入力したのと同じ登録 ID を [固有 NAT ID(Unique NAT ID)] テキスト ボックスに入力します。

手順 16　[登録(Register)] をクリックします。

成功メッセージが表示され、[ピア マネージャ(Peer Manager)] ページに、プライマリ 防御センター の現在の状態が示されます。

ハイ アベイラビリティ ステータスのモニタリングおよび変更

ライセンス: 任意(Any)

サポートされる防御センター: DC1000、DC1500、DC2000、DC3000、DC3500、DC4000

プライマリとセカンダリの Defense Center を特定した後、ハイ アベイラビリティ ペアのいずれかのアプライアンスから、ローカル Defense Center とそのピアに関する次の情報を確認できます。

- ピアとなる IP アドレスまたはホスト名
- ピアの製品モデル
- ピアのソフトウェア バージョン
- ピアのオペレーティング システム

- ハイ アベイラビリティ ペアのメンバーが最後に同期されてから経過した時間
- ローカル アプライアンスのロールとステータス（アクティブおよびプライマリ、非アクティブおよびプライマリ、非アクティブおよびセカンダリ、アクティブおよびセカンダリ）

プライマリ 防御センター に障害が発生した場合は、[ハイ アベイラビリティ（High Availability）] ページを使用して 防御センター のロールを変更することもできます。システムでは以下の機能をプライマリ 防御センター に制限しているため、そのアプライアンスで障害が発生した場合は、セカンダリ 防御センター をアクティブに昇格する必要があります。

- URL カテゴリおよびレピュテーション データの更新。詳細については、URL フィルタリングおよびセキュリティ インテリジェンス（4-13 ページ）を参照してください。
- セキュリティ インテリジェンス フィードの更新。詳細については、URL フィルタリングおよびセキュリティ インテリジェンス（4-13 ページ）を参照してください。
- 相関ルールと応答の関連付け。詳細については、相関応答（4-12 ページ）を参照してください。

ハイ アベイラビリティ ステータスを確認するには、以下を行います。

アクセス：管理

手順 1　ハイ アベイラビリティを使用してリンクした 防御センター のいずれか一方にログインします。

手順 2　[システム（System）] > [ローカル（Local）] > [登録（Registration）] を選択します。

[登録（Registration）] ページが表示されます。

手順 3　[ハイ アベイラビリティ（High Availability）] をクリックします。

[ハイ アベイラビリティ（High Availability）] ページが表示されます。

手順 4　[ハイ アベイラビリティ ステータス（High Availability Status）] に、ハイ アベイラビリティ ペアの防御センター に関する以下の情報が一覧表示されます。

- ピアとなる IP アドレスまたはホスト名
- ピアの製品モデル
- ピアのソフトウェア バージョン
- ピアのオペレーティング システム
- ハイ アベイラビリティ ペアのメンバーが最後に同期されてから経過した時間
- ローカル アプライアンスのロールとステータス（アクティブおよびプライマリ、非アクティブおよびプライマリ、非アクティブおよびセカンダリ、アクティブおよびセカンダリ）
- 2 つの Defense Center 間でロールを切り替えるためのオプション

手順 5　共有機能に影響するすべてのアクションの後、10 分以内に（各 防御センター ごとに 5 分間）、2 つの 防御センター が自動的に同期されます。たとえば、一方の 防御センター で新しいポリシーを作成すると、そのポリシーは 5 分以内にもう一方の 防御センター と自動的に共有されます。ただし、ポリシーを即時に同期させる必要がある場合は、[同期（Synchronize）] をクリックします。

（注）　ハイ アベイラビリティ ペアとして設定された 防御センター からデバイスを削除し、そのデバイスを再び追加する場合、シスコでは、削除してから追加するまでに少なくとも 5 分間待つことを推奨しています。この間隔を空けることにより、ハイ アベイラビリティ ペアが初回で再同期されることが確実になります。5 分間待たないと、1 回の同期サイクルでは、デバイスが両方の 防御センター に追加されない場合があります。

手順 6　[ロールの切り替え（Switch Roles）] をクリックして、ローカル ロールをアクティブから非アクティブ、または非アクティブからアクティブに変更します。

プライマリまたはセカンダリの指定は変更されずに、2 つのピア間でロールが切り替わります。

手順 7　ツールバーの [ピア マネージャ（Peer Manager）] をクリックします。

[ピア マネージャ（Peer Manager）] ページが表示されます。

次の情報が表示されます。

- ハイ アベイラビリティ ペアのもう一方の 防御センター の IP アドレス
- 通信リンクのステータス（登録済みまたは登録解除済み）
- ハイ アベイラビリティ ペアの状態（有効または無効）

2 つのアプライアンス間のリモート管理通信を編集する方法については、リモート管理の編集（4-23 ページ）を参照してください。

ハイ アベイラビリティの無効化とデバイスの登録解除

ライセンス：任意（Any）

サポートされる防御センター：DC1000、DC1500、DC2000、DC3000、DC3500、DC4000

ハイ アベイラビリティ ペアからいずれかの 防御センター を削除するには、その前に、この 2 つをリンクするハイ アベイラビリティ リンクを無効にする必要があります。

ハイ アベイラビリティ ペアを無効にするには、以下を行います。

アクセス：管理

手順 1　ハイ アベイラビリティ ペアのいずれか一方の 防御センター にログインします。

手順 2　[システム（System）] > [ローカル（Local）] > [登録（Registration）] を選択します。

[登録（Registration）] ページが表示されます。

手順 3　[ハイ アベイラビリティ（High Availability）] をクリックします。

[ハイ アベイラビリティ（High Availability）] ページが表示されます。

手順 4　[登録したデバイスの処理（Handle Registered Devices）] ドロップダウン リストから、以下のいずれかのオプションを選択します。

- このページでアクセスしている 防御センター を使用してすべての管理対象デバイスを制御する場合は、[別のピアのデバイスを登録解除する（Unregister devices on the other peer）] を選択します。
- もう一方の 防御センター を使用してすべての管理対象デバイスを制御する場合は、[このピアのデバイスを登録解除する（Unregister devices on this peer）] を選択します。
- デバイスの管理を完全に停止する場合は、[両方のピアのデバイスを登録解除する（Unregister devices on both peers）] を選択します。

手順 5　[ハイ アベイラビリティを無効にする（Break High Availability）] をクリックします。

「ハイ アベイラビリティを無効にしますか?（Do you really want to Break High Availability?）」というプロンプトに [OK] を選択して応答すると、ハイ アベイラビリティが無効になり、選択したオプションに従って、管理対象デバイスが 防御センター から削除されます。

別の 防御センター を使用してハイ アベイラビリティを有効にできます。この手順については、ハイ アベイラビリティのセットアップ（4-15 ページ）を参照してください。

ペアにされた 防御センター 間での通信の一時停止

ライセンス: 任意（Any）

サポートされる防御センター: DC1000、DC1500、DC2000、DC3000、DC3500、DC4000

一時的にハイ アベイラビリティを無効にする場合は、防御センター 間の通信チャネルを無効にします。

ハイ アベイラビリティ ペアの通信チャネルを無効にするには、以下を行います。

アクセス: 管理

手順 1　[ピア マネージャ（Peer Manager）] をクリックします。

[ピア マネージャ（Peer Manager）] ページが表示されます。

手順 2　2 つの 防御センター 間の通信チャネルを無効にするには、スライダをクリックします。

2 つのアプライアンス間のリモート管理通信を編集する方法については、リモート管理の編集（4-23 ページ）を参照してください。

ペアにされた 防御センター 間での通信の再開

ライセンス: 任意（Any）

サポートされる防御センター: DC1000、DC1500、DC2000、DC3000、DC3500、DC4000

ハイ アベイラビリティを一時的に無効にした場合、防御センター 間の通信チャネルを有効にすることで、ハイ アベイラビリティを再開できます。

ハイ アベイラビリティ ペアの通信チャネルを有効にするには、以下を行います。

アクセス: 管理

手順 1　[ピア マネージャ（Peer Manager）] をクリックします。

[ピア マネージャ（Peer Manager）] ページが表示されます。

手順 2　2 つの 防御センター 間の通信チャネルを有効にするには、スライダをクリックします。

2 つのアプライアンス間のリモート管理通信を編集する方法については、リモート管理の編集（4-23 ページ）を参照してください。

デバイスの操作

ライセンス: 任意（Any）

防御センター を使用して、FireSIGHT システムを構成するさまざまなデバイスを管理できます。デバイスを管理するには、防御センター とデバイスの間に双方向の SSL 暗号化通信チャネルをセットアップします。防御センター はこのチャネルを使用して、ネットワーク トラフィックの分析および管理方法に関する情報をデバイスに送信します。

デバイスはトラフィックを評価すると、イベントを生成し、同じチャネルを使用してそれらのイベントを 防御センター に送信します。

デバイスを管理する方法の詳細については、以下の項を参照してください。

- [デバイス管理（Device Management）] ページについて（4-20 ページ）
- リモート管理の設定（4-21 ページ）
- 防御センター へのデバイスの追加（4-25 ページ）
- リモート管理の設定（4-21 ページ）
- デバイス グループの管理（4-29 ページ）
- デバイスのクラスタリング（4-31 ページ）
- デバイス設定の編集（4-54 ページ）
- センシング インターフェイスの設定（4-66 ページ）

[デバイス管理（Device Management）] ページについて

ライセンス：任意（Any）

[デバイス管理（Device Management）] ページには、登録されたデバイス、デバイス クラスタおよびデバイス グループを管理するために使用できる、一連の情報とオプションが表示されます。このページには、現在 防御センター に登録されているすべてのデバイスのリストが表示されます。

このアプライアンスのリストは、必要に応じて、[ソート基準（sort-by）] ドロップダウン リストを使用してソートできます。アプライアンス リストには、ユーザが選択するカテゴリ別にグループ化されたデバイスが表示されます。以下のソート基準を使用できます。

- グループ（つまり、デバイス グループ）。詳細については、デバイス グループの管理（4-29 ページ）を参照してください。
- タイプ（つまり、デバイスに適用されるライセンスのタイプ）。詳細については、FireSIGHT システム のライセンス（65-1 ページ）を参照してください。
- モデル（つまり、防御センター で管理されているデバイスのモデル）
- 正常性ポリシー。詳細については、ヘルス モニタリングの使用（68-1 ページ）を参照してください。
- システム ポリシー。詳細については、システム ポリシーの管理（63-1 ページ）を参照してください。
- アクセス コントロール ポリシー。詳細についてはアクセス コントロール ポリシーの管理（12-12 ページ）を参照してください。

デバイス グループに属するデバイスのリストは、展開または縮小表示できます。デフォルトでは、このリストは縮小表示されます。

アプライアンス リストの詳細については、以下の表を参照してください。

表 4-1　アプライアンス リストのフィールド

フィールド	説明
名前（Name）	各デバイスのホスト名、IP アドレス、デバイス モデル、およびソフトウェア バージョンのリスト。アプライアンスの左側にあるステータス アイコンが、そのアプライアンスの現在のヘルス ステータスを示します。
ライセンスのタイプ（License Type）	管理対象デバイスで有効なライセンス。
ヘルス ポリシー（Health Policy）	デバイスに現在適用されている正常性ポリシー。正常性ポリシーの名前をクリックすると、そのポリシーの読み取り専用バージョンが表示されます。既存の正常性ポリシーを変更する方法については、正常性ポリシーの編集（68-35 ページ）を参照してください。
システム ポリシー（System Policy）	デバイスに現在適用されているシステム ポリシー。システム ポリシーの名前をクリックすると、そのポリシーの読み取り専用バージョンが表示されます。詳細については、システム ポリシーの管理（63-1 ページ）を参照してください。
アクセス コントロール ポリシー（Access Control Policy）	現在適用されているアクセス コントロール ポリシーへのリンク。アクセス コントロール ポリシーの管理（12-12 ページ）を参照してください。

詳細については、次の各項を参照してください。

- リモート管理の設定（4-21 ページ）
- 防御センター へのデバイスの追加（4-25 ページ）
- デバイス グループの管理（4-29 ページ）
- デバイスのクラスタリング（4-31 ページ）
- スタック構成のデバイスの管理（4-47 ページ）

リモート管理の設定

ライセンス：任意（Any）

ある FireSIGHT システム アプライアンスと別のアプライアンスを相互に管理できるようにするには、その前に、2 つのアプライアンスの間に双方向の SSL 暗号化通信チャネルをセットアップする必要があります。このチャネルを使用して、両方のアプライアンスが設定とイベント情報を共有します。ハイ アベイラビリティ ピアも、このチャネルを使用します。このチャネルは、デフォルトではポート 8305/tcp に位置します。

管理対象のアプライアンス、つまり防御センターで管理するデバイス上には、リモート管理を設定する必要があります。リモート管理を設定した後、管理側アプライアンスの Web インターフェイスを使用して、管理対象アプライアンスを展開環境に追加できます。

この項の手順では、FirePOWER の物理アプライアンス上にリモート管理を設定する方法について説明していることに注意してください。

2 つのアプライアンス間の通信を可能にするためには、アプライアンスが互いを認識する手段を提供しなければなりません。通信を許可するために、FireSIGHT システムでは 3 つの基準を使用します。

- 通信を確立する対象のアプライアンスのホスト名または IP アドレス

  NAT 環境では、ルーティング可能なアドレスがもう一方のアプライアンスにないとしても、リモート管理を設定する際、または管理対象アプライアンスを追加する際には、ホスト名または IP アドレスのいずれかを指定する必要があります。

- 接続を識別するために自己生成される、最大 37 文字の英数字による登録キー
- FireSIGHT システムが NAT 環境で通信を確立するために利用できる、オプションの一意の英数字による NAT ID

  NAT ID は、管理対象アプライアンスを登録するために使用されているすべての NAT ID の間で**一意でなければなりません**。詳細については、NAT 環境での作業（4-8 ページ）を参照してください。

管理対象デバイスを 防御センター に登録する際に、デバイスに適用するアクセス コントロール ポリシーを選択できます。ただし、デバイスがポリシーに準拠していない場合は、ポリシーの適用に失敗します。この不適合には、複数の要因が考えられます。たとえば、ライセンスの不一致、モデルの制限、パッシブとインラインの問題、その他の構成ミスなどです。最初のアクセス コントロール ポリシーの適用が失敗すると、最初のネットワーク ディスカバリ ポリシーの適用も失敗します。障害の原因となる問題を解決した後は、アクセス コントロール ポリシーおよびネットワーク ディスカバリ ポリシーを手動でデバイスに適用する必要があります。アクセス コントロール ポリシーの適用に失敗する原因となる問題の詳細については、アクセス コントロール ポリシーおよびルールのトラブルシューティング（12-25 ページ）を参照してください。

ローカル アプライアンスのリモート管理を設定するには、以下を行います。

アクセス: 管理

手順 1　管理するデバイスの Web インターフェイスで、[システム（System）] > [ローカル（Local）] > [登録（Registration）] を選択します。

[リモート管理（Remote Management）] ページが表示されます。

注意　シスコ では、管理ポートの値を変更しないことを**強く**推奨しています。変更する場合は、展開環境のすべてのアプライアンスで同じ変更を行わなければなりません。それには、アプライアンス間の相互通信が必要になります。詳細については、管理ポートの変更（4-24 ページ）を参照してください。

手順 2　[マネージャの追加（Add Manager）] をクリックします。

[リモート管理の追加（Add Remote Management）] ページが表示されます。

手順 3　[管理ホスト（Management Host）] に、このアプライアンスを管理するために使用するアプライアンスの IP アドレスまたはホスト名を入力します。

ホスト名は、完全修飾ドメイン名またはローカル DNS で有効な IP アドレスに解決される名前です。

NAT 環境では、管理対象アプライアンスを追加する際に IP アドレスまたはホスト名を指定する予定の場合、ここで IP アドレスまたはホスト名を指定する必要はありません。その場合、FireSIGHT システムは後で指定される NAT ID を使用して、管理対象アプライアンスの Web インターフェイス上のリモート マネージャを識別します。

注意　ネットワークで IP アドレスの割り当てに DHCP を使用している場合は、IP アドレスではなく、ホスト名を使用します。

手順 4　[登録キー（Registration Key）] フィールドに、アプライアンス間の通信をセットアップするために使用する登録キーを入力します。

手順 5　NAT 環境の場合は、[固有 NAT ID（Unique NAT ID）] フィールドに、アプライアンス間の通信をセットアップするために使用する、英数字による**一意**の NAT ID を入力します。

手順 6　[保存（Save）] をクリックします。

アプライアンスが相互に通信できることを確認すると、ステータスとして [登録保留（Pending Registration）] が表示されます。

手順 7　管理側アプライアンスの Web インターフェイスを使用して、このアプライアンスを展開環境に追加します。

詳細については、防御センター へのデバイスの追加（4-25 ページ）を参照してください。

（注）　NAT を使用する一部のハイ アベイラビリティ展開では、デバイスのリモート管理を有効にする際に、セカンダリ防御センターをマネージャとして追加しなければならない場合もあります。詳細については、サポートにお問い合わせください。

リモート管理の編集

ライセンス：任意（Any）

管理側アプライアンスのホスト名または IP アドレスを編集するには、以下の手順を使用します。また、管理側アプライアンスの表示名を変更することもできます。表示名は、FireSIGHT システムのコンテキスト内でのみ使用されます。ホスト名をアプライアンスの表示名として使用することもできますが、別の表示名を入力してもホスト名は変更されません。

デバイスが実行しているソフトウェアのバージョンが、防御センター で実行しているソフトウェアのメジャー バージョンより 2 つ以上低い場合、そのデバイスを追加することはできません。たとえば、防御センター がバージョン 5.4.0 を実行している場合、バージョン 5.3.x 以降を実行しているデバイスを追加することはできますが、バージョン 5.2.x を実行しているデバイスは追加できません。

ヒント　スライダをクリックすることで、管理対象デバイスの管理を有効または無効にできます。管理を無効化すると、Defense Center とデバイス間の接続がブロックされますが、Defense Center からデバイスは削除**されません**。デバイスを管理する必要がなくなった場合は、デバイスの削除（4-29 ページ）を参照してください。

リモート管理を編集するには、以下を行います。

アクセス: 管理

手順 1　デバイスの Web インターフェイスで、[システム（System）] > [ローカル（Local）] > [登録（Registration）] を選択します。

[リモート管理（Remote Management）] ページが表示されます。

手順 2　リモート管理設定を編集するマネージャの横にある編集アイコン（ ）をクリックします。

[リモート管理の編集（Edit Remote Management）] ページが表示されます。

手順 3　[名前（Name）] フィールドで、管理側アプライアンスの表示名を変更します。

手順 4　[ホスト（Host）] フィールドで、管理側アプライアンスの IP アドレスまたはホスト名を変更します。

ホスト名は、完全修飾ドメイン名またはローカル DNS で有効な IP アドレスに解決される名前です。

手順 5　[保存（Save）] をクリックします。

変更が保存されます。

管理ポートの変更

ライセンス: 任意（Any）

FireSIGHT システムアプライアンスは、双方向の SSL 暗号化通信チャネルを使用して通信します。このチャネルは、デフォルトではポート 8305 に位置します。

シスコ では、デフォルト設定のままにしておくことを**強く**推奨していますが、管理ポートがネットワーク上の他の通信と競合する場合は、別のポートを選択できます。通常、管理ポートの変更は、FireSIGHT システムのインストール時に行います。

注意　管理ポートを変更する場合は、導入内の相互に通信する必要があるすべてのアプライアンスの管理ポートを変更する必要があります。

管理ポートを変更するには、以下を行います。

アクセス: 管理

手順 1　デバイスの Web インターフェイスで、[システム（System）] > [ローカル（Local）] > [設定（Configuration）] を選択します。

[情報（Information）] ページが表示されます。

手順 2　[ネットワーク（Network）] をクリックします。

[ネットワーク設定（Network Settings）] ページが表示されます。

手順 3　[リモート管理ポート（Remote Management Port）] フィールドに、使用するポート番号を入力します。

手順 4　[保存（Save）] をクリックします。

管理ポートが変更されます。

手順 5　このアプライアンスと通信する必要がある、展開環境内のすべてのアプライアンスについて、この手順を繰り返します。

防御センター へのデバイスの追加

ライセンス: 任意（Any）

デバイスを管理するには、防御センター とデバイスの間に双方向の SSL 暗号化通信チャネルをセットアップします。防御センター はこのチャネルを使用して、ネットワーク トラフィックの分析方法に関する情報をデバイスに送信します。デバイスはトラフィックを評価すると、イベントを生成し、同じチャネルを使用してそれらのイベントを 防御センター に送信します。このチャネルの設定の詳細については、リモート管理の設定（4-21 ページ）を参照してください。

デバイスが実行しているソフトウェアのバージョンが、防御センター で実行しているソフトウェアのメジャー バージョンより 2 つ以上低い場合、そのデバイスを追加することはできません。たとえば、防御センター がバージョン 5.4 を実行している場合、バージョン 5.3.x 以降を実行しているデバイスは追加できますが、バージョン 5.2.x を実行しているデバイスは追加できません。

防御センター でデバイスを管理する前に、そのデバイスでネットワーク設定が正しく設定されていることを確認する必要があります。この確認は、一般にインストール プロセスの一環として行われます。詳細については、管理インターフェイスの構成（64-9 ページ）を参照してください。

IPv4 を使用している 防御センター とデバイスを登録しており、それらを IPv6 に変換する場合は、デバイスをいったん削除してから再登録する必要があります。

管理対象デバイスを 防御センター に登録する際に、デバイスに適用するアクセス コントロール ポリシーを選択できます。ただし、デバイスがポリシーに準拠していない場合は、ポリシーの適用に失敗します。この不適合には、複数の要因が考えられます。たとえば、ライセンスの不一致、モデルの制限、パッシブとインラインの問題、その他の構成ミスなどです。最初のアクセス コントロール ポリシーの適用が失敗すると、最初のネットワーク ディスカバリ ポリシーの適用も失敗します。障害の原因となる問題を解決した後は、アクセス コントロール ポリシーおよびネットワーク ディスカバリ ポリシーを手動でデバイスに適用する必要があります。アクセス コントロール ポリシーの適用に失敗する原因となる問題の詳細については、アクセス コントロール ポリシーおよびルールのトラブルシューティング（12-25 ページ）を参照してください。

デバイス クラスタまたはデバイス スタックを登録するときに、ライセンスを選択することはできますが、それらのライセンスをデバイスの登録時に適用することはできません。これは、ライセンスの不一致による劣化を回避するために、クラスタまたはスタックに適切なライセンスを実行させるための措置です。登録の完了後に、[デバイス管理（Device Management）] ページの一般プロパティ（クラスタの場合）またはスタック プロパティ（スタックの場合）でライセンスを評価できます。詳細については、デバイス クラスタの設定（4-35 ページ）またはデバイス スタックの確立（4-49 ページ）を参照してください。

シリーズ 2 デバイスを登録するときに、ライセンスを選択することはできますが、デバイスの登録時には、選択したライセンスはいずれも適用されません。シリーズ 2 デバイスには、セキュリティ インテリジェンス フィルタリングを除く、Protection 機能が自動的に組み込まれています。これらの機能を無効にすることも、他のライセンスを シリーズ 2 デバイスに適用することもできません。

ヒント　デバイスの詳細な設定を変更するには、デバイスの横にある編集アイコン（  ）をクリックします。詳細については、デバイス設定の編集（4-54 ページ）とセンシング インターフェイスの設定（4-66 ページ）を参照してください。

デバイスを 防御センター に追加するには、以下を行います。

アクセス：Admin/Network Admin

手順 1　デバイスを 防御センター の管理対象として設定します。

FirePOWER デバイスの場合は、リモート管理の設定（4-21 ページ）で説明している手順を使用します。デバイスが 防御センター との通信を確認すると、ステータスが [登録の保留（Pending Registration）] として表示されます。

仮想デバイス、Blue Coat X-Series 向け Cisco NGIPS、および ASA FirePOWER デバイスの場合は、デバイスのコマンド ライン インターフェイス（CLI）を使用してリモート管理を設定します。

（注）　ネットワーク アドレス変換（NAT）が使用される一部のハイ アベイラビリティ展開では、セカンダリ 防御センター をマネージャとして追加しなければならない場合もあります。詳細については、サポートにお問い合わせください。

手順 2　防御センター の Web インターフェイスで、[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 3　[追加（Add）] ドロップダウン メニューから、[デバイスの追加（Add Device）] を選択します。

[デバイスの追加（Add Device）] ポップアップ ウィンドウが表示されます。

手順 4　[ホスト（Host）] フィールドに、追加するデバイスの IP アドレスまたはホスト名を入力します。

デバイスのホスト名は、完全修飾ドメイン名またはローカル DNS で有効な IP アドレスに解決される名前です。

NAT 環境では、防御センター の管理対象としてデバイスを設定するときに 防御センター の IP アドレスまたはホスト名をすでに指定している場合、デバイスの IP アドレスまたはホスト名を指定する必要はありません。詳細については、NAT 環境での作業（4-8 ページ）を参照してください。

注意　ネットワークで IP アドレスの割り当てに DHCP を使用している場合は、IP アドレスではなく、ホスト名を使用します。

手順 5　[登録キー（Registration Key）] フィールドに、防御センター の管理対象としてデバイスを設定したときに使用したのと同じ登録キーを入力します。

手順 6　（任意）[グループ（Group）] ドロップダウン リストからデバイス グループを選択し、そのグループにデバイスを追加します。

デバイス グループの詳細については、デバイス グループの管理（4-29 ページ）を参照してください。

手順 7　[アクセス コントロール ポリシー（Access Control Policy）] ドロップダウン リストから、デバイスに適用する初期ポリシーを選択します。

- [デフォルト アクセス コントロール（Default Access Control）] ポリシーは、すべてのトラフィックをネットワークからブロックします。
- [デフォルト侵入防御（Default Intrusion Prevention）] ポリシーは、Balanced Security and Connectivity 侵入ポリシーにも合格したすべてのトラフィックを許可します。
- [デフォルト ネットワーク検出（Default Network Discovery）] ポリシーは、すべてのトラフィックを許可し、ネットワーク検出のみでトラフィックを検査します。
- 既存のユーザ定義アクセス コントロール ポリシーを選択することもできます。

詳細については、アクセス コントロール ポリシーの管理（12-12 ページ）を参照してください。

手順 8　デバイスに適用するライセンスを選択します。次の点に注意してください。

- Control、Malware、および URL フィルタリング（URL Filtering）ライセンスには、Protection ライセンスが必要です。
- VPN ライセンスは、仮想デバイス、Blue Coat X-Series 向け Cisco NGIPS、または ASA FirePOWER デバイスで有効にすることはできません。
- Blue Coat X-Series 向け Cisco NGIPS では、Control ライセンスを有効にできません。
- 仮想デバイスや ASA FirePOWER デバイスでは Control ライセンスを有効にすることができますが、これらのデバイスは高速パス ルール、スイッチング、ルーティング、スタック構成、クラスタリングを**サポートしていません**。
- クラスタを構成するデバイスでのライセンス設定を変更することはできません。
- スタック構成のデバイスの場合、アプライアンス エディタの [スタック（Stack）] ページで、スタックに対してラインセンスを有効または無効にします。
- シリーズ 2 デバイスを登録する場合、デバイスの登録時に、選択したライセンスはいずれも適用されません。シリーズ 2 デバイスには、セキュリティ インテリジェンス フィルタリングを除く、Protection 機能が自動的に組み込まれています。これらの機能を無効にすることも、他のライセンスを シリーズ 2 デバイスに適用することもできません。

詳細については、FireSIGHT システム のライセンス（65-1 ページ）を参照してください。

手順 9　デバイスを 防御センターの管理対象として設定するときに、NAT ID を使用してデバイスを識別した場合は、[詳細（Advanced）] セクションを展開して、[一意の NAT ID（Unique NAT ID）] フィールドに同じ NAT ID を入力します。

手順 10　デバイスに 防御センター へのパケット転送を許可するには、[パケットの転送（Transfer Packets）] チェックボックスをオンにします。

このオプションは、デフォルトで有効です。無効にすると、防御センター へのパケット転送が完全に禁止されます。

手順 11　[登録（Register）] をクリックします。

デバイスが 防御センター に追加されます。防御センター がデバイスのハートビートを確認して通信を確立するまでに、最大 2 分かかる場合があります。

デバイスへの変更の適用

ライセンス：任意（Any）

デバイス、デバイス クラスタ、またはデバイス スタックの設定に変更を加えた後、それらの変更を適用するまでは、システム全体に変更が反映されません。デバイスが変更適用前の状態でなければ、このオプションは無効になります。

ヒント　デバイスに変更を適用するには、[デバイス管理（Device Management）] ページまたはアプライアンス エディタの [インターフェイス（Interfaces）] タブを使用します。

変更をデバイスに適用するには、以下を行います。

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　変更を適用するデバイスの横にある適用アイコン（  ）をクリックします。

手順 3　プロンプトが出されたら、[適用（Apply）] をクリックします。

デバイスの変更が適用されます。

ヒント　必要に応じて、[デバイス変更の適用（Apply Device Changes）] ダイアログ ボックスで [変更の表示（View Changes）] をクリックします。新しいブラウザ ウィンドウに [デバイス管理のリビジョン比較レポート（Device Management Revision Comparison Report）] ページが表示されます。詳細については、デバイス管理のリビジョン比較レポートの使用（4-28 ページ）を参照してください。

手順 4　[OK] をクリックします。

[デバイス管理（Device Management）] ページに戻ります。

デバイス管理のリビジョン比較レポートの使用

ライセンス：任意（Any）

デバイス管理の比較レポートを使用して、変更を確認してから、アプライアンスに適用できます。このレポートには、現在のアプライアンスの設定と、変更適用後のアプライアンスの設定との間の差異がすべて表示されます。これにより、設定の潜在的なエラーを検出することができます。

変更適用前と適用後のアプライアンスを比較するには、以下を行います。

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　変更を適用するアプライアンスの横にある適用アイコン（  ）をクリックします。

[デバイス変更の適用（Apply Device Changes）] ポップアップ ウィンドウが表示されます。アプライアンスが変更適用前の状態でなければ、適用アイコンは無効になります。

手順 3　[変更の表示（View Changes）] をクリックします。

新しいウィンドウに [デバイス管理のレビジョン比較レポート（Device Management Revision Comparison Report）] ページが表示されます。

手順 4　[前へ（Previous）] と [次へ（Next）] をクリックして、現在のアプライアンスの設定と変更適用後のアプライアンスの設定との間のすべての差異を確認します。

手順 5　必要に応じて、レポートの PDF バージョンを生成するには、[比較レポート（Comparison Report）] をクリックします。

デバイスの削除

ライセンス：任意（Any）

デバイスを管理する必要がなくなった場合、防御センター からそのデバイスを削除できます。デバイスを削除すると、防御センター とそのデバイスとの間のすべての通信が切断されます。後日、削除したデバイスを再び管理するには、もう一度そのデバイスを 防御センター に追加する必要があります。

（注） ハイ アベイラビリティ ペアとして設定された 防御センター からデバイスを削除し、そのデバイスを再び追加する場合、シスコでは、削除してから追加するまでに少なくとも 5 分間待つことを推奨しています。この間隔を空けることにより、ハイ アベイラビリティ ペアが確実に再同期して、両方の 防御センター が削除を認識します。5 分間待たないと、1 回の同期サイクルでは、デバイスが両方の 防御センター に追加されない場合があります。

デバイスを 防御センター から削除するには、以下を行います。

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　削除するデバイスの横にある削除アイコン（ ）をクリックします。

プロンプトが表示されたら、デバイスを削除することを確認します。デバイスと 防御センター の間の通信が切断され、[デバイス管理（Device Management）] ページからデバイスが削除されます。デバイスに設定されているシステム ポリシーによって、デバイスが NTP を介して 防御センター から時間を受信する場合は、デバイスはローカル時間管理に戻ります。

デバイス グループの管理

ライセンス：任意（Any）

防御センター でデバイスをグループ化すると、複数のデバイスへのポリシーの適用やアップデートのインストールを簡単に行えます。グループに属するデバイスのリストは、展開または縮小表示できます。デフォルトでは、このリストは縮小表示されます。

詳細については、次の各項を参照してください。

- デバイス グループの追加（4-29 ページ）
- デバイス グループの編集（4-30 ページ）
- デバイス グループの削除（4-31 ページ）

デバイス グループの追加

ライセンス：任意（Any）

以下の手順では、デバイス グループを追加して、複数のデバイスへのポリシーの適用やアップデートのインストールを簡単に行う方法について説明します。

スタック内またはクラスタ内のプライマリ デバイスをグループに追加すると、両方のデバイスがグループに追加されます。デバイスのスタック構成またはクラスタ構成を解除しても、これらのデバイスは両方ともグループに属したままになります。

デバイス グループを作成してグループにデバイスを追加するには、以下を行います。

アクセス: Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　[追加（Add）] ドロップダウン メニューから、[グループの追加（Add Group）] を選択します。

[グループの追加（Add Group）] ポップアップ ウィンドウが表示されます。

手順 3　[名前（Name）] フィールドに、グループの名前を入力します。

手順 4　[使用可能なデバイス（Available Devices）] から、デバイス グループに追加するアプライアンスを 1 つ以上選択します。複数のアプライアンスを選択するには、Ctrl キーまたは Shift キーを押しながらクリックします。

手順 5　[追加（Add）] をクリックして、選択したアプライアンスをデバイス グループに追加します。

手順 6　[OK] をクリックします。

デバイス グループが追加されます。

デバイス グループの編集

ライセンス: 任意（Any）

任意のデバイス グループに含まれるデバイス一式を変更できます。アプライアンスが現在グループに属している場合は、現在のグループから削除してからでないと、アプライアンスを新しいグループに追加することはできません。

アプライアンスを新しいグループに移動しても、そのアプライアンスのポリシーが、新しいグループにすでに適用されているポリシーに変更されるわけではありません。デバイスのポリシーを変更するには、新しいポリシーをデバイスまたはデバイス グループに適用する必要があります。

スタック内またはクラスタ内のプライマリ デバイスをグループに追加すると、両方のデバイスがグループに追加されます。デバイスのスタック構成またはクラスタ構成を解除しても、これらのデバイスは両方ともグループに属したままになります。

デバイス グループを編集するには、以下を行います。

アクセス: Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　編集するデバイス グループの横にある編集アイコン（）をクリックします。

[グループの編集（Edit Group）] ポップアップ ウィンドウが表示されます。

手順 3　必要に応じて、[名前（Name）] フィールドに、グループの新しい名前を入力します。

手順 4　[使用可能なデバイス（Available Devices）] から、デバイス グループに追加するアプライアンスを 1 つ以上選択します。複数のアプライアンスを選択するには、Ctrl キーまたは Shift キーを押しながらクリックします。

手順 5　[追加（Add）] をクリックして、選択したアプライアンスをデバイス グループに追加します。

手順 6　選択したアプライアンスをデバイス グループから削除するには、削除アイコン（ ）をクリックします。

手順 7　[OK] をクリックします。

デバイス グループの変更が保存されます。

デバイス グループの削除

ライセンス：任意（Any）

デバイスが含まれているデバイス グループを削除すると、それらのデバイスは [デバイス管理（Device Management）] ページの [グループ解除（Ungrouped）] カテゴリに移動されます。防御センター からは削除されません。

デバイス グループを削除するには、以下を行います。

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　削除するデバイス グループの横にある削除アイコン（ ）をクリックします。

手順 3　プロンプトが表示されたら、デバイス グループを削除することを確認します。

デバイス グループが削除されます。

デバイスのクラスタリング

ライセンス：Control

サポートされるデバイス：シリーズ 3

デバイスのクラスタリング（デバイスのハイ アベイラビリティとも呼ばれます）を利用することで、2 つのピア デバイス間または 2 つのデバイス スタック間のネットワーキング機能と設定データの冗長性を確立できます。デバイス スタックを構成する方法の詳細については、スタック構成のデバイスの管理（4-47 ページ）を参照してください。

2 つのピア デバイスまたは 2 つのピア デバイス スタックでクラスタを構成し、そのクラスタを単一の論理システムとして、ポリシーの適用、システムの更新、および登録を行うことで、構成の冗長性を確立できます。その他の設定データは、システムによって自動的に同期されます。

クラスタリングの要件

デバイス クラスタを設定するには、両方のデバイスまたは両方のデバイス スタックのプライマリ メンバーが同じモデルであり、同一の銅線またはファイバ インターフェイスを備えていなければなりません。両方のデバイスまたはデバイス スタックが同じソフトウェアを実行し、同じライセンスが有効になっていることも要件となります。デバイス スタックのハードウェア構成は同一でなければなりませんが、インストール済みのマルウェア ストレージ パックについてはその限りではありません。たとえば、3D8290 と 3D8290 でクラスタを構成する場合、一方のスタックに、マルウェア ストレージ パックがインストールされているデバイスがなくても、あるいは 1 つまたはすべてのデバイスにマルウェア ストレージ パックがインストールされていても構いません。デバイスが NAT ポリシーのターゲットとなっている場合、両方のピアに同じ NAT ポリシーを適用する必要があります。デバイス クラスタを構成した後は、クラスタを構成する個々のデバイスのライセンス オプションを変更することはできませんが、クラスタ全体のライセンスは変更できます。詳細については、デバイス クラスタの設定（4-35 ページ）を参照してください。

注意　シスコから供給されたハード ドライブ以外はデバイスに取り付けないでください。サポートされていないハード ドライブを取り付けると、デバイスが破損する可能性があります。マルウェア ストレージ パック キットは、シスコから**のみ**購入でき、8000 シリーズ デバイスで**のみ**使用できます。マルウェア ストレージ パックのサポートが必要な場合は、サポートにお問い合わせください。詳細については、『*FireSIGHT システム Malware Storage Pack Guide*』を参照してください。

クラスタリングのフェールオーバーおよびメンテナンス モード

デバイス クラスタのフェールオーバーは、手動または自動で行われます。手動でフェールオーバーをトリガーするには、クラスタを構成するデバイスまたはスタックのいずれかをメンテナンス モードで開始します。メンテナンス モードの詳細については、クラスタを構成するデバイスのメンテナンス モードの開始（4-40 ページ）を参照してください。

自動フェールオーバーは、アクティブ デバイスまたはアクティブ スタックの正常性が損なわれた場合、システム更新中、または管理者権限のあるユーザがデバイスをシャットダウンした後に発生します。また、自動フェールオーバーは、アクティブ デバイスまたはデバイス スタックで NMSB 障害、NFE 障害、ハードウェア障害、ファームウェア障害、重大なプロセス障害、ディスクフル状態、または 2 つのスタック構成デバイス間のリンク障害が起きた場合にも発生します。バックアップ デバイスまたはバックアップ スタックの正常性が同じように損なわれている場合は、フェールオーバーは行われず、クラスタはデグレード状態になります。また、いずれかのデバイスまたはデバイス スタックがメンテナンス モードになっている場合も、フェールオーバーは行われません。アクティブ スタックからスタック ケーブルを切断すると、そのスタックはメンテナンス モードに入ることに注意してください。アクティブ スタックのセカンダリ デバイスをシャットダウンした場合も、スタックはメンテナンス モードに入ります。

（注）　アクティブ クラスタのメンバーがメンテナンス モードになり、アクティブ ロールが他のクラスタ メンバーにフェールオーバーされた場合、元のアクティブ クラスタのメンバーは、通常動作に復帰したときに自動的にアクティブ ロールを再要求しません。

ポリシーおよび更新の適用

ポリシーを適用する際には、個々のデバイスやデバイス スタックではなく、デバイス クラスタにポリシーを適用します。ポリシーの適用が失敗すると、システムはいずれのデバイスまたはスタックにもポリシーを適用しません。ポリシーは最初にアクティブ デバイスまたはスタックに適用されてから、バックアップに適用されます。したがって、クラスタでは常に、ピアのいずれかがネットワーク トラフィックを処理しています。

注意　ポリシーを適用した場合、リソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。さらに、構成の一部を適用するときに、Snort プロセスの再開が要求され、これにより一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。7010、7020、および 7030 の管理対象デバイスでは、設定変更の展開に最大 5 分かかる場合があります。Snort プロセスを再開する構成（1-8 ページ）および Snort の再開によるトラフィックへの影響（1-9 ページ）を参照してください。

更新は、個々のデバイスやスタックが受信するのではなく、クラスタを構成するデバイスが単一のエンティティとして受信します。更新が開始されると、システムは最初にバックアップ デバイスまたはスタックに更新を適用します。それによって、バックアップ デバイスまたはスタックはメンテナンス モードに入ります。この状態は、必要なプロセスが再開してデバイスがトラフィックの処理を再び開始するまで維持されます。次にシステムはアクティブなデバイスまたはスタックに更新を適用し、同じプロセスに従います。

デバイス クラスタなしの冗長性の確立

ほとんどの場合には、Cisco Redundancy Protocol（SFRP）を使用することによって、デバイスをクラスタリングせずにレイヤ 3 の冗長性を実現できます。SFRP では、指定した IP アドレスに対する冗長なゲートウェイとしてデバイスを機能させることができます。ネットワークの冗長性では、2 つのデバイスまたは 2 つのスタックが同一のネットワーク接続を提供するように設定することで、ネットワーク上の他のホストに対する接続を維持できます。SFRP の詳細については、SFRP の設定（7-9 ページ）を参照してください。

デバイスのハイ アベイラビリティを設定する方法は、FireSIGHT システム展開（パッシブ、インライン、ルーテッド、またはスイッチド）に応じて決定します。同時に複数のロールでシステムを展開することもできます。4 つの展開タイプのうち、冗長性をもたらすためにデバイスまたはスタックのクラスタリングが必要になるのは、パッシブ展開のみです。他の展開タイプでは、デバイス クラスタを使用しても使用しなくてもネットワークの冗長性を確立できます。以下の項で、各タイプの展開でのハイ アベイラビリティの概要を説明します。

パッシブ展開での冗長性

一般に、パッシブ インターフェイスは中央スイッチのタップ ポートに接続されます。この場合、スイッチを通過するトラフィックのすべてを、パッシブ インターフェイスで分析することが可能になります。複数のデバイスが同じタップ フィードに接続されている場合、システムはそれぞれのデバイスからイベントを生成します。クラスタを構成するデバイスはアクティブまたはバックアップのいずれかとして機能するため、システムはシステム障害が発生したとしてもトラフィックを分析できると同時に、重複するイベントを防止できます。

インライン展開での冗長性

インライン セットは、自身を通過するパケットのルーティングを制御できないため、展開環境で常にアクティブになっていなければなりません。したがって、冗長性を確立できるかどうかは、外部システムがトラフィックを適切にルーティングするかどうかに依存します。冗長インライン セットは、デバイス クラスタを使用しても使用しなくても設定できます。

冗長インライン セットを展開するには、循環ルーティングを防止する一方で、トラフィックがインラインセットのいずれか 1 つだけを通過できるようにネットワーク トポロジを設定します。インライン セットのいずれかで障害が発生すると、周辺ネットワークインフラストラクチャがゲートウェイ アドレスへの接続が切断されたことを検出し、ルートを調整して冗長セット経由でトラフィックを送信します。

ルーテッド展開での冗長性

IP ネットワーク内のホストは、既知のゲートウェイ アドレスを使用してトラフィックをさまざまなネットワークに送信する必要があります。ルーテッド展開で冗長性を確立するには、ルーテッド インターフェイスがゲートウェイ アドレスを共有し、そのアドレスに対するトラフィックを常に 1 つのインターフェイスだけが処理するようにしなければなりません。そのためには、仮想ルータで同じ数の IP アドレスを維持する必要があります。1 つのインターフェイスがアドレスをアドバタイズします。そのインターフェイスがダウンすると、バックアップ インターフェイスがアドレスのアドバタイジングを開始します。

クラスタに含まれていないデバイスの場合は、SFRP を使用して、複数のルーテッド インターフェイス間で共有されるゲートウェイ IP アドレスを設定することで、冗長性を確立します。SFRP は、デバイス クラスタを使用しても使用しなくても設定できます。また、OSPF や RIP などのダイナミック ルーティングを使用して冗長性を確立することもできます。

スイッチド展開での冗長性

スイッチド展開では、スパニング ツリー プロトコル（STP）を使用して冗長性を確立します。STP は、ブリッジ型ネットワーク トポロジを管理するプロトコルです。このプロトコルは、バックアップ リンクを設定することなく、冗長リンクでスイッチド インターフェイスの自動バックアップを行えるように設計されています。スイッチド展開でのデバイスは、STP に依存して、冗長インターフェイス間のトラフィックを管理します。同じブロードキャスト ネットワークに接続されている 2 つのデバイスは、STP によって計算されたトポロジに基づいてトラフィックを受信します。STP を有効にする方法の詳細については、仮想スイッチの詳細設定（6-8 ページ）を参照してください。

（注） デバイス クラスタに展開される予定の仮想スイッチを設定する際には、STP を有効にするよう、シスコ は強く推奨します。

デバイスおよびスタックのクラスタリングの詳細については、以下の項を参照してください。

- デバイス クラスタの設定（4-35 ページ）
- デバイス クラスタの編集（4-36 ページ）
- クラスタ内の個々のデバイスの設定（4-37 ページ）
- クラスタ内の個々のデバイス スタックの設定（4-38 ページ）
- クラスタを構成するデバイスでのインターフェイスの設定（4-38 ページ）
- クラスタ内のアクティブ ピアの切り替え（4-39 ページ）
- クラスタを構成するデバイスのメンテナンス モードの開始（4-40 ページ）
- クラスタを構成するスタック内のデバイスの交換（4-40 ページ）
- クラスタ状態共有の設定（4-41 ページ）
- クラスタ状態共有のトラブルシューティング（4-43 ページ）
- クラスタを構成するデバイスの分離（4-46 ページ）
- SFRP の設定（7-9 ページ）
- HA リンク インターフェイスの設定（4-69 ページ）

デバイス クラスタの設定

ライセンス: Control

サポートされるデバイス: シリーズ 3

デバイス クラスタを確立する前に、以下の前提条件を満たす必要があります。

- 各デバイスまたはスタック内の各プライマリ デバイスにインターフェイスを設定します。
- クラスタに含める各デバイスまたはデバイス スタック内のプライマリ メンバーは、同じモデルであり、同一の銅線またはファイバ インターフェイスを備えている必要があります。
- 両方のデバイスまたはデバイス スタックが正常なヘルス ステータスであり、同じソフトウェアを実行し、同じライセンスが有効になっている必要があります。詳細については、ヘルス モニタの使用（68-46 ページ）を参照してください。特に、デバイスでのハードウェア障害は許容されません。ハードウェア障害が発生すると、デバイスがメンテナンス モードに入り、フェールオーバーがトリガーされます。
- デバイスとスタックを混在させてクラスタを構成することはできません。単一のデバイスと単一のデバイスでクラスタを構成するか、ハードウェア構成が同じ（ただし、マルウェア ストレージ パックの有無を除く）デバイス スタックとデバイス スタックでクラスタを構成する必要があります。たとえば、3D8290 と 3D8290 でクラスタを構成する場合、一方のスタックに、マルウェア ストレージ パックがインストールされているデバイスがなくても、あるいは 1 つまたはすべてのデバイスにマルウェア ストレージ パックがインストールされていても構いません。マルウェア ストレージ パックの詳細については、『*FireSIGHT システム Malware Storage Pack Guide*』を参照してください。

注意　シスコから供給されたハード ドライブ以外はデバイスに取り付けないでください。サポートされていないハード ドライブを取り付けると、デバイスが破損する可能性があります。マルウェア ストレージ パック キットは、シスコから**のみ**購入でき、8000 シリーズ デバイスで**のみ**使用できます。マルウェア ストレージ パックのサポートが必要な場合は、サポートにお問い合わせください。詳細については、『*FireSIGHT システム Malware Storage Pack Guide*』を参照してください。

- デバイスが NAT ポリシーのターゲットとなっている場合、両方のピアに同じ NAT ポリシーを適用する必要があります。

デバイス クラスタを確立する際には、デバイスまたはスタックのうちの一方をアクティブとして指定し、もう一方をバックアップとして指定します。システムは、マージした設定を、クラスタを構成するデバイスに適用します。競合が存在する場合、システムはアクティブとして指定されたデバイスまたはスタックの設定を適用します。

デバイス クラスタを構成した後は、クラスタを構成する個々のデバイスのライセンス オプションを変更することはできませんが、クラスタ全体のライセンスは変更できます。詳細については、デバイス クラスタの編集（4-36 ページ）を参照してください。スイッチド インターフェイスまたはルーテッド インターフェイスで設定しなければならないインターフェイス属性がある場合、システムはクラスタを確立しますが、そのステータスを保留中に設定します。ユーザが必要な属性を設定した後、システムはデバイス クラスタを完成させて、正常なステータスに設定します。

クラスタを構成するペアを確立すると、ピア デバイスまたはスタックは、[デバイス管理（Device Management）] ページで単一のデバイスとして扱われます。デバイス クラスタには、アプライアンスのリストでクラスタ アイコン（ ）が表示されます。ユーザが行った設定変更は、いずれもクラスタを構成するデバイスの間で同期されます。[デバイス管理（Device Management）] ページには、クラスタ内のどのデバイスまたはスタックがアクティブであるかが表示されます。アクティブなデバイスまたはスタックは、手動または自動フェールオーバーが発生すると変更されます。手動フェールオーバーの詳細については、クラスタを構成するデバイスのメンテナンス モードの開始（4-40 ページ）を参照してください。

デバイス クラスタの登録を 防御センター から削除すると、その登録は両方のデバイスまたはスタックから削除されます。デバイス クラスタを 防御センター から削除する方法は、個々の管理対象デバイスを削除する場合の方法と同じです。詳細については、デバイスの削除（4-29 ページ）を参照してください。

登録が削除されたクラスタは、別の 防御センター に登録できます。クラスタを構成する単一のデバイスを登録するには、クラスタ内のアクティブ デバイスにリモート管理を追加してから、そのデバイスを 防御センター に追加します。これにより、クラスタ全体が追加されます。クラスタ化されたスタック構成のデバイスを登録するには、いずれかのスタックのプライマリ デバイスにリモート管理を追加してから、そのデバイスを 防御センター に追加します。これにより、クラスタ全体が追加されます。詳細については、防御センター へのデバイスの追加（4-25 ページ）を参照してください。

デバイス クラスタを確立した後、HA リンク インターフェイスの設定（4-69 ページ）で説明している手順に従って、ハイ アベイラビリティ リンク インターフェイスを設定できます。

デバイスまたはデバイス スタックでクラスタを構成するには、以下を行います。

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　[追加（Add）] ドロップダウン メニューから、[クラスタの追加（Add Cluster）] を選択します。

[クラスタの追加（Add Cluster）] ポップアップ ウィンドウが表示されます。

手順 3　[名前（Name）] フィールドに、クラスタの名前を入力します。

英数字と特殊文字を入力できます。ただし、+、(、)、{、}、#、&、\、<、>、?、‘、および “ の文字は無効です。

手順 4　[アクティブ（Active）] で、クラスタのアクティブ デバイスまたはスタックを選択します。

手順 5　[バックアップ（Backup）] で、クラスタのバックアップ デバイスまたはスタックを選択します。

手順 6　[クラスタ（Cluster）] をクリックします。

デバイス クラスタが追加されます。このプロセスではシステム データの同期が行われるため、プロセスが完了するまでに数分かかります。

デバイス クラスタの編集

ライセンス：Control

サポートされるデバイス：シリーズ 3

デバイス クラスタを確立した後は、デバイスの設定を変更すると、通常はクラスタ全体の設定も変更されます。

[一般（General）] セクションのステータス アイコンにマウスのポインタを合わせると、クラスタのステータスが表示されます。また、クラスタ内のデバイスまたはスタックのどれがアクティブ ピアで、どれがバックアップ ピアであるかも確認できます。

詳細については、次の各項を参照してください。

- 一般的なデバイス設定の編集（4-54 ページ）
- デバイス ライセンスの有効化と無効化（4-55 ページ）

- クラスタ状態共有の設定（4-41 ページ）
- 詳細なデバイス設定の編集（4-61 ページ）

デバイス クラスタを編集するには、以下を行います。

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　設定を編集するデバイス クラスタの横にある編集アイコン（）をクリックします。

[クラスタ（Cluster）] ページが表示されます。

手順 3　[クラスタ（Cluster）] ページのセクションを使用して、単一のデバイス設定を変更する場合と同じように、クラスタ構成の設定を変更します。

クラスタ内の個々のデバイスの設定

ライセンス：Control

サポートされるデバイス：シリーズ 3

デバイス クラスタを確立した後でも、クラスタ内の個々のデバイスに対して設定できる属性がいくつかあります。クラスタを構成するデバイスに変更を加える方法は、単一のデバイスに変更を加える場合の方法と同じです。

詳細については、次の各項を参照してください。

- 一般的なデバイス設定の編集（4-54 ページ）
- デバイス システム設定の編集（4-56 ページ）
- デバイスのヘルスの確認（4-58 ページ）
- デバイス管理設定の編集（4-58 ページ）

クラスタ内の個々のデバイスを設定するには、以下を行います。

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　設定を編集するデバイス クラスタの横にある編集アイコン（）をクリックします。

[クラスタ（Cluster）] ページが表示されます。

手順 3　[デバイス（Devices）] をクリックします。

[デバイス（Devices）] ページが表示されます。

手順 4　[選択されたデバイス（Selected Device）] ドロップダウン リストから、変更するデバイスを選択します。

手順 5　[デバイス（Devices）] ページのセクションを使用して、単一のデバイスに対して変更を加える場合と同じように、クラスタを構成する個々のデバイスに変更を加えます。

クラスタ内の個々のデバイス スタックの設定

ライセンス：Control

サポートされるデバイス：シリーズ 3

スタック構成のデバイスのペアでクラスタを構成した後は、編集可能なスタック属性が制限されます。クラスタを構成するスタックの名前は編集できます。また、クラスタを構成するデバイスでのインターフェイスの設定（4-38 ページ）で説明している手順に従って、スタックのネットワーク構成を編集できます。

クラスタ内のスタックの名前を編集するには、以下を行います。

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　設定を編集するデバイス クラスタの横にある編集アイコン（ ）をクリックします。

[クラスタ（Cluster）] ページが表示されます。

手順 3　[スタック（Stacks）] をクリックします。

[スタック（Stacks）] ページが表示されます。

[選択されたデバイス（Selected Device）] ドロップダウン リストから、変更するスタックを選択します。

手順 4　[一般（General）] セクションの横にある編集アイコン（ ）をクリックします。

[一般（General）] ポップアップ ウィンドウが表示されます。

手順 5　[名前（Name）] フィールドに、スタックに割り当てる新しい名前を入力します。

英数字と特殊文字を入力できます。ただし、+、(、)、{、}、#、&、\、<、>、?、‘、および “ の文字は無効です。

手順 6　[保存（Save）] をクリックします。

新しい名前が保存されます。スタック設定を適用するまでは、変更は反映されません。詳細については、デバイスへの変更の適用（4-27 ページ）を参照してください。

クラスタを構成するデバイスでのインターフェイスの設定

ライセンス：Control

サポートされるデバイス：シリーズ 3

クラスタ内の個々のデバイスに、インターフェイスを設定できます。ただし、その場合には、クラスタ内のピア デバイスにも同等のインターフェイスを設定する必要があります。クラスタを構成するスタックの場合は、スタックのプライマリ デバイスのそれぞれに、同じインターフェイスを設定する必要があります。仮想ルータを設定するときに、その仮想ルータを設定するスタックを選択します。詳細については、仮想ルータの設定（7-10 ページ）を参照してください。

クラスタを構成するデバイスの [インターフェイス（Interfaces）] ページに、個々のデバイスのハードウェアおよびインターフェイスのビューが含まれています。詳細については、センシング インターフェイスの設定（4-66 ページ）を参照してください。

クラスタを構成するデバイスにインターフェイスを設定するには、以下を行います。

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　インターフェイスを設定するデバイス クラスタの横にある編集アイコン（）をクリックします。

[クラスタ（Cluster）] ページが表示されます。

手順 3　[インターフェイス（Interfaces）] をクリックします。

[インターフェイス（Interfaces）] ページが表示されます。

手順 4　[選択されたデバイス（Selected Device）] ドロップダウン リストから、変更するデバイスを選択します。

手順 5　個々のデバイスに設定する場合と同じようにインターフェイスを設定します。詳細については、センシング インターフェイスの設定（4-66 ページ）を参照してください。

クラスタ内のアクティブ ピアの切り替え

ライセンス：Control

サポートされるデバイス：シリーズ 3

デバイス クラスタを確立した後、アクティブなピア デバイスまたはスタックをバックアップに、またはその逆に手動で切り替えることができます。

クラスタ内のアクティブ ピアを切り替えるには、以下を行います。

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　アクティブ ピアを変更するデバイス クラスタの横にある、アクティブ ピア切り替えアイコン（）をクリックします。

[アクティブ ピアの切り替え（Switch Active Peer）] ポップアップ ウィンドウが表示されます。

手順 3　クラスタ内のバックアップ デバイスを即時にアクティブ デバイスに切り替える場合は、[はい（Yes）] をクリックします。キャンセルして [デバイス管理（Device Management）] ページに戻る場合は、[いいえ（No）] をクリックします。

クラスタを構成するデバイスのメンテナンス モードの開始

ライセンス：Control

サポートされるデバイス：シリーズ 3

クラスタを確立した後に、デバイスのメンテナンスを行うために手動でフェールオーバーをトリガーするには、クラスタを構成するデバイスまたはスタックをメンテナンス モードに切り替えます。メンテナンス モードでは、システムが管理上、管理インターフェイスを除くすべてのインターフェイスをダウンさせます。メンテナンスの完了後、デバイスを再び有効にして、通常の動作を再開できます。

（注） クラスタの両方のメンバーを同時にメンテナンス モードにしないでください。これを行うと、そのクラスタでトラフィックを検査できなくなります。

クラスタを構成するデバイスでメンテナンス モードを開始するには、以下を行います。

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　クラスタを構成するデバイスのうち、メンテナンス モードを開始するデバイスの横にあるメンテナンス モード切り替えアイコン（）をクリックします。

[メンテナンス モードの確認（Confirm Maintenance Mode）] ポップアップ ウィンドウが表示されます。

手順 3　[はい（Yes）] をクリックしてメンテナンス モードを確認するか、[いいえ（No）] をクリックしてキャンセルします。

手順 4　メンテナンス モード切り替えアイコン（）を再度クリックすると、デバイスのメンテナンス モードが終了します。

クラスタを構成するスタック内のデバイスの交換

ライセンス：Control

サポートされるデバイス：シリーズ 3

クラスタのメンバーとなっているスタックをメンテナンス モードに切り替えた後、スタック内のセカンダリ デバイスを別のデバイスと交換できます。この場合、選択できるデバイスは、現在スタックのメンバーにも、クラスタのメンバーにもなっていないデバイスのみです。新しいデバイスは、デバイス スタックを確立する場合と同じガイドラインに従っている必要があります。デバイス スタックの確立（4-49 ページ）を参照してください。

クラスタを構成するスタック内のデバイスを交換するには、以下を行います。

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　メンテナンス モードを開始するスタック メンバーの横にあるメンテナンス モード切り替えアイコン（）をクリックします。

[メンテナンス モードの確認（Confirm Maintenance Mode）] ポップアップ ウィンドウが表示されます。

手順 3　[はい（Yes）] をクリックしてメンテナンス モードを確認するか、[いいえ（No）] をクリックしてキャンセルします。

手順 4　デバイス交換アイコン（）をクリックします。

[デバイスの交換（Replace Device）] ポップアップ ウィンドウが表示されます。

手順 5　ドロップダウン リストから [交換デバイス（Replacement Device）] を選択します。

手順 6　デバイスを交換するには、[交換（Replace）] をクリックします。現在のデバイスを保持して [デバイス管理（Device Management）] ページに戻るには、[キャンセル（Cancel）] をクリックします。

手順 7　メンテナンス モード切り替えアイコン（）を再度クリックすると、スタックのメンテナンス モードが即時に終了します。

デバイス設定を再適用する必要はありません。

クラスタ状態共有の設定

ライセンス：Control

サポートされるデバイス：シリーズ 3

クラスタ状態共有を使用すると、クラスタを構成するデバイス間、またはクラスタを構成するスタック間で、可能な限り状態を同期できます。したがって、いずれか一方のデバイスまたはスタックで障害が発生しても、もう一方のピアがトラフィック フローを中断せずに引き継ぐことができます。状態共有を使用しない場合、以下の機能が適切にフェールオーバーしない可能性があります。

- 厳密な TCP の適用（Strict TCP enforcement）
- 単方向アクセス コントロール ルール（Unidirectional access control rules）
- ブロッキングの永続性（Blocking persistence）

ただし、状態共有を有効にすると、システム パフォーマンスが低下することに注意してください。

クラスタ化された状態共有を設定するには、あらかじめクラスタ内の両方のデバイスまたはプライマリ スタック デバイスで HA リンク インターフェイスを設定し、有効にする必要があります。82xx ファミリおよび 83xx ファミリには 10 G の HA リンクが必要ですが、他のモデルのデバイスには 1 G の HA リンクで十分です。詳細については、HA リンク インターフェイスの設定（4-69 ページ）を参照してください。

(注)　クラスタを構成するデバイスでフェールオーバーが発生した場合は、アクティブ デバイス上の既存の SSL 暗号化セッションがすべて終了されます。クラスタ状態共有を設定しているとしても、これらのセッションをバックアップ デバイスで再ネゴシエートする必要があります。SSL セッションを確立しているサーバがセッションの再利用をサポートしている場合でも、バックアップ デバイスに SSL セッション ID がないと、セッションを再ネゴシエートできません。詳細については、デバイスのクラスタリング（4-31 ページ）を参照してください。

厳密な TCP の適用

ドメインに対して厳密な TCP 適用を有効にすると、システムは TCP セッションで正常ではないパケットをすべてドロップします。たとえば、未確立の接続で受信した SYN 以外のパケットはドロップされます。状態共有が有効な場合、厳密な TCP 適用が有効にされているとしても、クラスタ内のデバイスは、フェールオーバー後に接続を再び確立することなく TCP セッションを続行できます。厳密な TCP 適用は、インライン セット、仮想ルータ、および仮想スイッチで有効にすることができます。

単方向アクセス コントロール ルール

単方向アクセス コントロール ルールを設定している場合、システムがフェールオーバーの後に接続ミッドストリームを再評価する際に、ネットワーク トラフィックが意図されたものとは異なるアクセス コントロール ルールに一致する可能性があります。たとえば、ポリシーに以下の 2 つのアクセス コントロール ルールが含まれているとします。

```
Rule 1: Allow from 192.168.1.0/24 to 192.168.2.0/24
Rule 2: Block all
```

状態共有が有効でない場合、フェールオーバーの後に 192.168.1.1 ～ 192.168.2.1 の許可される接続がまだアクティブになっているために、次のパケットが応答パケットとしてみなされると、システムは接続を拒否します。状態共有が有効であれば、ミッドストリーム ピックアップが既存の接続に一致することになり、接続が引き続き許可されます。

ブロッキングの永続性

アクセス コントロール ルールやその他の要素に基づいて、最初のパケットで多数の接続がブロックされるとしても、システムが接続のブロッキングを決定する前に、いくつかのパケットを許可する場合があります。状態共有が有効な場合、システムはピア デバイスまたはスタックでも即時に接続をブロックします。

クラスタ状態共有を設定する際には、以下のオプションを設定できます。

[有効（Enabled）]

状態共有を有効にするには、このチェックボックスをクリックします。チェックボックスをクリアすると、状態共有が無効になります。

最短フロー寿命（Minimum Flow Lifetime）

最小セッション時間（ミリ秒）を指定します。この時間を経過すると、システムがセッションの同期メッセージを送信します。0 ～ 65535 の整数を使用できます。この最小フロー有効期間に達しないセッションは、いずれも同期されず、接続のパケットを受信した時点でのみ、同期が行われます。

最短同期間隔インターバル（Interval

セッションの更新メッセージ最短間隔（ミリ秒）を指定します。0 ～ 65535 の整数を使用できます。最短同期間隔を設定することで、特定の接続が最短有効期間に達した後、その接続に対して、設定された値より頻繁に同期メッセージが送信されないようにします。

HTTP URL の最大文字数（Maximum HTTP URL Length）

クラスタを構成するデバイス間で同期する、URL の最大文字数を指定します。0 ～ 225 の整数を使用できます。

（注）　シスコでは、展開で値を変更する正当な理由がない限り、デフォルト値を使用することを推奨しています。値を小さくすると、クラスタを構成するピアの即時対応性が向上し、値を大きくすると、パフォーマンスが向上します。

クラスタ状態共有を設定するには、以下を行います。

アクセス：Admin/Network Admin

手順 1　クラスタ内のデバイスごとに HA リンク インターフェイスを設定します。

詳細については、HA リンク インターフェイスの設定（4-69 ページ）を参照してください。

手順 2　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 3　編集するデバイス クラスタの横にある編集アイコン（）をクリックします。

[クラスタ（Cluster）] ページが表示されます。

手順 4　[状態共有（State Sharing）] セクションの横にある編集アイコン（）をクリックします。

[状態共有（State Sharing）] ポップアップ ウィンドウが表示されます。

手順 5　このセクションですでに説明したように、状態共有を設定します。

手順 6　[OK] をクリックします。

変更が保存されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくはデバイスへの変更の適用（4-27 ページ）を参照してください）。

クラスタ状態共有のトラブルシューティング

ライセンス：Control

サポートされるデバイス：シリーズ 3

状態共有を有効にした後は、[クラスタ（Cluster）] ページの [状態共有（State Sharing）] セクションで、設定に関する以下の情報を確認できます。

- 使用されている HA リンク インターフェイスおよび現在のリンク ステート
- 問題のトラブルシューティングに使用できる、同期に関する詳細な統計情報

状態共有の統計情報は、主に、クラスタで送受信された同期トラフィックのさまざまな側面に対するカウンタです。その他に、いくつかのエラー カウンタもあります。さらに、クラスタ内のデバイスごとの最新システム ログも表示できます。

各デバイスに関して確認できる統計情報、およびそれらの情報を使用してクラスタ状態共有設定のトラブルシューティングを行う方法の詳細については、以下の項を参照してください。

受信メッセージ(ユニキャスト)(Messages Received (Unicast))

受信メッセージは、クラスタを構成するピアから受信した、クラスタ同期メッセージの数です。

値は、ピアが送信したメッセージ数と同等になっているはずです。アクティブに使用されている間は、値が一致しない場合もありますが、その差は小さいはずです。トラフィックが停止すると、値は安定し、受信したメッセージ数が送信されたメッセージ数と一致します。

トラブルシューティングを行う場合は、受信したメッセージ数と送信されたメッセージ数の両方を確認して増加率を比較し、両方の値が同等であることを確認します。各ピアでの送信数の値は、対応するピアでの受信数の値とほぼ同じ率で増えていなければなりません。

受信したメッセージの数が増加しなくなった場合、または増加率がピアから送信されたメッセージ数に追いついていない場合は、サポートに連絡してください。

受信パケット数(Packets received)

システムはオーバーヘッドを低減させるために、複数のメッセージを単一のパケットにまとめます。[受信パケット数(Packets Received)] カウンタは、デバイスが受信したこれらのデータ パケットとその他の制御パケットの数を表示します。

値は、ピア デバイスが送信したパケット数と同等になっているはずです。アクティブに使用されている間は、値が一致しない場合もありますが、その差は小さいはずです。受信メッセージの数は、ピアが送信したメッセージ数と同等で、同じ率で増加していなければなりません。したがって、受信したパケットの数も同じ動作となるはずです。

トラブルシューティングを行う場合は、受信したパケットと送信されたメッセージの両方を確認して増加率を比較し、値が同じ率で増加していることを確認します。クラスタを構成するピアでの送信の値が増えている場合、デバイスでの受信の値も同じ率で増えているはずです。

受信したパケットの数が増加しなくなった場合、または増加率がピアから送信されたメッセージ数に追いついていない場合は、サポートに連絡してください。

合計受信バイト数(Total Bytes Received)

ピアで受信されたパケットの合計バイト数です。

値は、もう一方のピアが送信したバイト数と同等になっているはずです。アクティブに使用されている間は、値が一致しない場合もありますが、その差は小さいはずです。

トラブルシューティングを行う場合は、受信した合計バイト数と送信されたメッセージ数の両方を確認して増加率を比較し、両方の値が同じ率で増えていることを確認します。クラスタを構成するピアでの送信の値が増えている場合、デバイスでの受信の値も同じ率で増えているはずです。

受信バイト数が増加しなくなった場合、または増加率がピアから送信されたメッセージ数に追いついていない場合は、サポートに連絡してください。

受信プロトコル バイト数(Protocol Bytes Received)

受信したプロトコル オーバーヘッドのバイト数です。この数には、セッション状態同期メッセージのペイロードを除くすべてが含まれます。

値は、ピアが送信したバイト数と同等になっているはずです。アクティブに使用されている間は、値が一致しない場合もありますが、その差は小さいはずです。

トラブルシューティングを行う場合は、受信した合計バイト数を確認してプロトコル データと比較し、実際の状態データがどれだけ共有されているのかを調べます。プロトコル データが送信されるデータの大部分を占めている場合は、最小同期間隔を調整できます。

受信したプロトコル バイト数が、受信した合計バイト数と同等の割合で増えている場合は、サポートに連絡してください。受信したプロトコル バイト数が受信した合計バイト数に占める割合は、最小限でなければなりません。

送信メッセージ（Messages Sent）

送信メッセージは、クラスタを構成するピアに送信した、クラスタ同期メッセージの数です。

このデータは、受信メッセージ数との比較で役立ちます。アクティブに使用されている間は、値が一致しない場合もありますが、その差は小さいはずです。

トラブルシューティングを行う場合は、受信したメッセージ数と送信されたメッセージ数の両方を確認して増加率を比較し、両方の値が同等であることを確認します。

送信したメッセージ数が、受信した合計バイト数と同等の割合で増えている場合は、サポートに連絡してください。

送信バイト数（Bytes Sent）

送信バイト数は、ピアに送信したクラスタ同期メッセージの合計送信バイト数です。

このデータは、受信メッセージ数との比較で役立ちます。アクティブに使用されている間は、値が一致しない場合もありますが、その差は小さいはずです。ピアで受信されたバイト数は、この値と同等であり、それより大きい値にはなっていないはずです。

受信した合計バイト数が、送信されたバイト数と同じような比率で増えていない場合は、サポートに連絡してください。

Tx Errors

Tx エラーは、システムがクラスタを構成するピアに送信するメッセージ用にスペースを割り当てるときに発生した、メモリ割り当ての失敗数です。

この値は両方のピアで常にゼロでなければなりません。この数がゼロでない場合、あるいは着実に増加している場合（これは、システムにメモリ割り当てが不可能なエラーが発生していることを示します）は、サポートに連絡してください。

Tx オーバーラン（Tx Overruns）

システムがメッセージをトランジット キューに入れようとして失敗した回数です。

この値は両方のピアで常にゼロでなければなりません。値がゼロでない場合、あるいは着実に増加している場合、これは、システムが HA リンクの間で過剰なデータを共有していて、データの送信に時間がかかりすぎていることを示します。

HA リンク MTU がデフォルト値（9918 または 9922）未満に設定されている場合は、値を増やす必要があります。最小フロー有効期間と最小同期間隔の設定を変更することで、HA リンク間で共有されるデータ量を減らし、この数の増加を防ぐことができます。

この値がゼロにならない場合、または増加し続けている場合は、サポートに連絡してください。

最近のログ（Recent Logs）

システム ログには、最新のクラスタ同期メッセージが表示されます。ログには、ERROR または WARN メッセージが示されていてはなりません。ログの内容は、常にピア間で同等でなければなりません（接続ソケットの数が同じであるなど）。

ただし、場合によっては、対照的なデータが表示されることもあります。たとえば、一方のピアがもう一方のピアから接続を受信したことをレポートしている場合、それぞれのログで参照される IP アドレスは異なります。このログから、クラスタ状態共有接続を包括的に理解し、接続で発生したすべてのエラーを確認できます。

ログに、ERROR または WARN メッセージ、あるいは単なる通知目的ではないようなメッセージが示されている場合は、サポートに連絡してください。

クラスタ状態共有に関する統計情報を表示するには、以下を行います。

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　編集するデバイス クラスタの横にある編集アイコン（ ）をクリックします。

デバイス クラスタの [クラスタ（Cluster）] ページが表示されます。

手順 3　[状態共有（State Sharing）] セクションで、統計情報表示アイコン（ ）をクリックします。

[状態共有統計（State Sharing Statistics）] ポップアップ ウィンドウが表示されます。

手順 4　必要に応じて、[デバイス（Device）] を選択して、クラスタがデバイス スタックで構成されているかどうかを確認します。

手順 5　必要に応じて、[更新（Refresh）] をクリックして統計情報を更新します。

手順 6　必要に応じて、[表示（View）] をクリックして、クラスタを構成する各デバイスの最新データ ログを表示します。

クラスタを構成するデバイスの分離

ライセンス：Control

サポートされるデバイス：シリーズ 3

デバイス クラスタリングを解除しても、アクティブ デバイスまたはスタックは、完全な展開機能を維持します。バックアップ デバイスまたはスタックは、インターフェイス設定を失い、アクティブ デバイスまたはスタックにフェールオーバーします。ただし、インターフェイス設定をアクティブに維持することを選択すると、バックアップ デバイスまたはスタックは通常の動作を再開します。クラスタを解除すると、バックアップ デバイスのパッシブ インターフェイス設定は必ず削除されます。メンテナンス モードのデバイスは、クラスタが解除された時点で通常の動作を再開します。

クラスタを構成するデバイスを分離するには、以下を行います。

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　解除するデバイス クラスタの横にあるクラスタ解除アイコン（ ）をクリックします。

[解除の確認（Confirm Break）] ポップアップ ウィンドウが表示されます。

手順 3　必要に応じて、バックアップ デバイスまたはスタックのインターフェイス設定を削除するチェックボックスをオンにします。この場合、管理インターフェイスを除くすべてのインターフェイスが管理上、ダウン状態になります。

手順 4　[Yes] をクリックします。

デバイス クラスタが解除されます。

スタック構成のデバイスの管理

ライセンス: 任意（Any）

サポートされるデバイス: 3D8140、3D8200 ファミリ、3D8300 ファミリ、AMP8300 ファミリ、ASM3D9900

スタック構成に含まれるデバイスを使用して、ネットワーク セグメントで検査されるトラフィックの量を増やすことができます。それぞれのスタック構成では、スタックに含まれるすべてのデバイスが同じハードウェアを使用していなければなりません。ただし、スタックに 3D9900 が含まれない場合、マルウェア ストレージ パックがインストールされたデバイスがなくても、一部またはすべてのデバイスにマルウェア ストレージ パックがインストールされていても構いません。また、以下のスタック構成に従って、同じデバイス ファミリのデバイスを使用する必要があります。

シリーズ 2 および 81xx ファミリの場合:

- 2 つの 3D8140
- 2 つの 3D9900

82xx ファミリの場合:

- 最大 4 つの 3D8250
- 1 つの 3D8260（プライマリ デバイスおよびセカンダリ デバイス）
- 1 つの 3D8270（容量 40 G のプライマリ デバイスと 2 つのセカンダリ デバイス）
- 1 つの 3D8290（容量 40 G のプライマリ デバイスと 3 つのセカンダリ デバイス）

83xx ファミリの場合:

- 最大 4 つの 3D8350
- 1 つの 3D8360（容量 40 G のプライマリ デバイスとセカンダリ デバイス）
- 1 つの 3D8370（容量 40 G のプライマリ デバイスと 2 つのセカンダリ デバイス）
- 1 つの 3D8390（容量 40 G のプライマリ デバイスと 3 つのセカンダリ デバイス）
- 最大 4 つの AMP8350
- 1 つの AMP8360（容量 40 G のプライマリ デバイスとセカンダリ デバイス）
- 1 つの AMP8370（容量 40 G のプライマリ デバイスと 2 つのセカンダリ デバイス）
- 1 つの AMP8390（容量 40 G のプライマリ デバイスと 3 つのセカンダリ デバイス）

スタック構成の詳細については、『*FireSIGHT システム Installation Guide*』を参照してください。マルウェア ストレージ パックの詳細については、『*FireSIGHT システム Malware Storage Pack Guide*』を参照してください。

注意　シスコから供給されたハード ドライブ以外はデバイスに取り付けないでください。サポートされていないハード ドライブを取り付けると、デバイスが破損する可能性があります。マルウェア ストレージ パック キットは、シスコから**のみ**購入でき、8000 シリーズ デバイスで**のみ**使用できます。マルウェア ストレージ パックのサポートが必要な場合は、サポートにお問い合わせください。詳細については、『*FireSIGHT システム Malware Storage Pack Guide*』を参照してください。

スタック構成を確立するときに、各スタック構成のデバイスのリソースを 1 つの共有構成に統合します。

1 つのデバイスを *プライマリ* デバイスとして指定し、そのデバイスにスタック全体のインターフェイスを設定します。その他のデバイスは *セカンダリ* デバイスとして指定します。セカンダリ デバイスは、現在トラフィックを検知していないデバイスで、かつインターフェイス上にリンクがないデバイスでなければなりません。

単一のデバイスを設定する場合と同じように、プライマリ デバイスを分析対象のネットワーク セグメントに接続します。詳細については、センシング インターフェイスの設定（4-66 ページ）を参照してください。『*FireSIGHT システム Installation Guide*』で説明されている、スタック構成のデバイスの配線手順に従って、セカンダリ デバイスをプライマリ デバイスに接続します。

スタック構成に含まれるすべてのデバイスは、同じハードウェアを使用し、同じソフトウェア バージョンを実行し、同じライセンスが適用されている必要があります。デバイスが NAT ポリシーのターゲットとなっている場合は、プライマリ デバイスとセカンダリ デバイスの両方に同じ NAT ポリシーを適用する必要があります。詳細については、NAT ポリシーの管理（11-8 ページ）を参照してください。更新は、防御センター からスタック全体に対して適用する必要があります。スタックに含まれる 1 つ以上のデバイスで更新に失敗した場合、スタックはバージョンが混在した状態になります。バージョンが混在した状態のスタックには、ポリシーを適用することも、更新を適用することもできません。この状態を修正するには、スタックを解除するか、バージョンが異なる個々のデバイスを削除し、それらのデバイスを個別に更新してからスタック構成を再確立します。デバイスをスタックに入れた後は、ライセンスの変更は、スタック全体に対してのみ行うことができます。

スタック構成を確立した後は、スタックに含まれるすべてのデバイスが単一の共有構成のように機能します。プライマリ デバイスで障害が発生した場合、トラフィックはセカンダリ デバイスに渡されません。この場合、セカンダリ デバイスでスタック ハートビートが失敗したことを通知する、ヘルス アラートが生成されます。詳細については、ヘルス モニタリングの使用（68-1 ページ）を参照してください。

スタック内のセカンダリ デバイスで障害が発生すると、設定可能なバイパスが有効になっているインライン セットがプライマリ デバイス上でバイパス モードになります。それ以外のすべての設定では、システムは、失敗したセカンダリ デバイスへ継続してトラフィックをロード バランスします。いずれの場合も、リンクが失われたことを示すためのヘルス アラートが生成されます。

デバイス スタックは展開内で単一のデバイスと同じように使用できますが、いくつかの例外があります。クラスタを構成するデバイスが存在する場合、デバイス クラスタや、クラスタ ペアとなっているデバイスをスタックに含めることはできません。詳細については、デバイスのクラスタリング（4-31 ページ）を参照してください。また、デバイス スタックに NAT を設定することもできません。

（注） スタック構成のデバイスからのイベント データを、eStreamer を使用して外部クライアント アプリケーションにストリームする場合は、各デバイスからデータを収集して、各デバイスが同じように設定されていることを確認します。eStreamer 設定は、スタック構成のデバイス間で自動的に同期されません。

詳細については、次の各項を参照してください。

- デバイス スタックの確立（4-49 ページ）
- デバイス スタックの編集（4-51 ページ）
- スタックに含まれる個々のデバイスの設定（4-51 ページ）
- スタック構成のデバイスの分離（4-53 ページ）
- スタック内のデバイスの交換（4-53 ページ）

デバイス スタックの確立

ライセンス: 任意（Any）

サポートされるデバイス: 3D8140、3D8200 ファミリ、3D8300 ファミリ、AMP8300 ファミリ、3D9900

ネットワーク セグメントで検査されるトラフィック量を増やすには、ファイバベースの 3D9900（2 つ）、3D8140 デバイス（2 つ）、3D8250（最大 4 つ）、3D8260、3D8270、3D8290、3D8350（最大 4 つ）、3D8360、3D8370、3D8390、AMP8350（最大 4 つ）、AMP8360、AMP8370、または AMP8390 でスタックを構成し、それらのリソースを結合して単一の共有構成で使用します。始める前に、次の手順を実行する必要があります。

- プライマリ デバイスとして指定するユニットを決定します。
- プライマリとセカンダリの関係を指定する前に、適切にユニット間の配線を行います。配線については、『*FireSIGHT システム Installation Guide*』を参照してください。

（注） クラスタを構成するデバイスが存在する場合、デバイス クラスタや、クラスタ ペアとなっているデバイスをスタックに含めることはできません。ただし、デバイス スタックでクラスタを構成することはできます。詳細については、デバイスのクラスタリング（4-31 ページ）を参照してください。

デバイス スタックを確立すると、これらのデバイスは、[デバイス管理（Device Management）] ページで単一のデバイスとして扱われます。デバイス スタックには、アプライアンスのリストでスタック アイコン（ ）が表示されます。

デバイス スタックの登録を 防御センター から削除すると、その登録は両方のデバイスから削除されます。スタックに含まれるデバイスを 防御センター から削除する方法は、単一の管理対象デバイスを削除する場合と同じです。削除したスタックは、別の 防御センター に登録できます。新しい 防御センター に、スタック構成のデバイスのいずれか 1 つを登録するだけで、スタック全体が表示されるようになります。詳細については、デバイスの削除（4-29 ページ）と防御センターへのデバイスの追加（4-25 ページ）を参照してください。

デバイス スタックを確立した後は、スタックを解除して再確立しない限り、デバイスのプライマリまたはセカンダリとしての役割を変更することはできません。ただし、次の作業を実行できます。

- スタックで許容される最大 4 つの 3D8250 になるまで、2 つまたは 3 つの 3D8250、3D8260、または 3D8270 からなる既存のスタックにセカンダリ デバイスを追加します。
- スタックで許容される最大 4 つの 3D8350 になるまで、2 つまたは 3 つの 3D8350、3D8360、または 3D8370 からなる既存のスタックにセカンダリ デバイスを追加します。
- スタックで許容される最大 4 つの AMP8350 になるまで、2 つまたは 3 つの AMP8350、AMP8360、または AMP8370 からなる既存のスタックにセカンダリ デバイスを追加します。

デバイスを追加する場合、スタックのプライマリ デバイスに、追加のデバイスを配線するために必要なスタック NetMods がなければなりません。たとえば、プライマリに単一のスタック NetMod しかない 3D8260 を使用している場合、このスタックに別のセカンダリ デバイスを追加することはできません。セカンダリ デバイスを既存のスタックに追加する方法は、最初にスタック構成のデバイス設定を確立したときの方法と同じです。

スタック構成のデバイス設定を確立するには、以下を行います。

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　[追加（Add）] ドロップダウン メニューから、[スタックの追加（Add Stack）] を選択します。

[スタックの追加（Add Stack）] ポップアップ ウィンドウが表示されます。

手順 3　[プライマリ（Primary）] ドロップダウン リストから、プライマリ デバイスとして運用するために配線したデバイスを選択します。

（注）　プライマリ デバイスとして配線されていないデバイスを編集すると、以降の手順を実行できなくなります。

手順 4　[名前（Name）] フィールドに、スタックの名前を入力します。英数字と特殊文字を入力できます。ただし、+、(、)、{、}、#、&、\、<、>、?、‘、および “ の文字は無効です。

手順 5　[追加（Add）] をクリックして、スタックに含めるデバイスを選択します。

[セカンダリ接続の追加（Add Secondary Connection）] ポップアップ ウィンドウが表示されます。以下の図に、3D8140 のプライマリ デバイスの正面図を示します。

手順 6　[プライマリ デバイスのスロット（Slot on Primary Device）] ドロップダウン リストから、プライマリ デバイスをセカンダリ デバイスに接続するスタック構成ネットワーク モジュールを選択します。

手順 7　[セカンダリ デバイス（Secondary Device）] ドロップダウン リストから、セカンダリ デバイスとして運用するために配線したデバイスを選択します。

（注）　スタックに含まれるすべてのデバイスは、同じハードウェア モデルでなければなりません（たとえば、3D9900 と 3D9900、3D8140 と 3D8140 など）。82xx ファミリおよび 83xx ファミリでは、合計 4 つのデバイス（1 つのプライマリ デバイスと最大 3 つのセカンダリ デバイス）でスタックを構成できます。

手順 8　[セカンダリ デバイスのスロット（Slot on Secondary Device）] ドロップダウン リストから、セカンダリ デバイスをプライマリ デバイスに接続するスタック構成ネットワーク モジュールを選択します。

手順 9　[追加（Add）] をクリックします。

[スタックの追加（Add Stack）] ウィンドウが再表示されて、新しいセカンダリ デバイスがリストされます。

手順 10　（任意）3D8250 の既存のスタック、3D8260、3D8270、3D8350 の既存のスタック、3D8360、3D8370、AMP8350 の既存のスタック、AMP8360、または AMP8370 にセカンダリ デバイスを追加するには、ステップ 5 から 9 を繰り返します。

手順 11　[スタック（Stack）] をクリックします。

デバイス スタックが確立されるか、セカンダリ デバイスが追加されます。このプロセスではシステム データの同期が行われるため、プロセスが完了するまでに数分かかることに注意してください。

デバイス スタックの編集

ライセンス：任意（Any）

サポートされるデバイス：3D8140、3D8200 ファミリ、3D8300 ファミリ、AMP8300 ファミリ、3D9900

デバイス スタックを設定した後は、デバイスの設定を変更すると、通常はスタック全体の設定も変更されます。単一のデバイスの [デバイス（Device）] ページで設定を変更する場合と同じように、アプライアンス エディタの [スタック（Stack）] ページで、スタック設定に変更を加えることができます。

このページでは、スタックの表示名の変更、ライセンスの有効化と無効化、システム ポリシーと正常性ポリシーの表示、自動アプリケーション バイパスの設定、高速パス ルールの設定を行うことができます。

詳細については、次の各項を参照してください。

- 一般的なデバイス設定の編集（4-54 ページ）
- デバイス ライセンスの有効化と無効化（4-55 ページ）
- 詳細なデバイス設定の編集（4-61 ページ）

スタック構成の設定を編集するには、以下を行います。

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　設定を編集する、スタック構成のデバイスの横にある編集アイコン（ ）をクリックします。

そのデバイスの [スタック（Stack）] ページが表示されます。

手順 3　[スタック（Stack）] ページのセクションを使用して、単一のデバイス設定を変更する場合と同じように、スタック構成の設定を変更します。

スタックに含まれる個々のデバイスの設定

ライセンス：任意（Any）

サポートされるデバイス：3D8140、3D8200 ファミリ、3D8300 ファミリ、AMP8300 ファミリ、3D9900

デバイス スタックを確立した後でも、スタック内の個々のデバイスに対して設定できる属性がいくつかあります。アプライアンス エディタの [デバイス（Devices）] ページで、単一デバイスの [デバイス（Device）] ページの場合と同じように、スタックに含まれる個々のデバイスに変更を加えることができます。

このページでは、デバイスの表示名の変更、システム設定の表示、デバイスのシャットダウンまたは再起動、ヘルス情報の表示、およびデバイス管理設定の編集を行うことができます。

詳細については、次の各項を参照してください。

- 一般的なデバイス設定の編集（4-54 ページ）
- デバイス システム設定の編集（4-56 ページ）

- デバイスのヘルスの確認（4-58 ページ）
- デバイス管理設定の編集（4-58 ページ）

スタックに含まれる個々のデバイスを設定するには、以下を行います。

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　設定を編集する、スタック構成のデバイスの横にある編集アイコン（  ）をクリックします。

そのデバイスの [スタック（Stack）] ページが表示されます。

手順 3　[デバイス（Devices）] をクリックします。

[デバイス（Devices）] ページが表示されます。

手順 4　[選択されたデバイス（Selected Device）] ドロップダウン リストから、変更するデバイスを選択します。

手順 5　[デバイス（Devices）] ページのセクションを使用して、単一のデバイスに対して変更を加える場合と同じように、スタック構成の個々のデバイスに変更を加えます。

スタック構成のデバイスでのインターフェイスの設定

ライセンス：任意（Any）

サポートされるデバイス：3D8140、3D8200 ファミリ、3D8300 ファミリ、AMP8300 ファミリ、3D9900

管理インターフェイスを除き、スタック構成のデバイス インターフェイスを設定するには、スタックのプライマリ デバイスの [インターフェイス（Interfaces）] ページを使用します。管理インターフェイスを設定する場合は、スタックに含まれる任意のデバイスを選択できます。詳細については、管理インターフェイスの構成（64-9 ページ）を参照してください。

シリーズ 3 のスタック構成のデバイスの [インターフェイス（Interfaces）] ページに、個々のデバイスのハードウェアおよびインターフェイスのビューがあります。3D9900 の [インターフェイス（Interfaces）] ページには、これらのビューは含まれていません。詳細については、センシング インターフェイスの設定（4-66 ページ）を参照してください。

スタック構成のデバイスにインターフェイスを設定するには、以下を行います。

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　インターフェイスを設定する、スタック構成のデバイスの横にある編集アイコン（  ）をクリックします。

そのデバイスの [スタック（Stack）] ページが表示されます。

手順 3　[インターフェイス（Interfaces）] をクリックします。

[インターフェイス（Interfaces）] ページが表示されます。

手順 4　[選択されたデバイス(Selected Device)] ドロップダウン リストから、変更するデバイスを選択します。

手順 5　個々のデバイスに設定する場合と同じようにインターフェイスを設定します。詳細については、センシング インターフェイスの設定(4-66 ページ)を参照してください。

スタック構成のデバイスの分離

ライセンス: 任意(Any)

サポートされるデバイス: 3D8140、3D8200 ファミリ、3D8300 ファミリ、AMP8300 ファミリ、3D9900

デバイスのスタック構成を使用する必要がなくなった場合、スタックを解除してデバイスを分離できます。

スタック構成のデバイスを分離するには、以下を行います。

アクセス: Admin/Network Admin

手順 1　[デバイス(Devices)] > [デバイス管理(Device Management)] を選択します。

[デバイス管理(Device Management)] ページが表示されます。

手順 2　解除するデバイス スタックの横にあるスタック解除アイコン( )をクリックします。

[解除の確認(Confirm Break)] ポップアップ ウィンドウが表示されます。

ヒント　スタックを解除せずに、3 つ以上の 3D8250 デバイスで構成されるスタックからセカンダリ デバイスを削除するには、スタックから削除アイコン( )をクリックします。セカンダリ デバイスを削除すると、システムがそのデバイス抜きで動作するスタックを再設定する間、トラフィック インスペクション、トラフィック フロー、またはリンク ステートが短時間中断されます。

手順 3　[Yes] をクリックします。

デバイス スタックが解除されます。

スタック内のデバイスの交換

ライセンス: 任意(Any)

サポートされるデバイス: 3D8140、3D8200 ファミリ、3D8300 ファミリ、AMP8300 ファミリ、3D9900

スタック構成のデバイスを交換するには、スタックを解除する必要があります。

警告　**防御センター がデバイスと通信できない場合に、スタックを分離して 防御センター のデバイスの登録を解除するには、デバイスに接続して CLI コマンドを使用する必要があります。詳細については、コンフィギュレーション コマンド(D-31 ページ)の `stacking disable` CLI コマンドおよび `delete` CLI コマンドを参照してください。**

デバイス スタック内のデバイスを交換するには、以下を行います。

手順 1　デバイスを含むスタックを選択し、そのスタックを交換して解除します。詳細については、スタック構成のデバイスの分離（4-53 ページ）を参照してください。

手順 2　防御センター からデバイスを登録解除します。詳細については、ハイ アベイラビリティの無効化とデバイスの登録解除（4-18 ページ）を参照してください。

手順 3　交換デバイスを 防御センター に登録します。詳細については、防御センター へのデバイスの追加（4-25 ページ）を参照してください。

手順 4　交換デバイスを含むデバイス スタックを作成します。詳細については、デバイス スタックの確立（4-49 ページ）を参照してください。

デバイス設定の編集

ライセンス：任意（Any）

アプライアンス エディタの [デバイス（Device）] ページには、詳細なデバイス設定および情報が表示されます。また、デバイス設定の一部（ライセンスの有効化と無効化、デバイスのシャットダウンと再起動、管理の変更、高速パス ルールの設定など）を変更することもできます。

詳細については、次の各項を参照してください。

- 一般的なデバイス設定の編集（4-54 ページ）
- デバイス ライセンスの有効化と無効化（4-55 ページ）
- デバイス システム設定の編集（4-56 ページ）
- デバイスのヘルスの確認（4-58 ページ）
- デバイス管理設定の編集（4-58 ページ）
- 高度なデバイス設定について（4-59 ページ）

一般的なデバイス設定の編集

ライセンス：任意（Any）

[デバイス（Device）] タブの [一般（General）] セクションには、以下の変更可能な管理対象デバイスの設定が表示されます。

[名前（Name）]
管理対象デバイスに割り当てる名前。

パケット転送（Transfer Packets）
パケット データを 防御センター に転送してイベントと共に保存するかどうかを指定します。

一般的なデバイス設定の編集方法:

アクセス: Admin/Network Admin

手順 1　[デバイス(Devices)] > [デバイス管理(Device Management)] を選択します。

[デバイス管理(Device Management)] ページが表示されます。

手順 2　割り当てられた名前を編集するデバイスの横にある編集アイコン( )をクリックします。

デバイスの [インターフェイス(Interfaces)] ページが表示されます。

手順 3　[デバイス(Device)] をクリックします。

[デバイス(Device)] ページが表示されます。

ヒント　スタック構成のデバイスの場合、アプライアンス エディタの [スタック(Stack)] ページで、スタックでデバイスに割り当てられている名前を編集します。アプライアンス エディタの [デバイス(Devices)] ページでは、個々のデバイスに割り当てられているデバイス名を編集できます。

手順 4　[一般(General)] セクションの横にある編集アイコン( )をクリックします。

[一般(General)] ポップアップ ウィンドウが表示されます。

手順 5　[名前(Name)] フィールドに、デバイスに割り当てる新しい名前を入力します。英数字と特殊文字を入力できます。ただし、+、(、)、{、}、#、&、\、<、>、?、‘、および “ の文字は無効です。

手順 6　パケット データをイベントと一緒に 防御センター に保存できるようにするには、[パケットの転送(Transfer Packets)] チェックボックスをオンにします。管理対象デバイスがイベントと一緒にパケット データを送信できないようにするには、このチェックボックスをオフにします。

手順 7　[保存(Save)] をクリックします。

これにより、変更内容が保存されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください(詳しくはデバイスへの変更の適用(4-27 ページ)を参照してください)。

デバイス ライセンスの有効化と無効化

ライセンス: 任意(Any)

サポートされるデバイス: シリーズ 3、仮想、X-シリーズ、ASA FirePOWER

防御センター で使用可能なライセンスがある場合、デバイスでそのライセンスを有効にすることができます。次の点に注意してください。

- Control、Malware、および URL フィルタリング(URL Filtering) ライセンスには、Protection ライセンスが必要です。
- VPN ライセンスは、仮想デバイス、Blue Coat X-Series 向け Cisco NGIPS、または ASA FirePOWER デバイスで有効にすることはできません。
- Control ライセンスを仮想デバイス、Blue Coat X-Series 向け Cisco NGIPS、または ASA FirePOWER デバイスで有効にすることはできますが、これらのデバイスでは、高速パス ルール、スイッチング、ルーティング、スタック構成、クラスタリングを**サポートしていません**。Blue Coat X-Series 向け Cisco NGIPS は、アプリケーションやユーザの制御もサポートしていません。

- クラスタを構成するデバイスでのライセンス設定を変更することはできません。
- シリーズ 2 デバイスには、セキュリティ インテリジェンス フィルタリングを除く Protection 機能が自動的に有効になるため、これらの機能を無効にすることも、シリーズ 2 デバイスに他のライセンスを適用することもできません。

詳細については、FireSIGHT システム のライセンス（65-1 ページ）を参照してください。

デバイス ライセンスを有効または無効にするには、以下を行います。

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　ライセンスを有効または無効にするデバイスの横にある編集アイコン（）をクリックします。

デバイスの [インターフェイス（Interfaces）] タブが表示されます。

手順 3　[デバイス（Device）] をクリックします。

[デバイス（Devices）] タブが表示されます。

ヒント　スタック構成のデバイスの場合、アプライアンス エディタの [スタック（Stack）] ページで、スタックに対してラインセンスを有効または無効にします。

手順 4　[ライセンス（License）] セクションの横にある編集アイコン（）をクリックします。

[ライセンス（License）] ポップアップ ウィンドウが表示されます。

手順 5　次の選択肢があります。

- ライセンスを有効にする場合は、ライセンス名の横にあるチェックボックスをオンにします。
- ライセンスを無効にする場合は、ライセンス名の横にあるチェックボックスをオフにします。

手順 6　[保存（Save）] をクリックします。

これにより、変更内容が保存されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくはデバイスへの変更の適用（4-27 ページ）を参照してください）。

デバイス システム設定の編集

ライセンス：任意（Any）

[デバイス（Device）] タブの [システム（System）] セクションには、次の表に示すように、システム情報の読み取り専用テーブルが表示されます。

表 4-2　[システム(System)] セクション テーブルのフィールド

フィールド	説明
モデル（Model）	管理対象デバイスのモデル名と番号。
シリアル（Serial）	管理対象デバイスのシャーシのシリアル番号。
時刻（Time）	デバイスの現在のシステム時刻。
バージョン（Version）	管理対象デバイスに現在インストールされているソフトウェアのバージョン。
ポリシー（Policy）	管理対象デバイスに現在適用されているシステム ポリシーへのリンク。

デバイスをシャットダウンまたは再起動することもできます。

（注）　FireSIGHT システム ユーザ インターフェイスが設定されている X-シリーズ または ASA FirePOWER デバイスをシャットダウンしたり、再起動したりすることはできません。それぞれのデバイスをシャットダウンする方法の詳細については、『*Blue Coat X-Series 向け Cisco NGIPS Installation Guide*』または ASA のドキュメンテーションを参照してください。

管理対象デバイスをシャットダウンおよび再起動するには、以下を行います。

アクセス：Admin/Network Admin

手順 1　[デバイス(Devices)] > [デバイス管理(Device Management)] を選択します。

[デバイス管理(Device Management)] ページが表示されます。

手順 2　再起動するデバイスの横にある編集アイコン( )をクリックします。

デバイスの [インターフェイス(Interfaces)] タブが表示されます。

手順 3　[デバイス(Device)] をクリックします。

[デバイス(Devices)] タブが表示されます。

ヒント　スタック構成のデバイスの場合、アプライアンス エディタの [デバイス(Devices)] ページで、個々のデバイスをシャットダウンまたは再起動します。

手順 4　デバイスをシャットダウンするには、デバイスのシャット ダウン アイコン( )をクリックします。

手順 5　プロンプトが表示されたら、デバイスをシャットダウンすることを確認します。

[デバイス管理(Device Management)] ページに戻ります。

手順 6　デバイスを再起動するには、デバイスの再起動アイコン( )をクリックします。

手順 7　プロンプトが表示されたら、デバイスを再起動することを確認します。

デバイスが再起動されます。

デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくはデバイスへの変更の適用（4-27 ページ）を参照してください）。

デバイスのヘルスの確認

ライセンス：任意（Any）

[デバイス（Device）] タブの [状況（Health）] セクションには、ヘルス関連の情報が表示されます。管理対象デバイスの現在のヘルス ステータスを示すアイコンを確認できます。また、アイコンをクリックして、そのデバイスの [ヘルス モニタ（Health Monitor）] ページに移動することもできます。詳細については、ヘルス モニタ ステータスの解釈（68-47 ページ）を参照してください。

[ポリシー（Policy）] リンクをクリックすると、現在適用されている正常性ポリシーの読み取り専用バージョンが表示されます。詳細については、正常性ポリシーの編集（68-35 ページ）を参照してください。

また、[ブラックリスト（Blacklist）] リンクをクリックすると、[動作状況ブラックリスト（Health Blacklist）] ページが表示されます。このページで、ヘルス ブラックリスト モジュールを有効または無効にすることができます。詳細については、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（68-43 ページ）を参照してください。

デバイス管理設定の編集

ライセンス：任意（Any）

[デバイス（Device）] タブの [管理（Management）] セクションには、以下のリモート管理情報が表示されます。

ホスト

デバイスの現在の管理ホスト名または IP アドレス。この設定を使用して、管理ホスト名を指定したり、仮想 IP アドレスを再生成したりすることができます。

（注） 場合によっては、（デバイスの LCD パネルまたは CLI などを使用して）別の方法でデバイスのホスト名や IP アドレスを編集する場合、次の手順を実行して、管理用の 防御センター でホスト名や IP アドレスを手動で更新する必要があります。

ステータス（Status）

防御センター と管理対象デバイス間の通信チャネルのステータスを指定します。

ヒント スライダをクリックすることで、管理対象デバイスの管理を有効または無効にできます。管理を無効化すると、Defense Center とデバイス間の接続がブロックされますが、Defense Center からデバイスは削除**されません**。デバイスを管理する必要がなくなった場合は、デバイスの削除（4-29 ページ）を参照してください。

デバイス管理オプションを変更する方法：

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　管理オプションを変更するデバイスの横にある編集アイコン（ ）をクリックします。

デバイスの [インターフェイス（Interfaces）] タブが表示されます。

手順 3　[デバイス（Device）] をクリックします。

[デバイス（Devices）] タブが表示されます。

ヒント　スタック構成のデバイスの場合、アプライアンス エディタの [デバイス（Devices）] ページで、個々のデバイスの管理オプションを変更します。

手順 4　[管理（Management）] セクションの横にある編集アイコン（ ）をクリックします。

[管理（Management）] ポップアップ ウィンドウが表示されます。

手順 5　[ホスト（Host）] フィールドに、管理ホストの名前または IP アドレスを入力します。

手順 6　[保存（Save）] をクリックします。

変更が保存されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくはデバイスへの変更の適用（4-27 ページ）を参照してください）。

高度なデバイス設定について

ライセンス：任意（Any）

サポートされるデバイス：機能に応じて異なる

[デバイス（Device）] タブの [詳細設定（Advanced）] セクションには、次の表に示すように、構成時の詳細設定が表示されます。

表 4-3　[詳細設定（Advanced）] セクション テーブルのフィールド

フィールド	説明	サポートされるデバイス
アプリケーション バイパス（Application Bypass）	デバイスでの自動アプリケーション バイパスの状態。	シリーズ 2、シリーズ 3、仮想
バイパスしきい値（Bypass Threshold）	自動アプリケーション バイパスのしきい値（ミリ秒）。	シリーズ 2、シリーズ 3、仮想
ローカル ルータ トラフィックの検査（Inspect Local Router Traffic）	デバイスで、ルーテッド インターフェイスで受信した自己を宛先とするトラフィック（ICMP、DHCP、および OSPF トラフィックなど）を検査するかどうかを示します。	シリーズ 3
高速パス ルール（Fast-Path Rules）	デバイス上に作成されている高速パス ルールの数。	8000 シリーズ、3D9900

上記の設定は、いずれも [詳細設定（Advanced）] セクションを使用して編集できます。詳細については、次の各項を参照してください。

- 自動アプリケーション バイパス（4-60 ページ）
- 詳細なデバイス設定の編集（4-61 ページ）
- 高速パス ルールの設定（4-62 ページ）

自動アプリケーション バイパス

ライセンス：任意（Any）

自動アプリケーション バイパス（AAB）機能は、インターフェイスでのパケット処理時間に制限を設け、この時間を超過した場合、パケットに検出のバイパスを許可します。この機能は任意の展開で使用できますが、インライン展開ではとりわけ価値があります。

パケット処理の遅延は、ネットワークで許容できるパケット レイテンシとバランスを取って調整します。Snort 内での不具合やデバイスの誤った設定が原因で、トラフィックの処理時間が指定のしきい値を超えると、AAB により、その障害発生から 10 分以内に Snort が再起動され、トラブルシューティング データが生成されます。このデータを分析することで、過剰な処理時間の原因を調査できます。

バージョン 5.4.1 以降での AAB オプションのデフォルト動作は、デバイスによって以下のように異なります。

- シリーズ 3：off
- シリーズ 2 および仮想：オン
- ASA FirePOWER：未サポート
- X-シリーズ：未サポート

5.3 より前のバージョンからアップグレードする場合は、既存の設定が保持されます。このオプションが選択されている場合は、バイパスしきい値を変更できます。デフォルト設定は 3000 ミリ秒（ms）です。有効な範囲は 250 ms ～ 60,000 ms です。

一般に、レイテンシしきい値を超えた後は、高速パス パケットに対して侵入ポリシーのルール遅延しきい値（Rule Latency Thresholding）を使用します。ルール遅延しきい値（Rule Latency Thresholding）により、エンジンがシャットダウンされたり、トラブルシュート データが生成されたりすることはありません。詳細については、パケットおよび侵入ルール遅延しきい値の設定（18-14 ページ）を参照してください。

（注） AAB がアクティブ化されるのは、単一パケットに過剰な処理時間がかかっている場合のみです。AAB により Snort プロセスが再起動された場合は、一時的にトラフィック インスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort の再開によるトラフィックへの影響（1-9 ページ）を参照してください。

検出がバイパスされると、デバイスがヘルス モニタリング アラートを生成します。このヘルス モニタリング アラートの詳細については、ヘルス モニタの使用（68-46 ページ）を参照してください。

自動アプリケーション バイパスを有効にしてバイパスしきい値を設定する方法の詳細については、詳細なデバイス設定の編集（4-61 ページ）を参照してください。

詳細なデバイス設定の編集

ライセンス：任意（Any）

サポートされるデバイス：機能に応じて異なる

[デバイス（Devices）] タブの [詳細設定（Advanced）] セクションを使用して、[自動アプリケーション バイパス（Automatic Application Bypass）] および [ローカル ルータ トラフィックの検査（Inspect Local Router Traffic）] の設定を変更できます。また、高速パス ルールの設定（4-62 ページ）で説明する手順に従って、高速パス ルールを設定することもできます。

次の点に注意してください。

- 高速パス ルールを設定できるのは、8000 シリーズ および 3D9900 デバイスのみです。
- [ローカル ルータ トラフィックの検査（Inspect Local Router Traffic）] を設定できるのは、シリーズ 3 デバイスのみです。

詳細なデバイス設定を変更するには、以下を行います。

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　高度なデバイス設定を編集するデバイスの横にある編集アイコン（  ）をクリックします。

デバイスの [インターフェイス（Interfaces）] タブが表示されます。

手順 3　[デバイス（Device）] をクリックします。

[デバイス（Devices）] タブが表示されます。

ヒント　スタックに含まれるデバイスの場合、アプライアンス エディタの [スタック（Stack）] ページで、スタックの高度なデバイス設定を編集します。

手順 4　[詳細設定（Advanced）] セクションの横にある編集アイコン（  ）をクリックします。

[詳細設定（Advanced）] ポップアップ ウィンドウが表示されます。

手順 5　ネットワークがレイテンシの影響を受けやすい場合は、必要に応じて、[自動アプリケーション バイパス（Automatic Application Bypass）] を選択します。自動アプリケーション バイパスは、インライン展開でとりわけ役立ちます。詳細については、自動アプリケーション バイパス（4-60 ページ）を参照してください。

手順 6　[自動アプリケーション バイパス（Automatic Application Bypass）] オプションを選択すると、[バイパスしきい値（Bypass Threshold）] にバイパスしきい値（ミリ秒）を入力できるようになります。デフォルト設定は 3000 ms です。有効な範囲は 250 ms ～ 60,000 ms です。

手順 7　ルータとして展開されている場合は、必要に応じて [ローカル ルータ トラフィックの検査（Inspect Local Router Traffic）] チェックボックスをオンにして例外トラフィックを検査します。

手順 8　（任意）高速パス ルールを設定します。詳細については、高速パス ルールの設定（4-62 ページ）を参照してください。

手順 9　[保存（Save）] をクリックします。

変更が保存されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくはデバイスへの変更の適用（4-27 ページ）を参照してください）。

高速パス ルールの設定

ライセンス:任意（Any）

サポートされるデバイス:8000 シリーズ、3D9900

高速パス ルールを作成すると、さらに検査することなく、デバイスを介して直接トラフィックを送信できます。高速パス ルールは、分析する必要のないトラフィックを転送してデバイスをバイパスさせます。高速パス ルールは、トラフィックを（インターフェイス外の）高速パスに送信するか、あるいは引き続きデバイスに送信してさらに分析を行えるようにします。これを使用する利点は、トラフィックに適切なパスを判断する速度にあります。高速パス ルールはハードウェア レベルで機能するため、パケットに関する限られた情報だけを確認します。

詳細については、次の各項を参照してください。

- IPv4 高速パス ルールの追加（4-62 ページ）
- IPv6 高速パス ルールの追加（4-64 ページ）
- 高速パス ルールの削除（4-65 ページ）

IPv4 高速パス ルールの追加

ライセンス:任意（Any）

サポートされるデバイス:8000 シリーズ、3D9900

高速パス ルールは、トラフィックを（インターフェイス外の）高速パスに送信するか、あるいはデバイスに送信してさらに分析を行えるようにします。高速パスに転送して検査を行わない IPv4 トラフィックを、以下の基準を使用して選択できます。

- 発信側または応答側の IP アドレスまたは CIDR ブロック
- プロトコル
- 発信側または応答側ポート（TCP または UDP プロトコルの場合）
- VLAN ID（Admin. VLAN ID）
- 双方向オプション

高速パス ルールには、最も外側の ID が使用されるので注意してください。

ヒント　既存の高速パス ルールを編集するには、ルールの横にある編集アイコン（）をクリックします。

IPv4 高速パス ルールの作成または編集方法:

アクセス: Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　高速パス ルールを追加するデバイスの横にある編集アイコン（）をクリックします。

デバイスの [インターフェイス（Interfaces）] タブが表示されます。

手順 3　[デバイス（Device）] をクリックします。

[デバイス（Devices）] タブが表示されます。

手順 4　[詳細設定(Advanced)] セクションの横にある編集アイコン( )をクリックします。

[詳細設定(Advanced)] ポップアップ ウィンドウが表示されます。

手順 5　高速パス ルールを追加するには、[新しい IPv4 ルール(New IPv4 Rule)] をクリックします。

[新しい IPv4 ルール(New IPv4 Rule)] ポップアップ ウィンドウが表示されます。

手順 6　[ドメイン(Domain)] ドロップダウン リストから、インライン セットまたはパッシブ セキュリティ ゾーンを選択します。詳細については、IPS デバイスの設定(5-1 ページ)を参照してください。

手順 7　[イニシエータ(Initiator)] および [応答者(Responder)] フィールドに、パケットが以後の分析をバイパスする発信側または応答側の IP アドレスを、CIDR 表記を使用して指定します。

指定された発信側からのパケット、または指定された応答側へのパケットが、ルールと照合されます。FireSIGHT システムでの CIDR 表記の使用法の詳細については、IP アドレスの表記規則(1-24 ページ)を参照してください。

手順 8　(任意)[プロトコル(Protocol)] ドロップダウン リストから、ルールの対象となるプロトコルを選択するか、[すべて(All)] を選択してリストのあらゆるプロトコルのトラフィックを照合するようにします。

手順 9　ステップ 8 で TCP または UDP プロトコルを選択した場合は、必要に応じて、[イニシエータ ポート(Initiator Port)] および [応答側ポート(Responder Port)] フィールドに発信側と応答側のポートを入力して、対象とするポートを指定します。

ヒント　ルールごとに、カンマで区切ったポート番号のリストを入力できます。IPv4 高速パス ルールでは、ポート範囲を使用できません。空白のポート値は、[任意(Any)] として扱われることに注意してください。

[双方向(Bidirectional)] オプションも選択した場合は、発信側ポートからのパケットまたは応答側へのパケットにフィルタ条件が絞り込まれます。

手順 10　必要に応じて、[VLAN] フィールドに VLAN ID を入力します。

その VLAN のトラフィックのみがルールと照合されます。空白の VLAN 値は、[任意(Any)] として扱われることに注意してください。

手順 11　必要に応じて、指定した発信側 IP アドレスと応答側 IP アドレスの間で送受信されるすべてのトラフィックをフィルタリングするには、[双方向(Bidirectional)] オプションを選択します。指定した発信側 IP アドレスから指定した応答側 IP アドレスへのトラフィックのみをフィルタリングする場合は、このオプションをクリアします。

手順 12　[保存(Save)] をクリックします。

[詳細設定(Advanced)] ポップアップ ウィンドウの [高速パス ルール(Fast-Path Rules)] にルールが追加されます。ルールが追加されても、[保存(Save)] をクリックしなければルールは保存されません。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください(詳しくはデバイスへの変更の適用(4-27 ページ)を参照してください)。

IPv6 高速パス ルールの追加

ライセンス：任意（Any）

サポートされるデバイス：シリーズ 3、3D9900

高速パス ルールは、トラフィックを（インターフェイス外の）高速パスに送信するか、あるいはデバイスに送信してさらに分析を行えるようにします。高速パスに転送して検査を行わない IPv6 トラフィックを、以下の基準を使用して選択できます。

- 発信側または応答側の IP アドレスまたはアドレス ブロック
- プロトコル
- 発信側または応答側ポート（TCP または UDP プロトコルの場合）
- VLAN ID（Admin. VLAN ID）
- 双方向オプション

高速パス ルールには、最も外側の VLAN ID が使用されるので注意してください。

ヒント　既存の高速パス ルールを編集するには、ルールの横にある編集アイコン（）をクリックします。

IPv6 高速パス ルールの追加方法：

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　高速パス ルールを追加するデバイスの横にある編集アイコン（）をクリックします。

デバイスの [インターフェイス（Interfaces）] タブが表示されます。

手順 3　[デバイス（Device）] をクリックします。

[デバイス（Devices）] タブが表示されます。

手順 4　[詳細設定（Advanced）] セクションの横にある編集アイコンをクリックします。

[詳細設定（Advanced）] ポップアップ ウィンドウが表示されます。

手順 5　高速パス ルールを追加するには、[新しい IPv6 ルール（New IPv6 Rule）] をクリックします。

[新しい IPv6 ルール（New IPv6 Rule）] ポップアップ ウィンドウが表示されます。発信側と応答側のフィールドは固定されていることに注意してください。これらのフィールドは、発信側または応答側の IPv6 パケットにフィルタが適用されることを示しています。

手順 6　[ドメイン（Domain）] ドロップダウン リストから、インライン セットまたはパッシブ セキュリティ ゾーンを選択します。詳細については、IPS デバイスの設定（5-1 ページ）を参照してください。

手順 7　パケットが以後の分析をバイパスする発信側または応答側の IP アドレスに関して、[イニシエータ（Initiator）] または [応答者（Responder）] フィールドに、IP アドレスを入力するか、または IPv6 プレフィックス長の表記を使用してアドレス ブロックを指定します。

指定された発信側からのパケット、または指定された応答側へのパケットが、ルールと照合されます。FireSIGHT システムで IPv6 プレフィックス長の表記を使用する方法については、IP アドレスの表記規則（1-24 ページ）を参照してください。

手順 8　(任意)[プロトコル(Protocol)] ドロップダウン リストから、ルールの対象となるプロトコルを選択するか、[すべて(All)] を選択してリストのあらゆるプロトコルのトラフィックを照合するようにします。

選択したプロトコルのパケットだけが高速パス ルールと照合されます。

手順 9　ステップ 7 で TCP または UDP プロトコルを選択した場合は、必要に応じて、[イニシエータ ポート(Initiator Port)] および [応答側ポート(Responder Port)] フィールドに発信側と応答側のポートを入力して、対象とするポートを指定します。

ヒント　ルールごとに、カンマで区切ったポート番号のリストを入力できます。IPv6 高速パス ルールでは、ポート範囲を使用できません。空白のポート値は、[任意(Any)] として扱われることに注意してください。

手順 10　必要に応じて、[VLAN] フィールドに VLAN ID を入力します。

その VLAN のトラフィックのみがルールと照合されます。空白の VLAN 値は、[任意(Any)] として扱われることに注意してください。

手順 11　必要に応じて、[双方向(Bidirectional)] を選択して、指定した発信側と応答側のポート間で送受信されるすべてのトラフィックをフィルタリングします。発信側ポートからのパケットのみ、または応答側ポートへのパケットのみをルールと照合することを指定する場合は、このオプションをクリアします。

手順 12　[保存(Save)] をクリックします。

[詳細設定(Advanced)] ポップアップ ウィンドウの [高速パス ルール(Fast-Path Rules)] にルールが追加されます。

手順 13　[詳細設定(Advanced)] ポップアップ ウィンドウで、[保存(Save)] をクリックします。

ルールが保存されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください(詳しくはデバイスへの変更の適用(4-27 ページ)を参照してください)。

高速パス ルールの削除

ライセンス:任意(Any)

サポートされるデバイス:8000 シリーズ、3D9900

以下の手順では、IPv4 または IPv6 高速パス ルールを削除する方法について説明します。

高速パス ルールの削除方法:

アクセス: Admin/Network Admin

手順 1　[デバイス(Devices)] > [デバイス管理(Device Management)] を選択します。

[デバイス管理(Device Management)] ページが表示されます。

手順 2　高速パス ルールを削除するデバイスの横にある編集アイコン( )をクリックします。

デバイスの [インターフェイス(Interfaces)] タブが表示されます。

手順 3　[デバイス(Device)] をクリックします。

[デバイス(Devices)] タブが表示されます。

手順 4　[詳細設定(Advanced)] セクションの横にある編集アイコン( )をクリックします。

[詳細設定(Advanced)] ポップアップ ウィンドウが表示されます。

手順 5　削除する高速パス ルールの横にある削除アイコン( )をクリックします。

手順 6　プロンプトが表示されたら、ルールを削除することを確認します。

ルールが [詳細設定(Advanced)] ポップアップ ウィンドウから削除されます。

手順 7　[保存(Save)] をクリックします。

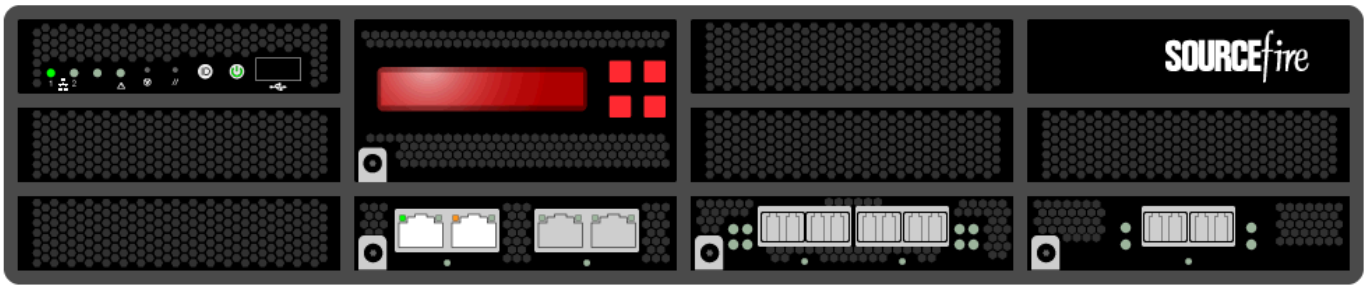
変更が保存されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください(詳しくはデバイスへの変更の適用(4-27 ページ)を参照してください)。

センシング インターフェイスの設定

ライセンス:任意(Any)

アプライアンス エディタの [インターフェイス(Interfaces)] ページで、FireSIGHT システムの展開に応じて、管理対象デバイスのセンシング インターフェイスを設定できます。

[インターフェイス(Interfaces)] ページの上部に、管理対象の シリーズ 3 デバイスの物理ハードウェア ビューが表示されます。シリーズ 2、仮想デバイス、Blue Coat X-Series 向け Cisco NGIPS、および ASA FirePOWER デバイスには、物理ハードウェアのビューはありません。以下の図は、3D8250 のハードウェア ビューを示しています。



以下の表では、物理ハードウェア ビューの使用法について説明しています。

表 4-4　ハードウェア ビューの使用法

目的	操作
ネットワーク モジュールのタイプ、部品番号、およびシリアル番号を確認する	ネットワーク モジュールの左下隅にある暗い円の上にマウスのカーソルを重ねます。
インターフェイス テーブル ビューでインターフェイスを選択する	インターフェイスをクリックします。
インターフェイス エディタを開く	インターフェイスをダブルクリックします。
インターフェイスの名前、タイプ、リンクの有無、速度設定、およびインターフェイスがバイパス モードになっているかを確認する	インターフェイスの上にマウスのカーソルを重ねます。
エラーまたは警告の詳細を参照する	ネットワーク モジュールの該当するポートの上にマウスのカーソルを重ねます。

シリーズ 3 ハードウェア ビューの下にあるインターフェイス テーブル ビューには、デバイスで使用可能なすべてのインターフェイスが一覧表示されます。テーブル内のナビゲーション ツリーを展開すると、設定されているすべてのインターフェイスを表示できます。インターフェイスの横にある矢印アイコンをクリックして、インターフェイスを縮小または展開することで、サブコンポーネントの非表示/表示を切り替えることができます。このインターフェイス テーブル ビューには、各インターフェイスに関する以下の要約情報が表示されます。[MAC アドレス(MAC Address)] 列と [IP アドレス(IP Address)] 列が表示されるのは、8000 シリーズ デバイスのみです。詳細については、以下の表を参照してください。

表 4-5　インターフェイス テーブル ビューのフィールド

フィールド	説明
名前(Name)	各インターフェイス タイプは、タイプとリンク ステート(該当する場合)を示す固有のアイコンによって表されます。名前またはアイコンの上にマウス ポインタを移動すると、インターフェイス タイプ、速度、デュプレックス モード(該当する場合)がツールチップに表示されます。インターフェイス アイコンについては、表 4-6(4-68 ページ)を参照してください。 アイコンでは、インターフェイスの現在のリンク ステートを示す表示方法が使用されています。次の 3 つの状態のいずれかが表示されます。 • エラー() • 障害() • 利用不可() 論理インターフェイスのリンク ステートは、親物理インターフェイスのリンク ステートと同じです。Blue Coat X-Series 向け Cisco NGIPS および ASA FirePOWER デバイスには、リンク ステートは表示されません。無効化されたインターフェイスは、半透明のアイコンで表されます。 アイコンの右側に表示されるインターフェイス名は自動生成されます。ただし、ハイブリッド インターフェイスと ASA FirePOWER インターフェイスの名前はユーザによって定義されます。ASA FirePOWER インターフェイスについては、有効で、名前が付けられており、リンクを持つインターフェイスのみが表示されることに注意してください。 物理インターフェイスでは、物理インターフェイスの名前が表示されます。論理インターフェイスでは、物理インターフェイスの名前と、割り当てられている VLAN タグが表示されます。 ASA FirePOWER インターフェイスでは、複数のセキュリティ コンテキストがある場合は、セキュリティ コンテキストの名前とインターフェイスの名前が表示されます。セキュリティ コンテキストが 1 つしかない場合は、インターフェイスの名前のみが表示されます。
セキュリティ ゾーン(Security Zone)	インターフェイスが割り当てられているセキュリティ ゾーン。セキュリティ ゾーンを追加または編集するには、編集アイコン()をクリックします。
使用者(Used by)	インターフェイスが割り当てられているインライン セット、仮想スイッチ、または仮想ルータ。ASA FirePOWER デバイスには、[使用者(Used by)] 列は表示されません。

表 4-5　インターフェイス テーブル ビューのフィールド(続き)

フィールド	説明
MAC アドレス(MAC Address)	スイッチド機能およびルーテッド機能で有効にされているインターフェイスに対して表示される MAC アドレス。 仮想デバイスの場合、表示された MAC アドレスにより、デバイス上に設定されたネットワーク アダプタと、[インターフェイス(Interfaces)] ページに表示されるインターフェイスを照合できます。Blue Coat X-Series 向け Cisco NGIPS および ASA FirePOWER デバイスには、MAC アドレスは表示されません。
IP アドレス(IP Address)	インターフェイスに割り当てられた IP アドレス。マウスのポインタを IP アドレスの上に重ねると、その IP アドレスがアクティブであるか非アクティブであるかを確認できます。非アクティブな IP アドレスはグレー表示されます。ASA FirePOWER デバイスには、IP アドレスは表示されません。

表 4-6　インターフェイス アイコンのタイプと説明

アイコン	インターフェイス タイプ	詳細
	物理的:未設定の物理インターフェイス。	—
	パッシブ:パッシブ展開でトラフィックを分析するように設定されているセンシング インターフェイス。	パッシブ インターフェイスの設定(5-2 ページ)
	インライン:インライン展開でトラフィックを処理するように設定されているセンシング インターフェイス。	インライン インターフェイスの設定(5-3 ページ)
	スイッチド:レイヤ 2 展開でトラフィックを切り替えるように設定されているインターフェイス。	スイッチド インターフェイスの設定(6-2 ページ)
	ルーテッド:レイヤ 3 展開でトラフィックをルーティングするように設定されているインターフェイス。	ルーテッド インターフェイスの設定(7-2 ページ)
	HA:デバイス間で冗長通信チャネルとして機能するように設定されている、デバイスのクラスタペア メンバー上のインターフェイスで、ハイ アベイラビリティ リンク インターフェイスとも呼ばれます。	HA リンク インターフェイスの設定(4-69 ページ)
	集約:1 つの論理リンクとして設定されている複数の物理インターフェイス。	集約インターフェイスのセットアップ(8-1 ページ)
	集約スイッチド:レイヤ 2 展開で 1 つの論理リンクとして設定されている複数の物理インターフェイス。	集約スイッチド インターフェイスの追加(8-5 ページ)
	集約ルーテッド:レイヤ 3 展開で 1 つの論理リンクとして設定されている複数の物理インターフェイス。	集約ルーテッド インターフェイスの追加(8-8 ページ)
	ハイブリッド:仮想ルータと仮想スイッチ間でトラフィックをブリッジするように設定されている論理インターフェイス。	論理ハイブリッド インターフェイスの追加(9-1 ページ)
	ASA FirePOWER:ASA FirePOWER モジュールがインストールされた ASA デバイスに設定されているインターフェイス。	Cisco ASA with FirePOWER Servicesインターフェイスの管理(4-71 ページ)

管理対象の FirePOWER デバイスには、合計 1024 個のインターフェイスを設定できることに注意してください。

(注)　防御センター では、ASA FirePOWER デバイスが SPAN ポート モードで展開されている場合、ASA インターフェイスを表示しません。

デバイスにインターフェイスを設定するさまざまな方法の詳細については、以下の項を参照してください。

- HA リンク インターフェイスの設定（4-69 ページ）
- 管理対象デバイスの MTU の範囲（4-70 ページ）
- Cisco ASA with FirePOWER Servicesインターフェイスの管理（4-71 ページ）
- インターフェイスの無効化（4-72 ページ）
- 重複する接続ロギングの防止（4-73 ページ）
- IPS デバイスの設定（5-1 ページ）
- 仮想スイッチのセットアップ（6-1 ページ）
- 仮想ルータのセットアップ（7-1 ページ）
- 集約インターフェイスのセットアップ（8-1 ページ）
- ハイブリッド インターフェイスの設定（9-1 ページ）

HA リンク インターフェイスの設定

ライセンス：任意（Any）

サポートされるデバイス：シリーズ 3

デバイス クラスタを確立した後、物理インターフェイスをハイ アベイラビリティ（HA）リンク インターフェイスとして設定できます。このリンクは、クラスタを構成するデバイス間でヘルス情報を共有するために使用する、冗長通信チャネルとして機能します。1 つのデバイスに HA リンク インターフェイスを設定すると、自動的に 2 番目のデバイスにインターフェイスが設定されます。同じブロードキャスト ドメインに、両方の HA リンクを設定する必要があります。詳細については、デバイスのクラスタリング（4-31 ページ）を参照してください。

ダイナミック NAT は、他の IP アドレスとポートにマップする IP アドレスとポートの動的割り当てに依存します。HA リンクがなければ、これらのマッピングはフェールオーバーで失われます。その場合、変換されたすべての接続はクラスタ内で新しくアクティブになったデバイスを介してルーティングされることになるため、それらの接続は失敗します。

注意　センシング インターフェイスまたはインライン セットの MTU の任意の値（シリーズ 2）または最高値（シリーズ 3）を変更すると、変更を適用する際、変更したインターフェイスだけではなく、デバイス上のすべてのセンシング インターフェイスに対するトラフィック インスペクションが一時的に中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。Snort の再開によるトラフィックへの影響（1-9 ページ）を参照してください。

HA リンク インターフェイスを設定するには、以下を行います。

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　HA リンク インターフェイスを設定する、クラスタを構成するデバイスの横にある編集アイコン（）をクリックします。

デバイスの [インターフェイス（Interfaces）] タブが表示されます。

手順 3　HA リンク インターフェイスとして設定するインターフェイスの横にある編集アイコン（）をクリックします。

[インターフェイスの編集（Edit Interface）] ポップアップ ウィンドウが表示されます。

手順 4　[HA リンク（HA Link）] をクリックして HA リンク オプションを表示します。

手順 5　[有効（Enabled）] チェックボックスをオンにして、HA リンク インターフェイスがリンクを提供できるようにします。

このチェック ボックスをオフにすると、インターフェイスは無効になり、管理上はダウンした状態になります。

手順 6　[モード（Mode）] ドロップダウン リストからリンク モードを指定するオプションを選択するか、[自動ネゴシエーション（Autonegotiation）] を選択して、速度とデュプレックスの設定を自動ネゴシエートするようにインターフェイスを設定します。

手順 7　[MDI/MDIX] ドロップダウン リストから、インターフェイスの設定対象として MDI（メディア依存型インターフェイス）、MDIX（メディア依存型インターフェイス クロスオーバー）、または Auto-MDIX のいずれかを指定するオプションを選択します。

通常、[MDI/MDIX] は [Auto-MDIX] に設定します。これにより、MDI と MDIX の間の切り替えが自動的に処理され、リンクが確立されます。

手順 8　[MTU] フィールドに最大伝送ユニット（MTU）を入力して、パケットの最大許容サイズを指定します。

設定可能な MTU の範囲は、FireSIGHT システムのデバイス モデルおよびインターフェイスのタイプによって異なる場合があります。詳細については、管理対象デバイスの MTU の範囲（4-70 ページ）を参照してください。

手順 9　[保存（Save）] をクリックします。

変更が保存されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくはデバイスへの変更の適用（4-27 ページ）を参照してください）。

管理対象デバイスの MTU の範囲

ライセンス：任意（Any）

注意　センシング インターフェイスまたはインライン セットの MTU の任意の値（シリーズ 2）または最高値（シリーズ 3）を変更すると、変更を適用する際、変更したインターフェイスだけではなく、デバイス上のすべてのセンシング インターフェイスに対するトラフィック インスペクションが一時的に中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。Snort の再開によるトラフィックへの影響（1-9 ページ）を参照してください。

Blue Coat X-Series 向け Cisco NGIPS の場合は、Blue Coat X-Series 向け Cisco NGIPS CLI を使用してインターフェイス MTU を設定することに注意してください。詳細については、『*Blue Coat X-Series 向け Cisco NGIPS Installation Guide*』を参照してください。

(注)　システムは、設定された MTU 値から自動的に 18 バイトを削減するため、IPv6 の場合、1298 未満の値は MTU の最小値である 1280 に準拠しません。IPv4 の場合は、594 未満の値は MTU の最小値 576 に準拠しません。たとえば、構成値 576 は自動的に 558 に削減されます。

次の表に、管理対象デバイスの MTU 設定範囲を示します。

表 4-7　デバイスごとの MTU 範囲

デバイス モデル	MTU 範囲
シリーズ 2（3D6500、3D9900 を除く）	576 ～ 1518（すべてのインターフェイス、インライン セット）
3D6500、3D9900、仮想	576 ～ 9018（すべてのインターフェイス、インライン セット）
シリーズ 3	576 ～ 9234（管理インターフェイス） 576 ～ 10172（インライン セット、パッシブ インターフェイス） 576 ～ 9922（その他）

Cisco ASA with FirePOWER Servicesインターフェイスの管理

ライセンス：Protection

サポートされるデバイス：ASA FirePOWER

ASA FirePOWER インターフェイスを編集する際に、FireSIGHT 防御センター から設定できるのは、インターフェイスのセキュリティ ゾーンのみです。詳細については、セキュリティ ゾーンの操作（3-44 ページ）を参照してください。

ASA FirePOWER インターフェイスを完全に設定するには、ASA 専用ソフトウェアおよび CLI を使用します。ASA FirePOWER デバイスを編集して、マルチ コンテキスト モードからシングル コンテキスト モード（またはその逆）に切り替えると、デバイスはそのインターフェイスの名前をすべて変更します。更新されたASA FirePOWER のインターフェイス名を使用する、すべての FireSIGHT システム セキュリティ ゾーン、相関ルール、および関連する設定の再設定が必要です。ASA FirePOWER インターフェイスの設定の詳細については、ASA のドキュメンテーションを参照してください。

(注)　ASA FirePOWER インターフェイスのタイプは変更できません。また、FireSIGHT 防御センターからインターフェイスを無効にすることもできません。

ASA FirePOWER インターフェイスを編集するには、以下を行います。

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　インターフェイスを編集するデバイスの横にある編集アイコン（）をクリックします。

デバイスの [インターフェイス（Interfaces）] タブが表示されます。

手順 3　編集するインターフェイスの横にある編集アイコン（）をクリックします。

[インターフェイスの編集（Edit Interface）] ポップアップ ウィンドウが表示されます。

手順 4　[セキュリティ ゾーン（Security Zone）] ドロップダウンリストから、既存のセキュリティ ゾーンを選択するか、または [新規（New）] を選択して、新しいセキュリティ ゾーンを追加します。

手順 5　[保存（Save）] をクリックします。

セキュリティ ゾーンが設定されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくはデバイスへの変更の適用（4-27 ページ）を参照してください）。

インターフェイスの無効化

ライセンス：任意（Any）

インターフェイス タイプを [なし（None）] に設定することで、インターフェイスを無効にすることができます。無効にされたインターフェイスは、インターフェイス リストでグレー表示されます。

（注）　ASA FirePOWER インターフェイスのタイプは変更できません。また、FireSIGHT 防御センターからインターフェイスを無効にすることもできません。

インターフェイスを無効にするには、以下を行います。

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

手順 2　インターフェイスを無効にするデバイスの横にある編集アイコン（）をクリックします。

デバイスの [インターフェイス（Interfaces）] タブが表示されます。

手順 3　無効にするインターフェイスの横にある編集アイコン（）をクリックします。

[インターフェイスの編集（Edit Interface）] ポップアップ ウィンドウが表示されます。

手順 4　[なし（None）] をクリックします。

手順 5　[保存（Save）] をクリックします。

変更が保存されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくはデバイスへの変更の適用（4-27 ページ）を参照してください）。

重複する接続ロギングの防止

ライセンス：任意（Any）

セキュリティ ゾーン オブジェクトを更新すると、システムはそのオブジェクトの新しいリビジョンを保存します。その結果、同じセキュリティ ゾーン内の管理対象デバイスに、インターフェイスで設定されたセキュリティ オブジェクトの異なるリビジョンがある場合、接続が重複しているようなログが記録される可能性があります。

接続の重複が報告されていることに気づいた場合、同じリビジョンのオブジェクトを使用するよう、すべての管理対象デバイスを更新できます。

デバイス全体でセキュリティ ゾーン オブジェクトのリビジョンを同期するには、以下を行います。

アクセス：Admin/Network Admin

手順 1　[デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

[デバイス管理（Device Management）] ページが表示されます。

注意　同期させるすべてのデバイスでインターフェイスのゾーン設定を編集するまでは、管理対象デバイスの変更を他のデバイスに再適用しないでください。

手順 2　セキュリティ ゾーンの選択を更新するデバイスの横にある編集アイコン（ ）をクリックします。

デバイスの [インターフェイス（Interfaces）] タブが表示されます。

手順 3　重複する接続のイベントを記録しているインターフェイスのそれぞれについて、[セキュリティ ゾーン（Security Zone）] を別のゾーンに変更して [保存（Save）] をクリックした後、目的のゾーンに再び設定し、もう一度 [保存（Save）] をクリックします。

手順 4　重複イベントを記録しているデバイスごとに、ステップ 2 から 3 を繰り返します。

手順 5　すべてのデバイスのすべてのインターフェイスを編集した後、デバイスの変更を同時にすべての管理対象デバイスに適用します。