デバイスの管理

防御センターは、FireSIGHT システムの主要コンポーネントです。FireSIGHT システムを構成するあらゆる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一箇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。
- ヘルス 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 ステータスを監視できます。

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監視して、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」（P.6-2）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。
- 「NAT 環境での作業」（P.6-3）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」（P.6-4）では、運用を継続できるように 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」（P.6-15）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。
- 「リモート管理の設定」（P.6-21）では、管理対象デバイスのリモート管理を確立する方法と、無効にする方法について説明しています。
- 「デバイス グループの管理」（P.6-24）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または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」（P.6-26）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」（P.6-47）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。
- 「スタックに含まれるデバイスの管理」（P.6-40）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。
- 「インターフェイスの設定」（P.6-58）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」（P.6-2）
- 「ポリシーとイベント以外の機能」（P.6-3）
- 「冗長防御センターの使用」（P.6-3）

防御センターで管理できるデバイス

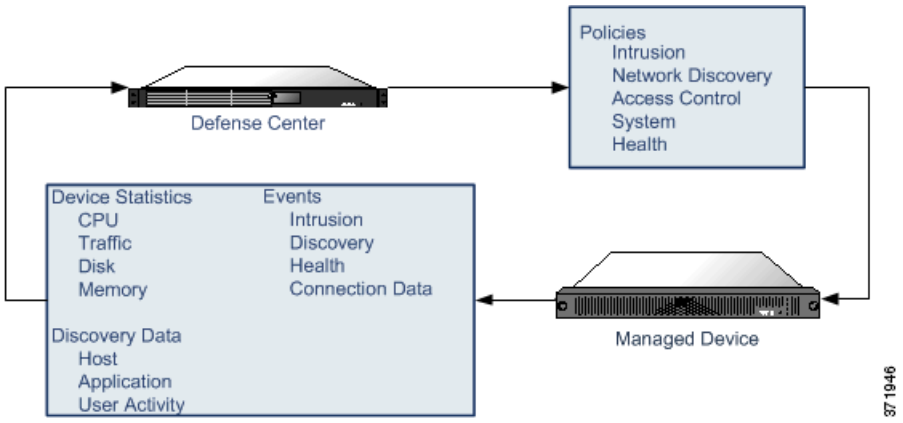
FireSIGHT システムの展開環境の中央管理ポイントとして防御センターを使用することで、以下のデバイスを管理できます。

- 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 Sourcefire Software for X-Series 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は最大で 3 つまで（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約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 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

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

イベント データを防御センターに送信するだけでなく、デバイスでの保存も行っている場合、デバイスに保存されたイベントを防御センターの Web インターフェイスを使用してバックアップできます。詳細については、「防御センターによる管理対象デバイスのバックアップ」（P.57-5）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
- ジオロケーションの更新
- 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。

冗長防御センターの使用

ライセンス：任意

サポート対象防御センター：DC1000、DC1500、DC3000、DC3500

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、ユーザ アカウントなどは、2 つの防御センター間で共有されます。イベントは自動的に両方の防御センターに送信されます。詳細については、「ハイ アベイラビリティの設定」（P.6-4）を参照してください。

NAT 環境での作業

ライセンス：Control

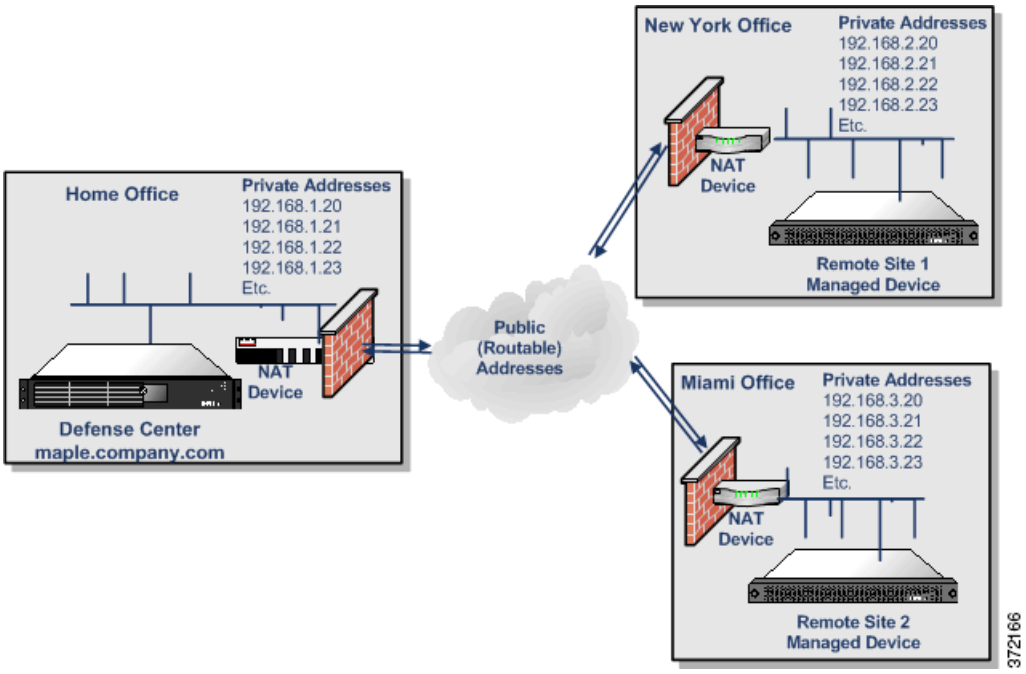
ネットワーク アドレス変換（NAT）とは、ルータを介したネットワーク トラフィックの送受信方式であり、ルータ経由でトラフィックがパススルーされるときに送信元または宛先 IP アドレスの再割り当てが行われます。NAT を使用した標準的なアプリケーションでは、プライベート ネットワーク上の複数のホストが、単一のパブリック IP アドレスを使用してパブリック ネットワークにアクセスできます。

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**。

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

サポート対象防御センター：DC1000、DC1500、DC3000、DC3500

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。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、および特定の設定要素は、両方の防御センターに維持されます。一方の防御センターで障害が発生しても、もう一方の防御センターを使用してネットワークの監視を中断せずに続行できます。

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 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 ステータスのモニタリングおよび変更」（P.6-11）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」（P.6-5）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」（P.6-9）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」（P.6-10）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」（P.6-11）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」（P.6-13）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」（P.6-14）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」（P.6-14）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

サポート対象防御センター：DC1000、DC1500、DC3000、DC3500

DC1500 および DC3500 ではハイ 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で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。防御センター 1500 と 防御センター 3500 との間には、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、いずれ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。（それぞれの防御センターには 5 分間の同期サイクルがありますが、サイクル自体が同期していない状態が最大 5 分間続く可能性があるため、変更が反映されるまでに 2 回の同期サイクルが必要になることもあります）。この 10 分間は、防御センターで設定が異なっているように見えることもあります。

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、管理者特権が割り当てられた 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、同じ地理的ロケーションに存在する必要もありません。

運用の継続性を確保するためには、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 アクセスの要件」（P.E-1）を参照してください。特定の機能では、プライマリ防御センターがインターネットに接続した上で、同期プロセス中に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」（P.6-11）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」（P.6-6）
- 「ヘルス ポリシーとシステム ポリシー」（P.6-7）
- 「相関応答」（P.6-7）
- 「ライセンス」（P.6-8）
- 「URL Filtering および Security Intelligence」（P.6-8）
- 「クラウド接続およびマルウェア情報」（P.6-8）
- 「ユーザ エージェント」（P.6-9）

共有される設定

ライセンス：任意

サポート対象防御センター：DC1000、DC1500、DC3000、DC3500

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識別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
- 侵入ポリシーおよび関連するルールの状態
- ファイル ポリシー
- アクセス コントロール ポリシーおよび関連するルール
- ローカル ルール
- カスタム侵入ルールの分類
- 変数値およびユーザ定義変数

- ネットワーク検出ポリシー
- ユーザ定義アプリケーション プロトコル ディテクタと、それらのディテクタが検出す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、ジオロケーション データベース（GeoDB）、および脆弱性データベース（VDB）の更新

ヘルス ポリシーとシステム ポリシー

ライセンス：任意

サポート対象防御センター：DC1000、DC1500、DC3000、DC3500

防御センターおよび管理対象デバイスのヘルス 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、ヘルス 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ヘルス 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）
- ヘルス 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

サポート対象防御センター：DC1000、DC1500、DC3000、DC3500

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。

修正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正モジュールをアップロードしてインストールし、修正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は、プライマリ防御センターに障害が発生した場合は、すぐ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正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プロモート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」（P.6-11）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」（P.39-48）および「修復の作成」（P.41-1）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正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正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

サポート対象防御センター：DC1000、DC1500、DC3000、DC3500

ハイ アベイラビリティ 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」（P.52-1）を参照してください。

URL Filtering および Security Intelligence

ライセンス：URL Filtering または Protection

サポート対象デバイス：シリーズ 3、仮想、X-Series、ASA FirePOWER

サポート対象防御センター：DC1000、DC1500、DC3000、DC3500

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の間で同期されます。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 にプロモート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」（P.6-11）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

サポート対象デバイス：シリーズ 3、仮想、X-Series、ASA FirePOWER

サポート対象防御センター：DC1000、DC1500、DC3000、DC3500

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、「マルウェア対策とファイル制御について」（P.33-3）を参照してください。

ユーザ エージェント

ライセンス：FireSIGHT

サポート対象防御センター：DC1000、DC1500、DC3000、DC3500

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、「ネットワーク検出の概要」（P.35-1）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

サポート対象防御センター：DC1000、DC1500、DC3000、DC3500

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化（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、工場出荷時のデフォルトに復元します。その場合、イベントと構成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 System Installation Guide*』を参照してください。

注　非アクティブの防御センターでは、反復タスク スケジュールを設定できません。非アクティブからアクティブに切り替わったときに、新しくアクティブにされた防御センターで反復タスク スケジュールを再作成する必要があります。

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」（P.6-23）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

サポート対象防御センター：DC1000、DC1500、DC3000、DC3500

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」（P.6-23）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、「時刻の同期」（P.50-26）を参照してください。

ポリシーの数とそれらのポリシーが使用するカスタム標準テキスト ルールの数によっては、両方の防御センターにすべてのルールとポリシーが出現するまでに最大 10 分かかる可能性があります。[High Availability] ページを表示すると、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、[Task Status] を監視することで、プロセスが完了したことを確認できます。「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」（P.6-11）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 ペアを再確立し、既存の防御センターのデータを新しく追加された防御センターに同期します。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：Admin

ステップ 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。

ステップ 2　[System] > [Local] > [Registration] を選択します。

[Registration] ページが表示されます。

ステップ 3　[High Availability] をクリックします。

[High Availability] ページが表示されます。

ステップ 4　[secondary Defense Cente] オプションをクリックします。

[Secondary Defense Cente Setup] ページが表示されます。

ステップ 5　[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、[Registration Key] と [Unique NAT ID] の両方のフィールドを使用します。

ステップ 6　[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。

ステップ 7　必要に応じて、[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。詳細については、「NAT 環境での作業」（P.6-3）を参照してください。

ステップ 8　[Register] をクリックします。

成功メッセージが表示され、[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。

ステップ 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。

ステップ 10　[System] > [Local] > [Registration] を選択します。

[Registration] ページが表示されます。

ステップ 11　[High Availability] をクリックします。

[High Availability] ページが表示されます。

ステップ 12　[primary Defense Cente] オプションをクリックします。

[Primary Defense Cente Setup] ページが表示されます。

ステップ 13　[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。

ステップ 14　[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。

ステップ 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 [Unique NAT ID] テキスト ボックスに入力します。

ステップ 16　[Register] をクリックします。

成功メッセージが表示され、[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

サポート対象防御センター：DC1000、DC1500、DC3000、DC3500

プライマリおよびセカンダリ防御センターを識別した後は、どちらか一方を使用して、もう一方のステータス情報を表示できます。ステータス情報には以下が含まれます。

- IP アドレス
- 製品モデル
- オペレーティング システム

- オペレーティング システムのバージョン
- ローカル ロール（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、またはアクティブおよびセカンダリ）
- 防御センターの最終同期時刻

プライマリ防御センターに障害が発生した場合は、[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プロモート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 Filtering および Security Intelligence」（P.6-8）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 Filtering および Security Intelligence」（P.6-8）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」（P.6-7）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：Admin

ステップ 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。

ステップ 2　[System] > [Local] > [Registration] を選択します。

[Registration] ページが表示されます。

ステップ 3　[High Availability] をクリックします。

[High Availability] ページが表示されます。

ステップ 4　[High Availability Status] に、ハイ アベイラビリティ ペアのもう一方の防御センターに関する以下の情報がリストされます。

- IP アドレス
- モデル名
- ソフトウェアのバージョン
- オペレーティング システム
- 2 つの防御センターの間で最後の通信が行われてから経過した時間。
- ローカル ロール（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、またはアクティブおよびセカンダリ）
- 防御センターの最終同期時刻
- 2 つの防御センターの間でのロール切り替えオプション

ステップ 5　共有機能に影響する操作が行われると、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、[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 分間待機する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 ペアがあらかじめ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。

ステップ 6　[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。

ステップ 7　ツールバーの [Peer Manager] をクリックします。

[Peer Manager] ページが表示されます。

以下の情報を確認できます。

- 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」（P.6-23）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

サポート対象防御センター：DC1000、DC1500、DC3000、DC3500

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：Admin

ステップ 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。

ステップ 2　[System] > [Local] > [Registration] を選択します。

[Registration] ページが表示されます。

ステップ 3　[High Availability] をクリックします。

[High Availability] ページが表示されます。

ステップ 4　[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、[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、[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、[Unregister devices on both peers] を選択します。

ステップ 5　[Break High Availability] をクリックします。

[Do you really want to Break High Availability?] というプロンプトに対し、[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」（P.6-10）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

サポート対象防御センター：DC1000、DC1500、DC3000、DC3500

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：Admin

ステップ 1　[Peer Manager] をクリックします。

[Peer Manager] ページが表示されます。

ステップ 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」（P.6-23）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

サポート対象防御センター：DC1000、DC1500、DC3000、DC3500

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：Admin

ステップ 1　[Peer Manager] をクリックします。

[Peer Manager] ページが表示されます。

ステップ 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」（P.6-23）を参照してください。

デバイスの操作

ライセンス：任意

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。

- 「[Device Management] ページについて」（P.6-15）
- 「防御センターへのデバイスの追加」（P.6-16）
- 「リモート管理の設定」（P.6-21）
- 「デバイス グループの管理」（P.6-24）
- 「デバイスのクラスタリング」（P.6-26）
- 「デバイス設定の編集」（P.6-47）
- 「インターフェイスの設定」（P.6-58）

[Device Management] ページについて

ライセンス：任意

[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、[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」（P.6-24）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」（P.52-1）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）
- ヘルス ポリシー。詳細については、「ヘルス モニタリングの使用」（P.55-1）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」（P.50-1）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」（P.13-31）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 6-1　アプライアンス リストのフィールド

フィールド	説明
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。
License Type	管理対象デバイスで有効なライセンス。
Health Policy	デバイスに現在適用されているヘルス ポリシー。ヘルス 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。既存のヘルス 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」（P.55-33）を参照してください。
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」（P.50-1）を参照してください。
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」（P.13-31）を参照してください。

[Device Management] ページからアクセスできるその他の機能については、以下の項を参照してください。

- 「防御センターへのデバイスの追加」（P.6-16）
- 「デバイス グループの管理」（P.6-24）
- 「デバイスのクラスタリング」（P.6-26）
- 「スタックに含まれるデバイスの管理」（P.6-40）

防御センターへのデバイスの追加

ライセンス：任意

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。

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 1 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 5.3.1 を実行している場合、バージョン 5.2.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 5.1.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、「ネットワーク設定の構成」（P.51-9）を参照してください。

IPv4 を使用して登録した防御センターとデバイスを 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。

デバイスに適用するアクセス コントロール ポリシーは、デバイスを防御センターに登録する際に選択できます。デバイスで有効になっていないライセンスを必要とするポリシーを適用しようとすると、ポリシーの適用は失敗します。また、アクセス コントロール ポリシーがネットワーク検出ポリシーと関連付けられている場合、ネットワーク検出ポリシーの適用も失敗します。アクセス コントロール が管理対象デバイスに適切に適用されることが、ネットワーク検出の要件となっているためです。

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、[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」（P.6-29）または「デバイス スタックの確立」（P.6-42）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 デバイスでは、セキュリティ インテリジェンス フィルタリングを除き、Protection 機能が自動的に有効になります。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」（P.6-47）および「インターフェイスの設定」（P.6-58）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

ステップ 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」（P.6-21）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 [Pending Registration] として表示されます。

仮想デバイス、Sourcefire Software for X-Series、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インターフェイスを設定します。

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。

ステップ 2　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 3　[Add] ドロップダウン メニューから、[Add Device] を選択します。

[Add Device] ポップアップ ウィンドウが表示されます。

ステップ 4　[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た場合、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」（P.6-3）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。

ステップ 5　[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。

ステップ 6　必要に応じて、[Group] ドロップダウン リストからグループを選択して、デバイスをデバイス グループに追加します。

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」（P.6-24）を参照してください。

ステップ 7　[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。

- [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。
- [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。
- [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 ポリシーの使用」（P.13-1）を参照してください。

ステップ 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。

- ControlMalware、および 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、Sourcefire Software for X-Series、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、Sourcefire Software for X-Series、または ASA FirePOWER で有効にすることはできますが、これらのデバイスでは Fast-Path 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。
- スタックに含まれるデバイスの場合、アプライアンス エディタの [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 デバイスでは、セキュリティ インテリジェンス フィルタリングを除き、Protection 機能が自動的に有効になります。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」（P.52-1）を参照してください。

ステップ 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、[Advanced] セクションを展開して、[Unique NAT ID] フィールドに同じ NAT ID を入力します。

ステップ 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、[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。

ステップ 11 [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

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。

インターフェイスを編集して、デバイス ポリシーを再適用すると、編集したインターフェイスだけではなく、デバイスのすべてのインターフェイス インスタンスに対して Snort が再起動されることに注意してください。

ヒント デバイスに変更を適用するには、[Device Management] ページまたはアプライアンス エディタの [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

ステップ 1 [Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 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。

ステップ 3 プロンプトが出されたら、[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、[Apply Device Changes] ダイアログ ボックスで [View Changes] をクリックします。新しいブラウザ ウィンドウに [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」（P.6-20）を参照してください。

ステップ 4 [OK] をクリックします。

[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

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

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 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。

[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。

ステップ 3　[View Changes] をクリックします。

新しいウィンドウに [Device Management Revision Comparison Report] ページが表示されます。

ステップ 4　[Previous] と [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。

ステップ 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、[Comparison Report] をクリックします。

デバイスの削除

ライセンス：任意

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、デバイスを再び管理するには、削除したデバイスを防御センターに再び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 分間待機する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

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 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。

プロンプトが出されたら、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との間の通信が切断され、デバイスが [Device Management] ページから削除されます。デバイスのシステム ポリシーにより、デバイスで NTP を介して防御センターから時刻が受信されるようになっている場合、デバイスはローカル時刻の管理に戻ります。

リモート管理の設定

ライセンス：任意

ある特定の FireSIGHT システム アプライアンスで別のアプライアンスを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。仮想デバイス、Sourcefire Software for X-Series、およびASA FirePOWER デバイスのリモート管理は、デバイスのコマンド ライン インターフェイス（CLI）を使用して設定します。

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」（P.6-3）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と、ユーザが選択したアクセス コントロール ポリシーがデバイスに適用されます。さらに、防御センター上のネットワーク検出ポリシーも自動的にデバイスに適用されます。ただし、選択したアクセス コントロール ポリシーで使用される機能に必要なライセンスがデバイスで有効になっていなければ、アクセス コントロール ポリシーの適用は失敗し、それによってネットワーク検出ポリシーの適用も失敗します。たとえば、侵入ポリシーをデフォルト アクションとして使用するアクセス コントロール ポリシーを選択する場合、Protection ライセンスを有効にしなければ、アクセス コントロール ポリシーとネットワーク検出ポリシーの適用が両方とも失敗します。

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：Admin

ステップ 1　管理するアプライアンスの Web インターフェイスで、[System] > [Local] > [Registration] を選択します。

[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」（P.6-23）を参照してください。

ステップ 2　[Add Manager] をクリックします。

[Add Remote Management] ページが表示されます。

ステップ 3　[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。

ステップ 4　[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。

ステップ 5　NAT 環境の場合は、[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。

ステップ 6　[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 [Pending Registration] が表示されます。

ステップ 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」（P.6-16）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

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 1 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 5.3.0 を実行している場合、バージョン 5.2.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 5.1.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、管理対象デバイスと防御センターの間の通信チャネルをブロックできます。通信チャネルを再び有効にするには、スライダをクリックします。

リモート管理を編集するには、以下を行います。

アクセス：Admin

ステップ 1　[System] > [Local] > [Registration] を選択します。

[Remote Management] ページが表示されます。

ステップ 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。

[Edit Remote Management] ページが表示されます。

ステップ 3　[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。

ステップ 4　[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。

ステップ 5　[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

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争する場合は、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　管理ポートを変更した場合は、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。

管理ポートを変更するには、以下を行います。

アクセス：Admin

ステップ 1　[System] > [Local] > [Configuration] を選択します。

[Information] ページが表示されます。

ステップ 2　[Network] をクリックします。

[Network Settings] ページが表示されます。

ステップ 3　[Remote Management Port] フィールドに、使用するポート番号を入力します。

ステップ 4　[Save] をクリックします。

管理ポートが変更されます。

ステップ 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。

デバイス グループの管理

ライセンス：任意

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、次の項を参照してください。

- 「デバイス グループの追加」（P.6-24）
- 「デバイス グループの編集」（P.6-25）
- 「デバイス グループの削除」（P.6-26）

デバイス グループの追加

ライセンス：任意

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

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　[Add] ドロップダウン メニューから、[Add Group] を選択します。

[Add Group] ポップアップ ウィンドウが表示されます。

ステップ 3　[Name] フィールドに、グループの名前を入力します。

ステップ 4　[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。

ステップ 5　[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。

ステップ 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

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、現行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、新しいグループに既に適用されているポリシーに変更される訳ではありません。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

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 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。

[Edit Group] ポップアップ ウィンドウが表示されます。

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

ステップ 4　[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。

ステップ 5　[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。

ステップ 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。

ステップ 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

削除するデバイス グループにデバイスが含まれている場合、それらのデバイスは [Device Management] ページの [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

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 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。。

ステップ 3　プロンプトが出されたら、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

サポート対象デバイス：シリーズ 3

デバイスのクラスタリング（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構成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、「スタックに含まれるデバイスの管理」（P.6-40）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。その他の構成データは、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 クラスタを構成するには、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 n。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」（P.6-29）を参照してください。

⚠
注意　シスコから提供されたものではないハード ドライブを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**購入できます。このキットを使用できるのは、FireSIGHT システムのバージョン 5.3 以降を実行している 8000 シリーズ デバイス**のみ**です。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 System Malware Storage Pack Guide*』を参照してください。

クラスタ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でメンテナンス モードを開始します。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」（P.6-34）を参照してください。

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、またはシステム更新時に、自動フェールオーバーが行われます。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。

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、クラスターでは常に、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。

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。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、同じプロセスを行います。

デバイス クラスタなしの冗長性の確立

通常は、シスコ冗長性プロトコル（SFRP）を使用することで、デバイス クラスタを構成することなく、レイヤ 3 の冗長性を実現できます。SFRP を使用すると、デバイスは指定された IP アドレスに対する冗長ゲートウェイとして機能することが可能になります。ネットワーク冗長性では、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」（P.9-8）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を持たせて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 セットを配置するには、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 トポロジーを設定します。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ズを開始します。

クラスタに含まれていないデバイスでは、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の 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 などの動的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、Spanning Tree Protocol（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」（P.8-8）を参照してください。

注　シスコでは、デバイス クラスタに展開する予定の仮想スイッチを設定する場合は、STP を有効にすることを強く推奨しています。

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」（P.6-29）
- 「デバイス クラスタの編集」（P.6-31）
- 「クラスタ内の個々のデバイスの設定」（P.6-31）

- 「クラスタ内の個々のデバイス スタックの設定」（P.6-32）
- 「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」（P.6-33）
- 「クラスタ内のアクティブ ピアの切り替え」（P.6-33）
- 「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」（P.6-34）
- 「クラスタを構成するスタック内のデバイスの交換」（P.6-34）
- 「クラスタ状態共有の設定」（P.6-35）
- 「クラスタ状態共有のトラブルシューティング」（P.6-37）
- 「クラスタを構成するデバイスの分離」（P.6-40）
- 「SFRP の設定」（P.9-8）
- 「HA リンク インターフェイスの設定」（P.6-62）

デバイス クラスタの設定

ライセンス：Control

サポート対象デバイス：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」（P.55-44）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 ソフトウェア 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 System Malware Storage Pack Guide*』を参照してください。

注意　シスコから提供されたものではないハード ドライブを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**購入できます。このキットを使用できるのは、FireSIGHT システムのバージョン 5.3 以降を実行している 8000 シリーズ デバイス**のみ**です。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 System 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」（P.6-31）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。

デバイスまたはスタックを、クラスタを構成するペアとして設定すると、そのペアは、[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。[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」（P.6-34）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」（P.6-20）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。クラスタを構成するスタック内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クから、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」（P.6-16）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」（P.6-62）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

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　[Add] ドロップダウン メニューから、[Add Cluster] を選択します。

[Add Cluster] ポップアップ ウィンドウが表示されます。

ステップ 3　[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。

ステップ 4　[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。

ステップ 5　[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。

ステップ 6　[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

サポート対象デバイス：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。

[General] セクションのステータス アイコン上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、次の項を参照してください。

- 「割り当てられたデバイス名の編集」（P.6-47）
- 「デバイス ライセンスの有効化と無効化」（P.6-48）
- 「クラスタ状態共有の設定」（P.6-35）
- 「高度なデバイス設定の編集」（P.6-53）

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

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 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。

[Cluster] ページが表示されます。

ステップ 3　[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

サポート対象デバイス：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、次の項を参照してください。

- 「割り当てられたデバイス名の編集」（P.6-47）
- 「デバイス システム設定の編集」（P.6-49）
- 「デバイスのヘルスの確認」（P.6-50）
- 「デバイス管理設定の編集」（P.6-51）

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

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 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。

[Cluster] ページが表示されます。

ステップ 3　[Devices] をクリックします。

[Devices] ページが表示されます。

ステップ 4　[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。

ステップ 5　[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

サポート対象デバイス：シリーズ 3

スタックに含まれる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限られてきます。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」（P.6-33）で説明している手順に従って、スタックのネットワーク設定を編集できます。

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

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 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。

[Cluster] ページが表示されます。

ステップ 3　[Stacks] をクリックします。

[Stacks] ページが表示されます。

[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。

ステップ 4　[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。

[General] ポップアップ ウィンドウが表示されます。

ステップ 5　[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。

ステップ 6　[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」（P.6-19）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

サポート対象デバイス：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」（P.9-9）を参照してください。

クラスタを構成するデバイスの [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、「インターフェイスの設定」（P.6-58）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

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 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。

[Cluster] ページが表示されます。

ステップ 3　[Interfaces] をクリックします。

[Interfaces] ページが表示されます。

ステップ 4　[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。

ステップ 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、「インターフェイスの設定」（P.6-58）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

サポート対象デバイス：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

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 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。

[Switch Active Peer] ポップアップ ウィンドウが表示されます。

ステップ 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、[Yes] をクリックします。キャンセルして [Device Management] ページに戻る場合は、[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

サポート対象デバイス：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で同時にメンテナンス モードを開始することはできません。

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

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 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。

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

ステップ 3　[Yes] をクリックしてメンテナンス モードを確認するか、[No] をクリックしてキャンセルします。

ステップ 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

サポート対象デバイス：シリーズ 3

クラスタのメンバ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にも、クラスタのメンバ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」（P.6-42）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

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　メンテナンス モードを開始するスタック メンバ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。

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

ステップ 3　[Yes] をクリックしてメンテナンス モードを確認するか、[No] をクリックしてキャンセルします。

ステップ 4　デバイス交換アイコン（）をクリックします。

[Replace Device] ポップアップ ウィンドウが表示されます。

ステップ 5　ドロップダウン リストから [Replacement Device] を選択します。

ステップ 6　デバイスを交換するには、[Replace] をクリックします。現在のデバイスを保持して [Device Management] ページに戻るには、[Cancel] をクリックします。

ステップ 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

サポート対象デバイス：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 適用
- 単方向アクセス コントロール ルール
- ブロッキングの永続性

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。

クラスタ状態共有を設定するには、その前に、クラスタを構成する両方のデバイスまたはスタック内のプライマリ デバイスに HA リンク インターフェイスを設定して有効にする必要があります。3D8250 デバイスには 10G の HA リンクが必要ですが、他のモデルのデバイスには 1G 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」（P.6-62）を参照してください。

厳密な TCP 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、システムは未確立の接続で受信した SYN 以外のパケットをドロップします。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。

```
ルール 1：192.168.1.0/24 ～ 192.168.2.0/24 からの接続を許可
ルール 2：すべての接続をブロック
```

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 から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。

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。

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。

Minimum Sync.Interval

セッションの更新メッセージ間隔（ミリ秒）を指定します。0 ～ 65535 の整数を使用できます。最小同期間隔を設定することで、特定の接続が最小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。

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準備が向上し、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

ステップ 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」（P.6-62）を参照してください。

ステップ 2　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 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。

[Cluster] ページが表示されます。

ステップ 4　[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。

[State Sharing] ポップアップ ウィンドウが表示されます。

ステップ 5　このセクションで前に説明したように、状態共有を設定します。

ステップ 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」（P.6-19）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

サポート対象デバイス：シリーズ 3

状態共有を有効にした後は、[Cluster] ページの [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状態
- 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。

Messages Received (Unicast)

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。

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。[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。

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。

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。

Messages Sent

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。

Bytes Sent

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

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 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。

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

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 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 [Cluster] ページが表示されます。

ステップ 3　[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。

[State Sharing Statistics] ポップアップ ウィンドウが表示されます。

ステップ 4　必要に応じて、[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。

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

ステップ 6　必要に応じて、[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

サポート対象デバイス：シリーズ 3

デバイス クラスタを解除しても、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

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 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。

[Confirm Break] ポップアップ ウィンドウが表示されます。

ステップ 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。

ステップ 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。

スタックに含まれるデバイスの管理

ライセンス：任意

サポート対象デバイス：3D8140、3D8200 ファミリ、3D8300 ファミリ、3D9900

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 40G 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 40G 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 40G 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 40G 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 40G 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 System 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 System Malware Storage Pack Guide*』を参照してください。

注意　シスコから提供されたものではないハード ドライブを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**購入できます。このキットを使用できるのは、FireSIGHT システムのバージョン 5.3 以降を実行している 8000 シリーズ デバイス**のみ**です。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 System 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、スタックに含まれる各デバイスのリソースが単一の共有設定に結合されることになります。

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、「インターフェイスの設定」（P.6-58）を参照してください。『*FireSIGHT System Installation Guide*』で説明されているスタックに含まれる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」（P.12-8）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。バージョンが混在するスタックには、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 ハード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」（P.55-1）を参照してください。

セカンダリ デバイスで障害が発生した場合、プライマリ デバイスはトラフィックの検知、アラートの生成、およびすべてのセカンダリ デバイスへのトラフィックの送信を続行します。障害が発生したセカンダリ デバイスでは、トラフィックがドロップされます。その場合、リンク切断を通知する、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」（P.6-26）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　スタックに含まれる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配信する場合は、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、スタック内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、次の項を参照してください。

- 「デバイス スタックの確立」（P.6-42）
- 「デバイス スタックの編集」（P.6-44）
- 「スタックに含まれる個々のデバイスの設定」（P.6-45）
- 「スタックに含まれるデバイスの分離」（P.6-46）

デバイス スタックの確立

ライセンス：任意

サポート対象デバイス：3D8140、3D8200 ファミリ、3D8300 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、ファイアパワーの 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、または 3D8390 でスタックを構成し、リソースを単一の共有設定に結合して使用します。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 System 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」（P.6-26）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、[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、スタックに含まれる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」（P.6-20）および「防御センターへのデバイスの追加」（P.6-16）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、次の作業は実行できます。

- 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。

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、最初にスタックに含まれるデバイスの設定を確立したときの方法と同じです。

デバイスのスタック構成を確立するには、以下を行います。

アクセス：Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　[Add] ドロップダウン メニューから、[Add Stack] を選択します。

[Add Stack] ポップアップ ウィンドウが表示されます。

ステップ 3　[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。

ステップ 4　[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。

ステップ 5　[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。

[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。

ステップ 6　[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。

ステップ 7　[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。

ステップ 8　[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。

ステップ 9　[Add] をクリックします。

[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。

ステップ 10　必要に応じて、3D8250 の既存のスタック、3D8260、3D8270、3D8350 の既存のスタック、3D8360、または 3D8370 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。

ステップ 11　[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

サポート対象デバイス：3D8140、3D8200 ファミリ、3D8300 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 [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 [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 ポリシーとヘルス ポリシーの表示、Automatic Application Bypass の設定、Fast-Path ルールの設定を行うことができます。

詳細については、次の項を参照してください。

- 「割り当てられたデバイス名の編集」（P.6-47）
- 「デバイス ライセンスの有効化と無効化」（P.6-48）
- 「高度なデバイス設定の編集」（P.6-53）

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

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　設定を編集する、スタックに含まれる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 [Stack] ページが表示されます。

ステップ 3　[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

サポート対象デバイス：3D8140、3D8200 ファミリ、3D8300 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 [Devices] ページで、単一デバイスの [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、次の項を参照してください。

- 「割り当てられたデバイス名の編集」（P.6-47）
- 「デバイス システム設定の編集」（P.6-49）
- 「デバイスのヘルスの確認」（P.6-50）
- 「デバイス管理設定の編集」（P.6-51）

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

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　設定を編集する、スタックに含まれる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 [Stack] ページが表示されます。

ステップ 3　[Devices] をクリックします。

[Devices] ページが表示されます。

ステップ 4　[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。

ステップ 5　[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、スタックに含まれる個々のデバイスに変更を加えます。

スタックに含まれるデバイスでのインターフェイスの設定

ライセンス：任意

サポート対象デバイス：3D8140、3D8200 ファミリ、3D8300 ファミリ、3D9900

管理インターフェイスを除き、スタックに含まれるデバイスに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 [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構成の編集」（P.51-11）を参照してください。

スタックに含まれるシリーズ 3 デバイスの [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 [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、「インターフェイスの設定」（P.6-58）を参照してください。

スタックに含まれ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

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　インターフェイスを設定する、スタックに含まれる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 [Stack] ページが表示されます。

ステップ 3　[Interfaces] をクリックします。

[Interfaces] ページが表示されます。

ステップ 4　[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。

ステップ 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、「インターフェイスの設定」（P.6-58）を参照してください。

スタックに含まれるデバイスの分離

ライセンス：任意

サポート対象デバイス：3D8140、3D8200 ファミリ、3D8300 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。

スタックに含まれ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

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 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。

[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、またはリンク状態が短時間中断されます。

ステップ 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。

デバイス設定の編集

ライセンス：任意

アプライアンス エディタの [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、このページでは、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、Fast-Path 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、次の項を参照してください。

- 「割り当てられたデバイス名の編集」（P.6-47）
- 「デバイス ライセンスの有効化と無効化」（P.6-48）
- 「デバイス システム設定の編集」（P.6-49）
- 「デバイスのヘルスの確認」（P.6-50）
- 「デバイス管理設定の編集」（P.6-51）
- 「高度なデバイス設定について」（P.6-52）

割り当てられたデバイス名の編集

ライセンス：任意

[Device] タブの [General] セクションに表示されるデバイス名は、変更できます。

デバイスに割り当てられた名前を編集するには、以下を行います。

アクセス：Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 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。

そのデバイスの [Interfaces] ページが表示されます。

ステップ 3　[Device] をクリックします。

[Device] ページが表示されます。

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 [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 [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。

ステップ 4　[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。

[General] ポップアップ ウィンドウが表示されます。

ステップ 5　[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。

ステップ 6　[Save] をクリックします。

新しい名前が保存されます。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」（P.6-19）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

サポート対象デバイス：シリーズ 3、仮想、X-Series、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。

- ControlMalware、および 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、Sourcefire Software for X-Series、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、Sourcefire Software for X-Series、または ASA FirePOWER で有効にすることはできますが、これらのデバイスでは Fast-Path 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。
- 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」（P.52-1）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

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 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 [Interfaces] タブが表示されます。

ステップ 3　[Device] をクリックします。

[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 [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。

ステップ 4　[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。。

[License] ポップアップ ウィンドウが表示されます。

ステップ 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。

ステップ 6　[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」（P.6-19）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

[Device] タブの [System] セクションには、システム情報の読み取り専用テーブルが表示されます。以下の表に、表示される情報をリストします。

表 6-2　[System] セクション テーブルのフィールド

フィールド	説明
Model	管理対象デバイスのモデル名と番号。
Serial	管理対象デバイスのシャーシのシリアル番号。
Time	デバイスの現在のシステム時刻。
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。
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-Series 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、『*Sourcefire Software for X-Series Installation Guide*』または ASA の資料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

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 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 [Interfaces] タブが表示されます。

ステップ 3　[Device] をクリックします。

[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 [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。

ステップ 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。

ステップ 5　プロンプトが出されたら、デバイスをシャットダウンすることを確認します。

[Device Management] ページに戻ります。

ステップ 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。

ステップ 7　プロンプトが出されたら、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」（P.6-19）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

[Device] タブの [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 [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」（P.55-45）を参照してください。

[Policy] リンクをクリックすると、現在適用されているヘルス 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」（P.55-33）を参照してください。

また、[Blacklist] リンクをクリックすると、[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」（P.55-41）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

[Device] タブの [Management] セクションには、リモート管理情報のリストが表示されます。以下の表に、表示される情報をリストします。

表 6-3　[Management] セクション テーブルのフィールド

フィールド	説明
Host	デバイスの現在の管理ホスト名または IP アドレス。
Status	ローカル イベント ストレージがデバイスに対して有効かどうかを示します。
Transfer Packets	パケット データが防御センターに転送されるかどうかを示します。

[Management] セクションを使用して、管理ホストを指定したり、仮想 IP を再生成することができます。また、ローカル イベント ストレージに関する管理オプションを指定したり、パケット データを防御センターに転送するかどうかを指定したりすることもできます。

ヒント　スライダをクリックすることで、防御センターと管理対象デバイス間の通信チャネルをブロックできます。通信チャネルを再び有効にするには、スライダをクリックします。

デバイスの管理オプションを変更するには、以下を行います。

アクセス：Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 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 [Interfaces] タブが表示されます。

ステップ 3　[Device] をクリックします。

[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 [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。

ステップ 4　[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。

[Management] ポップアップ ウィンドウが表示されます。

ステップ 5　[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。

ステップ 6　デバイスの管理を無効にするには、[Enabled] チェック ボックスをオフにします。管理を有効にするには、このチェック ボックスをオンにします。

ステップ 7　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、[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。

ステップ 8　[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」（P.6-19）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

サポート対象デバイス：機能に応じて異なる

[Device] タブの [Advanced] セクションには、高度な設定をリストするテーブルが表示されます。以下の表に、これらの設定を記載します。

表 6-4　[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
Application Bypass	デバイスでの Automatic Application Bypass の状態。	シリーズ 2、シリーズ 3、仮想
Bypass Threshold	Automatic Application Bypass のしきい値（ミリ秒）。	シリーズ 2、シリーズ 3、仮想
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
Fast-Path Rules	デバイス上に作成されている Fast-Path ルールの数。	8000 シリーズ、3D9900

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

- 「Automatic Application Bypass」（P.6-52）
- 「高度なデバイス設定の編集」（P.6-53）
- 「Fast-Path ルールの設定」（P.6-54）

Automatic Application Bypass

ライセンス：任意

Automatic Application Bypass（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 5.3.1 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：オフ
- シリーズ 2 および仮想：オン
- ASA FirePOWER：未サポート
- X-Series：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、Fast-Path パケットに対して侵入ポリシーの Rule Latency Thresholding を使用します。Rule Latency Thresholding により、エンジンがシャットダウンされたり、しきい値データが生成されることはありません。詳細については、「ルール遅延しきい値構成について」（P.24-6）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 がアクティブになると、システムはすべての Snort プロセスをキルします。

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」（P.55-44）を参照してください。

Automatic Application Bypass 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、「高度なデバイス設定の編集」（P.6-53）を参照してください。

高度なデバイス設定の編集

ライセンス：任意

サポート対象デバイス：機能に応じて異なる

[Devices] タブの [Advanced] セクションを使用して、[Automatic Application Bypass] および [Inspect Local Router Traffic] の設定を変更できます。また、「Fast-Path ルールの設定」（P.6-54）で説明する手順に従って、Fast-Path 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。

- Fast-Path 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。
- [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。

高度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

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 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 [Interfaces] タブが表示されます。

ステップ 3　[Device] をクリックします。

[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 [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。

ステップ 4　[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。

[Advanced] ポップアップ ウィンドウが表示されます。

ステップ 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、[Automatic Application Bypass] を選択します。Automatic Application Bypass 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、「Automatic Application Bypass」（P.6-52）を参照してください。

ステップ 6　[Automatic Application Bypass] オプションを選択すると、[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。

ステップ 7　ルータとして展開されている場合は、必要に応じて [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。

ステップ 8　必要に応じて、Fast-Path ルールを設定します。詳細については、「Fast-Path ルールの設定」（P.6-54）を参照してください。

ステップ 9　[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」（P.6-19）を参照してください）。

Fast-Path ルールの設定

ライセンス：任意

サポート対象デバイス：8000 シリーズ、3D9900

トラフィックを送信してインスペクションなしでデバイスを通過させるには、Fast-Path ルールを作成できます。Fast-Path ルールにより、分析する必要のないトラフィックを方向転換してデバイスをバイパスさせます。Fast-Path ルールは、トラフィックを（インターフェイス外の）Fast-Path 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。Fast-Path 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判断します。

詳細については、次の項を参照してください。

- 「IPv4 Fast-Path ルールの追加」（P.6-55）
- 「IPv6 Fast-Path ルールの追加」（P.6-56）
- 「Fast-Path ルールの削除」（P.6-58）

IPv4 Fast-Path ルールの追加

ライセンス：任意

サポート対象デバイス：8000 シリーズ、3D9900

Fast-Path ルールは、トラフィックを（インターフェイス外の）Fast-Path 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。Fast-Path に転送してインスペクションを行わない IPv4 トラフィックを選択するには、以下の基準を使用できます。

- 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
- 双方向オプション

Fast-Path ルールには、最も外側の ID が使用されることに注意してください。

ヒント　既存の Fast-Path 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 Fast-Path ルールを作成または編集するには、以下を行います。

アクセス：Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　Fast-Path 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 [Interfaces] タブが表示されます。

ステップ 3　[Device] をクリックします。

[Devices] タブが表示されます。

ステップ 4　[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。

[Advanced] ポップアップ ウィンドウが表示されます。

ステップ 5　Fast-Path ルールを追加する場合は、[New IPv4 Rule] をクリックします。

[New IPv4 Rule] ポップアップ ウィンドウが表示されます。

ステップ 6　[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 デバイスのセットアップ」（P.7-1）を参照してください。

ステップ 7　[Initiator] および [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を、ルールに突き合わせます。FireSIGHT システムでの CIDR 表記の詳細については、「IP アドレスの表記法」（P.1-19）を参照してください。

ステップ 8　必要に応じて、[Protocol] ドロップダウン リストからルールの対象とするプロトコルを選択するか、[All] を選択して、リストの任意のプロトコルによるトラフィックを突き合わせます。

ステップ 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、[Initiator Port] および [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、ポート番号のカンマ区切りリストを入力できます。IPv4 Fast-Path 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、任意として扱われることに注意してください。

[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基準を絞り込みます。

ステップ 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を、ルールに突き合わせます。空白の VLAN 値は、任意として扱われることに注意してください。

ステップ 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、[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。

ステップ 12　[Save] をクリックします。

[Advanced] ポップアップ ウィンドウの [Fast-Path Rules] にルールが追加されます。ルールが追加されても、[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」（P.6-19）を参照してください）。

IPv6 Fast-Path ルールの追加

ライセンス：任意

サポート対象デバイス：シリーズ 3、3D9900

Fast-Path ルールは、トラフィックを（インターフェイス外の）Fast-Path 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。Fast-Path に転送してインスペクションを行わない IPv6 トラフィックを選択するには、以下の基準を使用できます。

- 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
- 双方向オプション

Fast-Path ルールには、最も外側の VLAN ID が使用されることに注意してください。

ヒント　既存の Fast-Path 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 Fast-Path ルールを追加するには、以下を行います。

アクセス：Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　Fast-Path 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 [Interfaces] タブが表示されます。

ステップ 3　[Device] をクリックします。

[Devices] タブが表示されます。

ステップ 4　[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。

[Advanced] ポップアップ ウィンドウが表示されます。

ステップ 5　Fast-Path ルールを追加する場合は、[New IPv6 Rule] をクリックします。

[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。

ステップ 6　[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 デバイスのセットアップ」（P.7-1）を参照してください。

ステップ 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、[Initiator] または [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を、ルールに突き合わせます。FireSIGHT システムで IPv6 プレフィクス長の表記を使用する方法については、「IP アドレスの表記法」（P.1-19）を参照してください。

ステップ 8　必要に応じて、[Protocol] ドロップダウン リストからルールの対象とするプロトコルを選択するか、[All] を選択して、リストの任意のプロトコルによるトラフィックを突き合わせます。

選択されたプロトコルのパケットだけを、Fast-Path ルールに突き合わせます。

ステップ 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、[Initiator Port] および [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、ポート番号のカンマ区切りリストを入力できます。IPv6 Fast-Path 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、任意として扱われることに注意してください。

ステップ 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を、ルールに突き合わせます。空白の VLAN 値は、任意として扱われることに注意してください。

ステップ 11　必要に応じて、[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に突き合わせ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。

ステップ 12　[Save] をクリックします。

[Advanced] ポップアップ ウィンドウの [Fast-Path Rules] にルールが追加されます。

ステップ 13　[Advanced] ポップアップ ウィンドウで、[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」（P.6-19）を参照してください）。

Fast-Path ルールの削除

ライセンス：任意

サポート対象デバイス：8000 シリーズ、3D9900

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

Fast-Path ルールを削除するには、以下を行います。

アクセス：Admin/Network Admin

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　Fast-Path 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 [Interfaces] タブが表示されます。

ステップ 3　[Device] をクリックします。

[Devices] タブが表示されます。

ステップ 4　[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。

[Advanced] ポップアップ ウィンドウが表示されます。

ステップ 5　削除する Fast-Path ルールの横にある削除アイコン（ ）をクリックします。

ステップ 6　プロンプトが出されたら、ルールを削除することを確認します。

ルールが [Advanced] ポップアップ ウィンドウから削除されます。

ステップ 7　[Save] をクリックします。

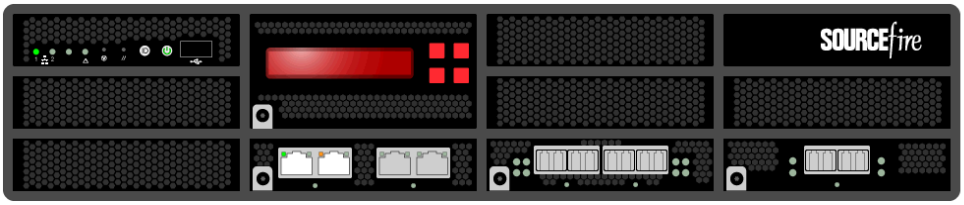
変更が保存されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくは「デバイスへの変更の適用」（P.6-19）を参照してください）。

インターフェイスの設定

ライセンス：任意

アプライアンス エディタの [Interfaces] ページから、FireSIGHT システム展開に応じて、管理対象デバイスのインターフェイスを設定できます。

[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、Sourcefire Software for X-Series、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。以下のグラフィックは、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 6-5　　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、デバイスに設定されているすべてのインターフェイスがリストされます。このテーブルには、各インターフェイスに関する要約情報が記載されます。以下の表に、これらの情報をリストします。[MAC Address] 列と [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 6-6　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
Link	インターフェイスの現在のリンク状態。論理インターフェイスのリンク状態は、親物理インターフェイスのリンク状態と同じです。Sourcefire Software for X-Series および ASA FirePOWER デバイスには、リンク状態は表示されません。
Name	インターフェイスの名前。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 インターフェイスおよび ASA FirePOWER インターフェイスはその例外で、ユーザが名前を定義します。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。
Type	インターフェイスの設定。以下のいずれかになります。 • None • Management • Passive • Inline • Switched • Routed • Hybrid • HA link • ASA
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。
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、[Used by] 列は表示されません。
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、[Interfaces] ページに表示されるインターフェイスを対応させることができます。Sourcefire Software for X-Series 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 Addresses	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。

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。

- 「管理インターフェイスの設定」（P.6-61）
- 「HA リンク インターフェイスの設定」（P.6-62）
- 「インターフェイス MTU の設定」（P.6-63）
- 「Cisco ASA with FirePOWER Services インターフェイスの管理」（P.6-64）
- 「インターフェイスの無効化」（P.6-65）
- 「重複する接続ロギングの防止」（P.6-65）
- 「IPS デバイスのセットアップ」（P.7-1）
- 「仮想スイッチのセットアップ」（P.8-1）
- 「仮想ルータのセットアップ」（P.9-1）
- 「ハイブリッド インターフェイスの設定」（P.10-1）

管理インターフェイスの設定

ライセンス：任意

管理インターフェイスのリンク モードおよび MDI/MDIX 設定は、アプライアンス エディタで構成できます。管理インターフェイスのその他すべての設定（IPv4 アドレス、IPv6 アドレス、DNS 設定など）は、デバイスでローカルに構成する必要があります。

注意　最大伝送単位（MTU）を変更すると、デバイス上のトラフィックが中断されます。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、「インターフェイス MTU の設定」（P.6-63）を参照してください。

管理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

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 2　管理インターフェイスを設定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 [Interfaces] タブが表示されます。

ステップ 3　管理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。

[Edit Interface] ポップアップ ウィンドウが表示されます。

ステップ 4　[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、[Autonegotiation] を選択して、速度およびデュプレックス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。

ステップ 5　[MDI/MDIX] ドロップダウン リストから、MDI（Medium Dependent Interface）、MDIX（Medium Dependent Interface Crossover）、Auto-MDIX のどのタイプのインターフェイスとして構成する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。

ステップ 6　[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、「インターフェイス MTU の設定」（P.6-63）を参照してください。

ステップ 7　[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」（P.6-19）を参照してください）。

HA リンク インターフェイスの設定

ライセンス：任意

サポート対象デバイス：シリーズ 3

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」（P.6-26）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ー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　最大伝送単位（MTU）を変更すると、デバイス上のトラフィックが中断されます。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、「インターフェイス MTU の設定」（P.6-63）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

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 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 [Interfaces] タブが表示されます。

ステップ 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。

[Edit Interface] ポップアップ ウィンドウが表示されます。

ステップ 4　[HA Link] をクリックして HA オプションを表示します。

ステップ 5　[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。

ステップ 6　[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、[Autonegotiation] を選択して、速度およびデュプレックス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することを指定します。

ステップ 7　[MDI/MDIX] ドロップダウン リストから、MDI（Medium Dependent Interface）、MDIX（Medium Dependent Interface Crossover）、Auto-MDIX のどのタイプのインターフェイスとして構成する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。

ステップ 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、「インターフェイス MTU の設定」（P.6-63）を参照してください。

ステップ 9　[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」（P.6-19）を参照してください）。

インターフェイス MTU の設定

ライセンス：任意

インターフェイスまたはインライン セットの最大伝送単位（MTU）を変更すると、以下の機能が影響を受ける可能性があります。

- トラフィック インスペクション（アプリケーション認識および制御、URL フィルタリング、侵入検知および防御、接続ロギングを含む）
- トラフィック フロー（スイッチング、ルーティング、および関連する機能を含む）
- リンク ステート

ネットワーク トラフィックがどのように、どれだけの期間中断するかは、インターフェイスのタイプとデバイスの設定および展開方法によって異なります。

また、Sourcefire Software for X-Series の場合は、Sourcefire Software for X-Series CLI を使用してインターフェイス MTU を設定することにも注意してください。詳細については、『*Sourcefire Software for X-Series 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、設定値が 576 の場合、自動的に 558 に削減されます。

以下の表に、管理対象デバイスの MTU 設定範囲をリストします。

表 6-7　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） 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：Control、Protection

サポート対象デバイス：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」（P.5-43）を参照してください。

ASA FirePOWER インターフェイスを設定するには、ASA 専用ソフトウェアおよび CLI を使用します。詳細については、ASA のマニュアル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

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 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 [Interfaces] タブが表示されます。

ステップ 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。

[Edit Interface] ポップアップ ウィンドウが表示されます。

ステップ 4　[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 [New] を選択して、新しいセキュリティ ゾーンを追加します。

ステップ 5　[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」（P.6-19）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

インターフェイス タイプを [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

ステップ 1　[Devices] > [Device Management] を選択します。

[Device Management] ページが表示されます。

ステップ 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 [Interfaces] タブが表示されます。

ステップ 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。

[Edit Interface] ポップアップ ウィンドウが表示されます。

ステップ 4　[None] をクリックします。

ステップ 5　[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」（P.6-19）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

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

ステップ 1　[Devices] > [Device Management] を選択します。

[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。

ステップ 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 [Interfaces] タブが表示されます。

ステップ 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、[Security Zone] を別のゾーンに変更して [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 [Save] をクリックします。

ステップ 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。

ステップ 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。