修復

以下のトピックでは、修復の設定について説明します。

修復の概要

修復は Firepower システムが相関ポリシー違反に応じて起動するプログラムです。

修復を実行すると、システムは修復ステータス イベントを生成します。修復ステータス イベントには、修復の名前、相関ポリシー、修復をトリガーしたルール、終了ステータス メッセージなどの詳細が含まれています。

システムは以下に挙げる複数の修復モジュールをサポートしています。

- Cisco ISE のエンドポイント保護サービス（EPS）：相関ポリシー違反に関連するホストやネットワークへ送信されるトラフィックを検疫、隔離解除、またはシャットダウンします。
- Cisco IOS Null ルート：相関ポリシー違反に関連するホストやネットワークへ送信されるトラフィックをブロックします（Cisco IOS バージョン 12.0 以降が必要）。
- Nmap スキャン：ホストをスキャンして、実行中のオペレーティング システムおよびサーバを決定します。
- 属性値の設定：相関ポリシー違反に関連するホストのホスト属性を設定します。

ヒント 他のタスクを実行するカスタム モジュールをインストールすることもできます。*Firepower System Remediation API Guide*を参照してください。

修復の実装

修復を実装するには、まず選択したモジュールに対して少なくとも1つのインスタンスを作成します。モジュールごとに複数のインスタンスを作成することができ、各インスタンスは別々に設定できます。たとえば、Cisco IOS Null ルート修復モジュールを使用して複数のルータと通信するには、そのモジュールのインスタンスを複数設定します。

次に、ポリシー違反の際に実行するアクションを説明する複数の修復を各インスタンスに追加します。

最後に、相関ポリシーに応じてシステムが修復を開始するように相関ポリシーで修復とルールを関連付けます。

修復およびマルチテナンシー

マルチドメイン展開では、どのドメインのレベルでもカスタムの修復モジュールをインストールできます。システム提供のモジュールはグローバル ドメインに属します。

先祖ドメインで作成されたインスタンスに修復を追加することはできませんが、現在のドメインで同様に設定されるインスタンスを作成し、そのインスタンスに修復を追加することは可能です。また、先祖ドメインで作成した修復は、相関応答として使用することもできます。

関連トピック

Firepower Management Center アラート応答
Nmap スキャン
ルールとホワイトリストに応答を追加する

Cisco ISE EPS 修復

ISE 導入環境で、エンドポイント保護サービス（EPS）が設定され、有効になっている場合、Firepower Management Center を設定することで、ISE を使った修復を起動させることが可能です。ISE EPS 修復は、完全に設定された状態では、相関ポリシー違反を起こした送信元または宛先ホストに対し、次の**緩和アクション（Mitigation Actions）**を実行します。

- **検疫（quarantine）**：エンドポイントのネットワークへのアクセスを制限または拒否します。
- **隔離解除（unquarantine）**：エンドポイントの検疫ステータスを解除し、ネットワークへのフル アクセスを許可します。
- **シャットダウン（shotdown）**：エンドポイントのNASポートを非アクティブ化し、ネットワークから切断します。

また、ネットワークを**ホワイトリストに登録（Whitelist）**して、システムが当該アドレスに対して ISE EPS 修復を行わないようにすることも可能です。

（注） 使用するISEバージョンと構成は、FirepowerシステムでのISEの使用方法に影響を与えます。たとえば、ISE-PIC では、ISE EPS 修復を実行できません。詳細については、ISE/ISE-PIC アイデンティティ ソースを参照してください。

ISE EPS アクションの詳細については、『*Cisco Identity Services Engine User Guide*』を参照してください。

ISE EPS 修復の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin Discovery Admin

送信元または宛先ホストでISE EPS 修復を実行することによって、相関ポリシー違反に応答できます。

（注） ISE-PIC は ISE EPS 修復を実行できません。

始める前に

- ISE サーバ上で EPS 操作を設定します。
- ユーザ制御用 ISE/ISE-PIC の設定の説明に従って ISE への接続を設定します。

手順

ステップ 1 **[ポリシー（Policies）]>[アクション（Actions）]>[インスタンス（Instances）]**を選択します。

ステップ 2 ISE EPS インスタンスの追加 （4 ページ）の説明に従って pxGrid 緩和インスタンスを追加します。

ステップ 3 ISE EPS 修復の追加 （4 ページ）の説明に従って 1 つ以上の ISE EPS 修復を追加します。

次のタスク

- ルールとホワイトリストに応答を追加するの説明に従って相関ポリシー違反への応答として修復を割り当てます。

ISE EPS インスタンスの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin Discovery Admin

ISE EPS インスタンスを作成し、ロギング タイプごとに個々の修復をグループ化します。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクション（Actions）]** > **[インスタンス（Instances）]**を選択します。

ステップ 2 [新規インスタンスの追加（Add a New Instance）] リストから、モジュール タイプとして [pxGrid Mitigation(v1.0)] を選択し、[追加（Add）] をクリックします。

ステップ 3 [インスタンス名（Instance Name）] と [説明（Description）] に入力します。

ステップ 4 [ロギングの有効化（Enable Logging）] オプションを設定し、システム ロギングを有効または無効にします。

ステップ 5 [作成（Create）] をクリックします。

次のタスク

- セット属性値修復の追加 （13 ページ）の説明に従って ISE EPS 修復を作成します。

関連トピック

Firepower システムの IP アドレス表記法

ISE EPS 修復の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin Discovery Admin

相関ポリシー違反に含まれる送信元または宛先ホストで [緩和アクション（Mitigation Actions）] を実行するため、インスタンス内に 1 つ以上の ISE EPS 修復を作成します。

マルチドメイン展開では、先祖ドメインで作成されたインスタンスに修復を追加することはできません。

始める前に

- ISE EPS インスタンスの追加 （4 ページ）の説明に従って ISE EPS インスタンスを作成します。

手順

ステップ 1 **[ポリシー（Policies）]>[アクション（Actions）]>[インスタンス（Instances）]**を選択します。

ステップ 2 修復を追加するインスタンスの横にある表示アイコン（🔍）をクリックします。

ステップ 3 [設定済み修復（Configured Remediations）] セクションで、[宛先の緩和（Mitigate Destination）] または [送信元の緩和（Mitigate Source）] を選択し、[追加（Add）] をクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [修復名（Remediation Name）] と [説明（Description）] に入力します。

ステップ 5 次のいずれかの緩和アクションを選択します。[検疫（quarantine）]、[隔離解除（unquarantine）]、[シャットダウン（shutdown）] 。

ステップ 6 （オプション）ホワイトリストに目的の IP アドレスまたは範囲を入力し、修復から除外します。

ステップ 7 [作成（Create）] をクリックし、次に [完了（Done）] をクリックします。

次のタスク

- 相関ポリシー違反への応答として修復を割り当てます（ルールとホワイトリストに応答を追加する を参照）。

Cisco IOS Null ルート修復

Cisco IOS Null ルート修復モジュールでは、シスコ「null route」コマンドを使って、個別の IP アドレスまたは IP アドレスの範囲をブロックすることができます。これにより、ホストまたはネットワークに送信されるすべてのトラフィックがルータの NULL インターフェイスにルーティングされ、ドロップされます。違反ホストまたはネットワークから送信されるトラフィックはブロックされません。

（注） ディスカバリまたはホスト入力イベントに基づく相関ルールへの応答として接続先ベースの修復を使用しないでください。これらのイベントは、送信元ホストに関連付けられます。

注意 Cisco IOS 修復がアクティブになる際、タイムアウト期間はありません。IP アドレスまたはネットワークのブロックを解除するには、ルータから手動でルーティング変更をクリアする必要があります。

Cisco IOS ルータ用修復の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin Discovery Admin

（注） 検出またはホスト入力イベントに基づく相関ルールへの応答として、宛先ベースの修復を使用しないでください。これらのイベントは、送信元ホストに関連付けられます。

注意 Cisco IOS 修復がアクティブになる際、タイムアウト期間はありません。IP アドレスまたはネットワークのブロックを解除するには、ルータから手動でルーティング変更をクリアする必要があります。

始める前に

- Cisco ルータが Cisco IOS 12.0 以降を実行していることを確認します。
- ルータへのレベル 15 の管理アクセス権を持っていることを確認します。

手順

ステップ 1 Cisco ルータまたは IOS ソフトウェアに付属のドキュメントの説明に従って、Cisco ルータで Telnet を有効にします。

ステップ 2 Firepower Management Center で、使用する予定の各 Cisco IOS ルータに対する Cisco IOS ヌルルート インスタンスを追加します。Cisco IOS インスタンスの追加 （7 ページ）を参照してください。

ステップ 3 相関ポリシーに違反した場合にルータで実現する応答のタイプに基づき、インスタンスごとに修復を作成します。

- Cisco IOS ブロック宛先の修復の追加 （8 ページ）
- Cisco IOS ブロック宛先ネットワークの修復の追加 （9 ページ）
- Cisco IOS ブロック送信元の修復の追加 （10 ページ）
- Cisco IOS ブロック送信元ネットワークの修復の追加 （11 ページ）

次のタスク

- 相関ポリシー違反への応答として修復を割り当てます（ルールとホワイトリストに応答を追加する を参照）。

Cisco IOS インスタンスの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin Discovery Admin

修復を送信するルータが複数ある場合は、各ルータに対して別々のインスタンスを作成します。

始める前に

- ルータまたはIOS ソフトウェアのドキュメントの説明に従って、Cisco IOS ルータの Telnet アクセスを設定します。

手順

ステップ 1 **[ポリシー（Policies）]>[アクション（Actions）]>[インスタンス（Instances）]**を選択します。

ステップ 2 [新しいインスタンスの追加（Add a New Instance）] リストから [Cisco IOS Null ルート（Cisco IOS Null Route）] を選択し、[追加（Add）] をクリックします。

ステップ 3 [インスタンス名（Instance Name）] と [説明（Description）] を入力します。

ステップ 4 [ルータ IP（Router IP）] フィールドに、修復のために使用する Cisco IOS ルータの IP アドレスを入力します。

ステップ 5 [ユーザ名（Username）] フィールドに、ルータの Telnet ユーザ名を入力します。このユーザは、ルータでレベル 15 管理アクセスを持っている必要があります。

ステップ 6 [接続パスワード（Connection Password）] フィールドに、Telnet ユーザのパスワードを入力します。

ステップ 7 [イネーブル パスワード（Enable Password）] フィールドに、Telnet ユーザのイネーブル パスワードを入力します。これは、ルータの特権モードに入るために使用するパスワードです。

ステップ 8 [ホワイトリスト（White List）] フィールドに、修復から除外する IP アドレスまたは範囲を 1 行につき 1 つ入力します。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

ステップ 9 [作成（Create）] をクリックします。

次のタスク

- Cisco IOS ブロック宛先の修復の追加 （8 ページ）、Cisco IOS ブロック宛先ネットワークの修復の追加 （9 ページ）、Cisco IOS ブロック送信元の修復の追加 （10 ページ）、およびCisco IOS ブロック送信元ネットワークの修復の追加 （11 ページ）の説明に従い、相関ポリシーで使用する特定の修復を追加します。

関連トピック

Firepower システムの IP アドレス表記法

Cisco IOS ブロック宛先の修復の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin Discovery Admin

Cisco IOS ブロック宛先修復は、ルータから、相関ポリシー違反に関与している宛先ホストに送信されるトラフィックをブロックします。この修復を、検出またはホスト入力イベントに基づく相関ルールへの応答として使用しないでください。これらのイベントは、送信元ホストに関連付けられています。

マルチドメイン展開では、先祖ドメインで作成されたインスタンスに修復を追加することはできません。

始める前に

- Cisco IOS インスタンスの追加 （7 ページ） の説明に従い、Cisco IOS インスタンスを追加します。

手順

ステップ 1 **[ポリシー（Policies）]>[アクション（Actions）]>[インスタンス（Instances）]**を選択します。

ステップ 2 修復を追加するインスタンスの横にある表示アイコン（）をクリックします。

ステップ 3 [設定されている修復（Configured Remediations）] セクションで、[宛先のブロック（Block Destination）] を選択し、[追加（Add）] をクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [修復名（Remediation Name）] と [説明（Description）] を入力します。

ステップ 5 [作成（Create）] をクリックし、次に [完了（Done）] をクリックします。

次のタスク

- 相関ポリシー違反への応答として修復を割り当てます（ルールとホワイトリストに応答を追加する を参照）。

Cisco IOS ブロック宛先ネットワークの修復の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin Discovery Admin

Cisco IOS ブロック宛先ネットワーク修復は、ルータから、相関ポリシー違反に関与している宛先ホストのネットワークに送信されるトラフィックをブロックします。この修復を、検出またはホスト入力イベントに基づく相関ルールへの応答として使用しないでください。これらのイベントは、送信元ホストに関連付けられています。

マルチドメイン展開では、先祖ドメインで作成されたインスタンスに修復を追加することはできません。

始める前に

- Cisco IOS インスタンスの追加 （7 ページ） の説明に従い、Cisco IOS インスタンスを追加します。

手順

ステップ 1 **[ポリシー（Policies）]>[アクション（Actions）]>[インスタンス（Instances）]**を選択します。

ステップ 2 修復を追加するインスタンスの横にある表示アイコン（🔍）をクリックします。

ステップ 3 [設定されている修復（Configured Remediations）] セクションで、[宛先ネットワークのブロック（Block Destination Network）] を選択し、[追加（Add）] をクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [修復名（Remediation Name）] と [説明（Description）] を入力します。

ステップ 5 [ネットマスク（Netmask）] フィールドに、サブネット マスクを入力するか、または CIDR 表記を使用して、トラフィックをブロックするネットワークを記述します。

たとえば、1 つのホストがルールをトリガーとして使用したときにクラス C ネットワーク全体へのトラフィックをブロックするには、ネットマスクとして `255.255.255.0` または `24` を使用します。

別の例として、トリガーの IP アドレスを含む 30 個のアドレスへのトラフィックをブロックするには、ネットマスクとして `255.255.255.224` または `27` を指定します。この場合、IP アドレス `10.1.1.15` が修復をトリガーとして使用し、`10.1.1.1` と `10.1.1.30` の間のすべての IP アドレ

スがブロックされます。トリガーの IP アドレスのみをブロックするには、このフィールドは空のままにして、32 を入力するか、または 255.255.255.255 を入力します。

ステップ 6 [作成（Create）] をクリックし、次に [完了（Done）] をクリックします。

次のタスク

- 相関ポリシー違反への応答として修復を割り当てます（ルールとホワイトリストに応答を追加する を参照）。

関連トピック

Firepower システムの IP アドレス表記法

Cisco IOS ブロック送信元の修復の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin Discovery Admin

Cisco IOS ブロック送信元修復は、ルータから、相関ポリシー違反に関与している送信元ホストに送信されるトラフィックをブロックします。

マルチドメイン展開では、先祖ドメインで作成されたインスタンスに修復を追加することはできません。

始める前に

- Cisco IOS インスタンスの追加 （7 ページ） の説明に従い、Cisco IOS インスタンスを追加します。

手順

ステップ 1 **[ポリシー（Policies）]>[アクション（Actions）]>[インスタンス（Instances）]**を選択します。

ステップ 2 修復を追加するインスタンスの横にある表示アイコン（🔍）をクリックします。

ステップ 3 [設定されている修復（Configured Remediations）] セクションで、[送信元のブロック（Block Source）] を選択し、[追加（Add）] をクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [修復名（Remediation Name）] と [説明（Description）] を入力します。

ステップ 5 [作成（Create）] をクリックし、次に [完了（Done）] をクリックします。

次のタスク

- 相関ポリシー違反への応答として修復を割り当てます（ルールとホワイトリストに応答を追加する を参照）。

Cisco IOS ブロック送信元ネットワークの修復の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin Discovery Admin

Cisco IOS ブロック送信元ネットワーク修復は、ルータから、相関ポリシー違反に関与している送信元ホストのネットワークに送信されるトラフィックをブロックします。

マルチドメイン展開では、先祖ドメインで作成されたインスタンスに修復を追加することはできません。

始める前に

- Cisco IOS インスタンスの追加 （7 ページ） の説明に従い、Cisco IOS インスタンスを追加します。

手順

ステップ 1 **[ポリシー（Policies）]>[アクション（Actions）]>[インスタンス（Instances）]**を選択します。

ステップ 2 修復を追加するインスタンスの横にある表示アイコン（🔍）をクリックします。

ステップ 3 [設定されている修復（Configured Remediations）] セクションで、[送信元ネットワークのブロック（Block Source Network）] を選択し、[追加（Add）] をクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [修復名（Remediation Name）] と [説明（Description）] を入力します。

ステップ 5 [ネットマスク（Netmask）] フィールドに、トラフィックをブロックするネットワークの説明となるサブネット マスクまたは CIDR 表記を入力します。

たとえば、1 つのホストがルールをトリガーとして使用したときにクラス C ネットワーク全体へのトラフィックをブロックするには、ネットマスクとして `255.255.255.0` または `24` を使用します。

別の例として、トリガーの IP アドレスを含む 30 個のアドレスへのトラフィックをブロックするには、ネットマスクとして `255.255.255.224` または `27` を指定します。この場合、IP アドレス `10.1.1.15` が修復をトリガーとして使用し、`10.1.1.1` と `10.1.1.30` の間のすべての IP アドレスがブロックされます。トリガーの IP アドレスのみをブロックするには、このフィールドは空のままにして、`32` を入力するか、または `255.255.255.255` を入力します。

ステップ 6 [作成（Create）] をクリックし、次に [完了（Done）] をクリックします。

次のタスク

- 相関ポリシー違反への応答として修復を割り当てます（ルールとホワイトリストに応答を追加する を参照）。

関連トピック

Firepower システムの IP アドレス表記法

Nmap スキャン修復

Firepower システムには、Nmap™ という、ネットワーク調査およびセキュリティ監査を目的としたオープン ソースのアクティブ スキャナが統合されています。Nmap修復を使用して、相関ポリシー違反に対応できます。これは、Nmap スキャン修復をトリガーします。

Nmap スキャンの詳細については、Nmap スキャンを参照してください。

セット属性値修復

トリガーイベントが発生したホストでホスト属性値を設定することにより、相関ポリシー違反に応答できます。テキストのホスト属性の場合、イベントの説明を属性値として使用できます。

セット属性修復の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin Discovery Admin

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクション（Actions）]** > **[インスタンス（Instances）]**を選択します。

ステップ 2 セット属性値インスタンスの追加 （13 ページ）の説明に従って、セット属性インスタンスを作成します。

ステップ 3 セット属性値修復の追加 （13 ページ）の説明に従って、セット属性修復を追加します。

次のタスク

- 相関ポリシー違反への応答として修復を割り当てます（ルールとホワイトリストに応答を追加する を参照）。

関連トピック

定義済みホスト属性
ユーザ定義のホスト属性

セット属性値インスタンスの追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin Discovery Admin

手順

ステップ 1 **[ポリシー（Policies）]>[アクション（Actions）]>[インスタンス（Instances）]**を選択します。

ステップ 2 [新しいインスタンスの追加（Add a New Instance）] リストから [セット属性値（Set Attribute Value）] を選択し、[追加（Add）] をクリックします。

ステップ 3 [インスタンス名（Instance Name）] と [説明（Description）] を入力します。

ステップ 4 [作成（Create）] をクリックします。

次のタスク

- セット属性値修復の追加 （13 ページ） の説明に従って、セット属性修復を作成します。

セット属性値修復の追加

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin Discovery Admin

セット属性値修復は相関ポリシー違反に関与したホストにホスト属性を設定します。属性を設定する各属性の値について修復を作成します。テキスト属性の場合、トリガーイベントの説明を属性値として使用できます。

マルチドメイン展開では、先祖ドメインで作成されたインスタンスに修復を追加することはできません。

始める前に

- セット属性値インスタンスの追加 （13 ページ） の説明に従って、セット属性インスタンスを作成します。

手順

ステップ 1 **[ポリシー（Policies）]>[アクション（Actions）]>[インスタンス（Instances）]**を選択します。

ステップ 2 修復を追加するインスタンスの横にある表示アイコン（）をクリックします。

ステップ 3 [設定されている修復（Configured Remediations）] セクションで、[セット属性値（Set Attribute Value）] を選択し、[追加（Add）] をクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [修復名（Remediation Name）] と [説明（Description）] を入力します。

ステップ 5 送信元データ、宛先データをもつイベントへの応答としてこの修復を使用するには、[イベントが決定するホストを更新（Update Which Host(s) From Event）] オプションを選択します。

ステップ 6 テキスト属性の場合、以下に従い [属性値にイベントからの説明を使用（Use Description From Event For Attribute Value）] を指定します。

- イベントの説明を属性値として使用するには、[オン（On）] をクリックし、設定する [属性値（Attribute Value）] を入力します。
- 修復の [属性値（Attribute Value）] 設定を属性値として使用するには、[オフ（Off）] をクリックします。

ステップ 7 [作成（Create）] をクリックし、次に [完了（Done）] をクリックします。

次のタスク

- 相関ポリシー違反への応答として修復を割り当てます（ルールとホワイトリストに応答を追加する を参照）。

修復モジュールの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin Discovery Admin

マルチドメイン展開では、現在のドメインでインストールされた修復モジュールが表示されます。このモジュールは削除可能です。また、先祖ドメインでインストールされたモジュールも表示されますが、これは削除できません。下位ドメインの修復モジュールを管理するには、そのドメインに切り替えます。

手順

ステップ 1 **[ポリシー（Policies）] > [アクション（Actions）] > [モジュール（Modules）]**を選択します。

ステップ 2 修復モジュールを管理します。

- 設定：モジュールの [モジュール詳細（Module Detail）] ページを表示して、そのモジュールのインスタンスと修復を設定するには、表示アイコン（）をクリックします。マルチドメイン展開では、[モジュール詳細（Module Detail）] ページを使用して、先祖ドメインでインストールされたモジュールに対応する現在のドメイン内のインスタンスを追加、削除、または編集することはできません。代わりに、[インスタンス（Instances）] ページ（**[ポリシー（Policies）] > [アクション（Actions）] > [インスタンス（Instances）]**）を使用します。修復インスタンスの管理 （15 ページ）を参照してください。
- 削除：使用されていないカスタム モジュールを削除するには、削除アイコン（）をクリックします。システム付属のモジュールは削除できません。
- インストール：カスタム モジュールをインストールするには、[ファイルの選択（Choose File）] をクリックしてモジュールを参照し、[インストール（Install）] をクリックします。詳細については、*Firepower System Remediation API Guide*を参照してください。

修復インスタンスの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin Discovery Admin

[インスタンス（Instances）] ページには、すべての修復モジュールのすべての設定済みインスタンスがリスト表示されます。

マルチドメイン展開では、現在のドメインで作成された修復インスタンスが表示されます。このインスタンスは編集可能です。また、先祖ドメインで作成されたインスタンスも表示されますが、これは編集できません。下位ドメインの修復インスタンスを管理するには、そのドメインに切り替えます。

先祖ドメインで作成したインスタンスに修復を追加することはできませんが、同様の設定済みインスタンスを現在のドメインに作成して、そのインスタンスに修復を追加することはできます。また、先祖ドメインで作成した修復は、相関応答として使用することもできます。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクション（Actions）]** > **[インスタンス（Instances）]**を選択します。

ステップ 2 修復インスタンスを管理します。

- 追加：インスタンスを追加するには、インスタンスを追加する修復モジュールを選択して、[追加（Add）] をクリックします。システム付属のモジュールについては、次を参照してください。
  - ISE EPS インスタンスの追加 （4 ページ）
  - Cisco IOS インスタンスの追加 （7 ページ）
  - Nmap スキャン インスタンスの追加
  - セット属性値インスタンスの追加 （13 ページ）

  カスタムモジュールを追加する際のヘルプは、そのモジュールのドキュメントを参照してください（使用可能な場合）。
- 設定：インスタンスの詳細を設定して、インスタンスに修復を追加するには、表示アイコン（）をクリックします。
- 削除：使用されていないインスタンスを削除するには、削除アイコン（）をクリックします。

1 つの修復モジュールのインスタンスの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin Discovery Admin

[モジュール詳細（Module Detail）] ページには、特定の修復モジュールに設定されたインスタンスと修復がすべて表示されます。

マルチドメイン展開では、現在のドメインと先祖ドメインにインストールされた修復モジュールの [モジュール詳細（Module Detail）] ページにアクセスできます。ただし、[モジュール詳細（Module Detail）] ページを使用して、先祖ドメインにインストールされているモジュールに対応する現在のドメイン内のインスタンスを追加、削除または編集することはできません。代わりに、[インスタンス（Instances）] ページ（**[ポリシー（Policies）]** > **[アクション（Actions）]** > **[インスタンス（Instances）]**）を使用します。修復インスタンスの管理 （15 ページ）を参照してください。

手順

ステップ 1 **[ポリシー（Policies）] > [アクション（Actions）] > [モジュール（Modules）]**を選択します。

ステップ 2 管理するインスタンスを持つ修復モジュールの横にある表示アイコン（  ）をクリックします。

ステップ 3 修復インスタンスを管理します。

- 追加：インスタンスを追加するには、[追加（Add）] をクリックします。システム付属のモジュールについては、次を参照してください。
  - ISE EPS インスタンスの追加 （4 ページ）
  - Cisco IOS インスタンスの追加 （7 ページ）
  - Nmap スキャン インスタンスの追加
  - セット属性値インスタンスの追加 （13 ページ）

  カスタムモジュールのインスタンスを追加する際のヘルプは、そのモジュールのドキュメントを参照してください（提供されている場合）。
- 設定：インスタンスの詳細を設定して、インスタンスに修復を追加するには、表示アイコン（  ）をクリックします。
- 削除：使用されていないインスタンスを削除するには、削除アイコン（  ）をクリックします。